

# Jellyfin Media Server on AWS

## Project Overview

This project creates a Jellyfin media server with scalable storage hosted on AWS. It combines multiple AWS services to reliably stream via web browser access and flexible media management.

### What You'll Build

- **Jellyfin Server** - A media server running on AWS EC2
- **Secure Access** - HTTPS-enabled access via Application Load Balancer
- **Scalable Storage** - EBS volumes for high-throughput media storage
- **Content Management** - S3 bucket integration for easy media uploads

### Architecture Overview

This solution uses these AWS microservices:

- **VPC** provides secure networking with public and private subnets
- **EC2** hosts the Jellyfin media server application
- **EBS** provides high-performance storage for media content
- **S3** stores your media files for easy uploading and management
- **ALB** provides HTTPS access and could enable future scaling
- **IAM Roles** allow secure connections between services

### Prerequisites

#### Software Requirements

- Web browser to access AWS Console and Jellyfin interface
- SSH client (built into browser for EC2)
- Media files to stream (videos, music, etc.)

#### Cost

- EC2 t2.micro: ~\$8.50/month (free tier eligible for 12 months)
- EBS SC1 storage: ~\$0.025/GB-month (SC1 because we don't need as much throughput for small amount of people)
- S3 storage: ~\$0.023/GB-month
- Application Load Balancer: ~\$16.20/month

## Knowledge

- Basic understanding of AWS services
- Basic Linux command line knowledge
- Familiarity with editing text files in terminal

## Project Start

### Create VPC

Create a VPC with 2 public subnets and a private subnet. The reason we are creating two public subnets is for the ALB for later that requires two availability zones (AZ).

The screenshot shows the AWS VPC creation process. On the left, the 'VPC settings' section includes:

- Resources to create:**  VPC only (selected)  VPC and more
- Name tag auto-generation:**  Auto-generate, value: JellyfinVPC
- IPv4 CIDR block:**  No IPv4 CIDR block (selected)  Amazon-provided IPv4 CIDR block. Value: 10.0.0.0/16 (65,536 IPs)
- Tenancy:** Default
- Number of Availability Zones (AZs):**  1 (selected),  2,  3. Option to **Customize AZs**.
- Number of public subnets:**  0 (selected),  2,  4.
- Number of private subnets:**  0 (selected),  2,  4.

On the right, the 'Preview' section shows the VPC configuration:

- VPC:** JellyfinVPC-vpc (Show details)
- Subnets (4):** us-east-1a (JellyfinVPC-subnet-public1-us-), us-east-1a (JellyfinVPC-subnet-private1-us-), us-east-1b (JellyfinVPC-subnet-public2-us-), us-east-1b (JellyfinVPC-subnet-private2-us-)
- Route tables (3):** JellyfinVPC-rtb-public, JellyfinVPC-rtb-private1-us-east-1a, JellyfinVPC-rtb-private2-us-east-1b

At the bottom, there are links for CloudShell, Feedback, and a footer with copyright information: © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

### NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

**None**

In 1 AZ

1 per AZ

### VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

**None**

S3 Gateway

### DNS options [Info](#)

- Enable DNS hostnames
- Enable DNS resolution

### ▼ Additional tags

Add tags to the VPC and all resources within the VPC. Do not set the Name tag here. Set the Name tag under Name tag auto-generation above or directly in the visualizer.

[Add new tag](#)

You can add 49 more tags.

[Cancel](#)

 [Preview code](#)

[Create VPC](#)

## Create EC2 Instance

We are naming it EC2Image because we will use this to make images (copies) later.

## Name and tags Info

### Name

[Add additional tags](#)

## ▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

[Recents](#)[My AMIs](#)[Quick Start](#)[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

### Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type  
ami-084568db4383264d4 (64-bit (x86)) / ami-0ce4e709339fa8521a (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible



### Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

### Architecture

64-bit (x86)

### AMI ID

ami-084568db4383264d4

### Publish Date

2025-03-05

### Username

ubuntu

Verified provider

Search our full catalog including 1000s of application and OS Images

Recents | My AMIs | **Quick Start**

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

**Amazon Machine Image (AMI)**

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type | Free tier eligible ▾

ami-084568db4383264d4 (64-bit (x86)) / ami-0c4e709339fa8521a (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**  
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture	AMI ID	Publish Date	Username
64-bit (x86) ▾	ami-084568db4383264d4	2025-03-05	ubuntu

**Verified provider**

**▼ Instance type** [Info](#) | [Get advice](#)

**Instance type**

t2.micro | Free tier eligible ▾

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour  
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour  
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

[Compare instance types](#)

**Additional costs apply for AMIs with pre-installed software**

Configure the network to use the VPC we just made. Do not enable http access yet.

**▼ Network settings** [Info](#)

**VPC - required** | [Info](#)

vpc-039305848ac3e5f0d (JellyfinVPC-vpc)  
10.0.0.0/16

**Subnet** | [Info](#)

subnet-08e59ebd66d025f23 JellyfinVPC-subnet-public1-us-east-1a  
VPC: vpc-039305848ac3e5f0d Owner: 831926625893 Availability Zone: us-east-1a  
Zone type: Availability Zone IP addresses available: 4090 CIDR: 10.0.0.0/20

**Create new subnet** [Create new subnet](#)

**Auto-assign public IP** | [Info](#)

Enable

Additional charges apply when outside of [free tier allowance](#)

**Firewall (security groups)** | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  Select existing security group

**Security group name - required**

launch-wizard-5

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#,@[]+=&:{\$^\*

**Description - required** | [Info](#)

launch-wizard-5 created 2025-04-01T04:56:05.041Z

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type	Protocol	Port range
ssh	TCP	22

We're going to need a public ip to connect to the EC2 for now. So enable this.

**Auto-assign public IP** | [Info](#)

Enable

Additional charges apply when outside of [free tier allowance](#)

## Configuring EBS Storage

EBS storage is a storage device that can mount to EC2 for high throughput operations, such as video streaming. We're using SC1 for cheaper(but still fast enough) usage.

**Configure storage** Info Advanced

1x **8** GiB **gp3** Root volume, 3000 IOPS, Not encrypted

1x **125** GiB **sc1** EBS volume, Not encrypted Remove

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance.

## Setting up the EC2 Server

Connect to the EC2 instance using the browser connect.

Now let's download jellyfin and install it.

```
curl https://repo.jellyfin.org/install-debuntu.sh | sudo bash
```

Let it run through the process

## Attach the EBS

```
sudo mkfs -t ext4 /dev/xvdb
sudo mkdir /content
sudo mount /dev/xvdb /content
sudo mkdir /content/Movies
sudo chown -R jellyfin:jellyfin /content
sudo chmod 755 /content
echo "/dev/xvdb /content//Movies ext4 defaults,nofail 0 2" | sudo tee -a /etc/fstab
```

```
sudo systemctl restart jellyfin
```

# Testing the EC2 server

Let's quickly test our server. Even though its public, we need to enable access to it in the security group

The screenshot shows the AWS EC2 Instances page for instance i-0d6f0155437f01754. The instance is running and has a public IPv4 address of 54.197.88.22. It is associated with a VPC ID (vpc-039305848ac5e5f0d) and a subnet (subnet-0794f1c1c64c4f493). The instance type is t2.micro. The security group assigned is JellyfnEC2SSReader. The instance was launched on March 31, 2025, at 14:23:32 GMT-0400.

Click on launch wizard security group

The screenshot shows the Security groups section. Two security groups are listed: sg-0cdd22001efbe957d (default) and sg-023c09592abc9ad1e (launch-wizard-4). The second one is underlined, indicating it is selected.

## Inbound rules

Edit the inbound rules

The screenshot shows the Edit inbound rules interface. A single rule is listed: a Custom TCP rule on port 8096 from the source 67.170.232.89/32. There are buttons for Manage tags and Edit inbound rules.

Add a TCP rule for 8096 for YOUR IP specifically.

The screenshot shows the Add new rule interface. A TCP rule is being created for port 8096. The source is set to 67.170.232.89/32. The Description field is empty. A Delete button is visible.

Now connect to it with its public ip

## i-0d6f0155437f01754 (JellyfinEC2Image)

Details Status and alarms Monitoring Security Networking Storage Tags

### ▼ Instance summary Info

#### Instance ID

 i-0d6f0155437f01754

#### IPv6 address

-

#### Hostname type

Will have to use http, so replace the https with http

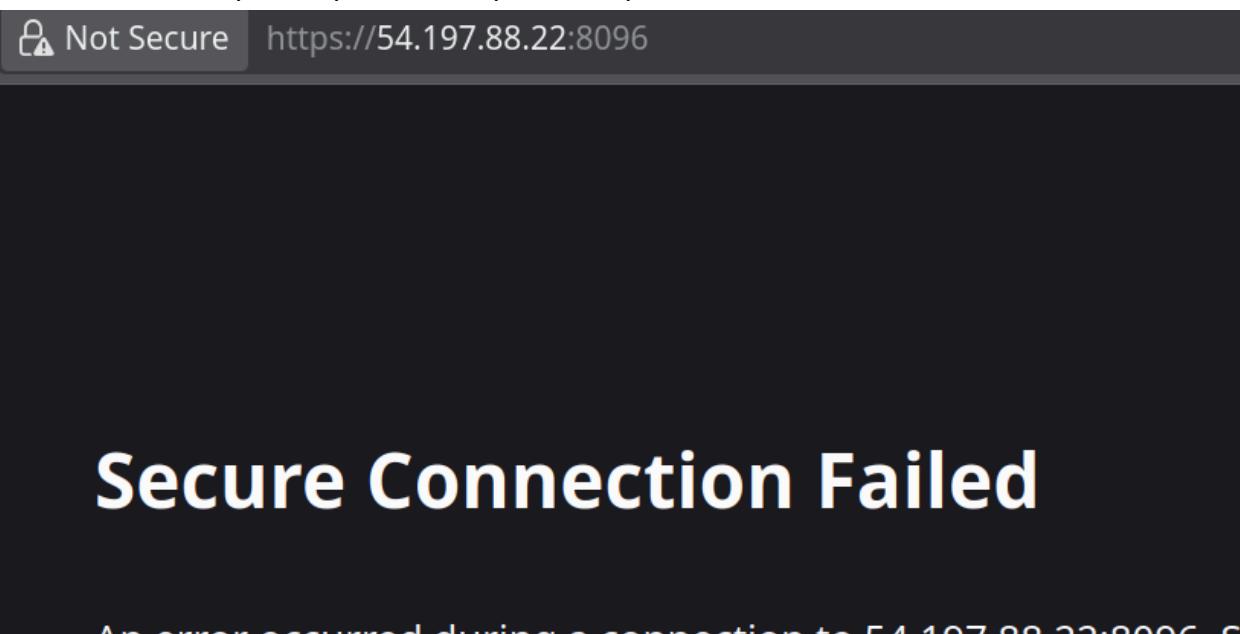
#### Public IPv4 address

 54.197.88.22 | [open address](#) 

#### Instance state

 Running

#### Private IP DNS name (IPv4 only)



Do **NOT** go through the set up wizard yet. You are on http! It's not safe.

## Setting up HTTPS -> Create a target group

On the EC2 Homepage, go to target groups and create one for instances. Name it something fitting.

## Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

### Basic configuration

Settings in this section can't be changed after the target group is created.

#### Choose a target type

##### Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

##### IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

##### Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

##### Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

#### Target group name

JellyFinTargets

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

#### Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

We're going to be using http(not https) protocol to communicate within the VPC.

##### Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

#### Target group name

JellyFinTargets

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

#### Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation is created. This choice cannot be changed after creation

HTTP

80

1-65535

#### IP address type

Only targets with the indicated IP address type can be registered to this target group.

##### IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

##### IPv6

Each instance register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

#### VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

JellyfinVPC-vpc

vpc-039305848ac3e5f0d

IPv4 VPC CIDR: 10.0.0.0/16

#### Protocol version

##### HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

##### HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

##### gRPC

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Now target the 8096 port on the Jellyfin EC2. This is the port jellyfin will start on. Press include as pending below, then create the target group.

### Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

**Available instances (1/1)**

Instance ID	Name	State	Security groups	Zone	Private IP
<input checked="" type="checkbox"/> i-0d6f0155437f01754	JellyfinEC2Image	<span>Running</span>	launch-wizard-4	us-east-1b	10.0.2

1 selected

**Ports for the selected instances**  
Ports for routing traffic to the selected instances.

8096
------

1-65535 (separate multiple ports with commas)

[Include as pending below](#)

**Review targets**

**Targets (0)**

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
-------------	------	------	-------	-----------------	------	----------------------	-----------	-------------

No instances added yet  
Specify instances above, or leave the group empty if you prefer to add targets later.

0 pending [Cancel](#) [Previous](#) [Create target group](#)

# Create Application Load Balancer

We'll be using a public application load balancer has the public facing access for our EC2s

### Load balancer types

**Application Load Balancer** [Info](#)

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Create](#)

**Network Load Balancer** [Info](#)

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Create](#)

**Gateway Load Balancer** [Info](#)

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

[Create](#)

► **Classic Load Balancer - previous generation**

Create the ALB with these settings

#### Basic configuration

##### Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

JellyfinALB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

##### Scheme [Info](#)

Scheme can't be changed after the load balancer is created.

Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

##### Load balancer IP address type [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

IPv4

Includes only IPv4 addresses.

Dualstack

Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

**Network mapping** [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | [Info](#)  
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

JellyfinVPC-vpc  
vpc-039305848ac3e5f0d  
IPv4 VPC CIDR: 10.0.0.0/16

**IP pools - new** | [Info](#)  
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools](#) in [Amazon VPC IP Address Manager console](#).

Use IPAM pool for public IPv4 addresses  
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

**Availability Zones and subnets** | [Info](#)  
Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

us-east-1a (use1-az1)  
Subnet  
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.  
subnet-08e59ebd66d025f23  
IPv4 subnet CIDR: 10.0.0.0/20

us-east-1b (use1-az2)  
Subnet  
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.  
subnet-0794f1c1c64c4f493  
IPv4 subnet CIDR: 10.0.16.0/20

JellyfinVPC-subnet-public1-us-east-1a  
JellyfinVPC-subnet-public2-us-east-1b

## Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

### Security groups

Select up to 5 security groups

default

sg-0cdd22001efbe957d VPC: vpc-039305848ac3e5f0d

Set the target as the previous target group we had earlier.

## Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

### ▼ Listener HTTP:80

Protocol

HTTP

Port

: 80

▼

1-65535

Default action | [Info](#)

Forward to  Select a target group

[Create target group](#)

✖ You must select at least one target group.

### Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

Create the ALB

## Creating a self signed certificate

Create a self signed certificate here

[https://www.samltool.com/self\\_signed\\_certs.php](https://www.samltool.com/self_signed_certs.php)

This will allow us to use https on our server.

## Use the ALB DNS for the Common Name.

A private key, the certificate signing request, will be created for you.

CLEAR FORM FIELDS

Country Name	Locality Name (Optional)
United States	
State or Province Name	Organization Unit Name (Optional)
Organization Name	Email Address (Optional)
Common Name, the domain	Bits to generate the private key
	1024 bits
Valid days	Digest Algorithm
365	SHA512

## Add an https listener to our ALB.

JellyfinALB [Alt+S] United States (N. Virginia) K12ThalisonAWSCourse

Application Load Balancers now support public IPv4 IP Address Management (IPAM)  
You can get started with this feature by configuring IP pools in the Network mapping section.

Actions ▲

**JellyfinALB**

**▼ Details**

Load balancer type Application	Status Active	VPC vpc-039305048ac3e5f0d	Load balancer IP address IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones subnet-0794f1c1c64caf493 us-east-1b (use1-az2) subnet-08e59ebd66d025f23 us-east-1a (use1-az1)	Date created March 31, 2025, 05:53:22
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:831926625893:loadbalancer/app/JellyfinALB/5225a3e4723b1046		DNS name info JellyfinALB-1867737233.us-east-1.elb.amazonaws.com (A Record)	Add listener

Listeners and rules | Network mapping | Resource map | Security | Monitoring | Integrations | Attributes | Capacity | Tags

**Listeners and rules (1) Info**

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
HTTPS:443	Forward to target group • JellyFinTargets 1 (100%) • Target group stickiness: Off	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2...	JellyfinALB-1867737233.us-eas...	Off	Not applicable

### Listener details: HTTPS:443

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

#### Listener configuration

The listener will be identified by the protocol and port.

##### Protocol

Used for connections from clients to the load balancer.

HTTPS

##### Port

The port on which the load balancer is listening for connections.

443

1-65535

#### Default actions | Info

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

#### Authentication | Info

Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#)

Use OpenID or Amazon Cognito

Include authentication using either OpenID Connect (OIDC) or Amazon Cognito.

#### Routing actions

Forward to target groups

Redirect to URL

Return fixed response

#### Forward to target group | Info

Choose a target group and specify routing weight or [Create target group](#)

##### Target group

JellyFinTargets

Target type: Instance, IPv4

HTTP

Weight	Percent
1	100% 0-999

[Add target group](#)

You can add up to 4 more target groups.

#### Target group stickiness | Info

Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

Turn on target group stickiness

### Secure listener settings | Info

These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.

#### Security policy | Info

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

##### Security category

All security policies

ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

#### Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a cert to your listener certificate list.

##### Certificate source

From ACM

From IAM

Import certificate

##### Certificate import destination

Import your certificate to either AWS Certificate Manager (ACM) or Amazon Identity and Access Management (IAM). It will be imported and made the default SSL/TLS server certificate for this load balancer's secure listeners.

Import to ACM - recommended

Prerequisites apply. [Learn more](#)

Import to IAM

Use IAM as a certificate manager only if you must support HTTPS connections in a Region not supported by ACM. [Learn more](#)

##### Certificate private key

```
-----BEGIN PRIVATE KEY-----  
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDXRyXP+TvD4Ub2  
ZUvV1IfJmisR7iQCQrRUKVULogFCC1vCOS1ih3Yx2A08JEFvyodboxC/Dv3jDJCr
```

##### Certificate body

```
-----BEGIN CERTIFICATE-----  
MIIDKzCCAhMCFHykVKdOkB1dvZXKtqnmGmyapKaxMA0GCSqGSIb3DQEBCwUAMFk  
C2AJBgNVBAYTAlVTMREwDwYDVQQIDAhOZXcgWW9yazERMA8GA1UEBwwIQnJvb2ts
```

##### Certificate chain - optional

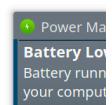
Paste the PEM-encoded certificate chain here

#### Client certificate handling | Info

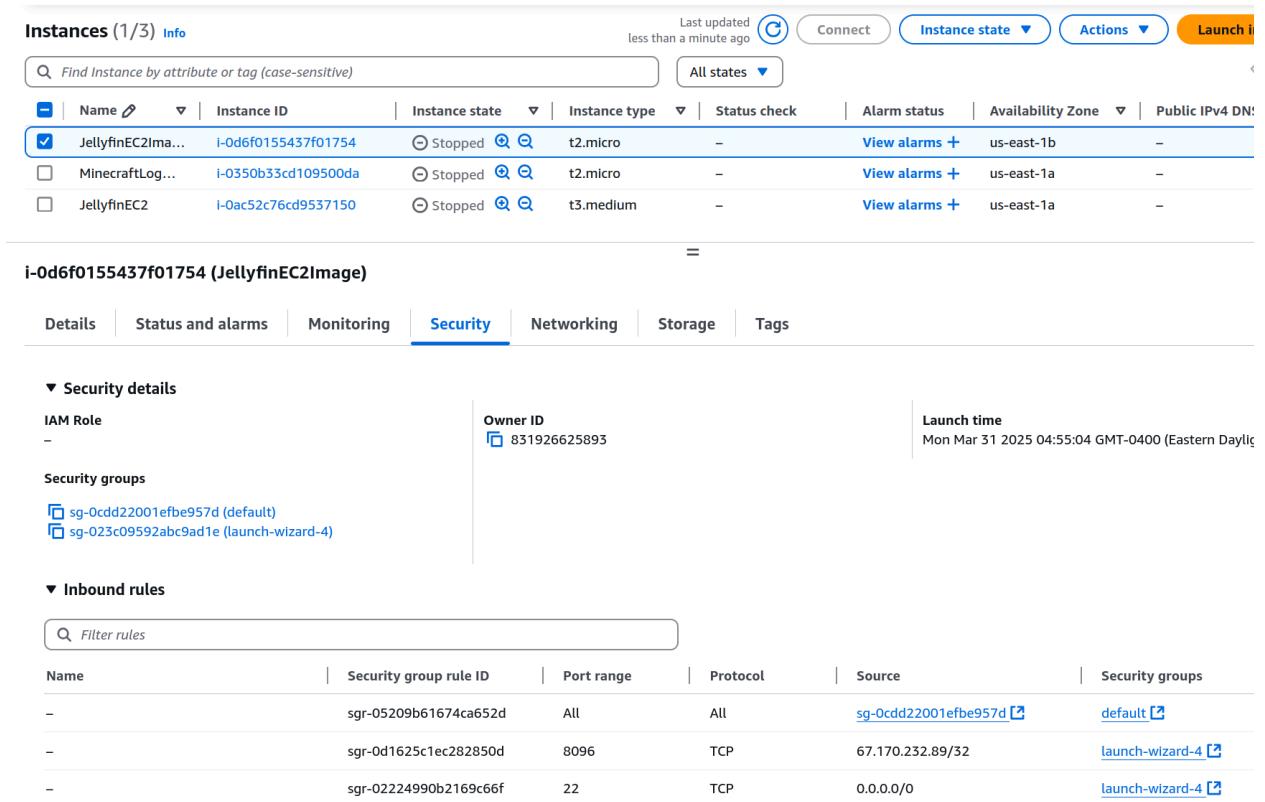
Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

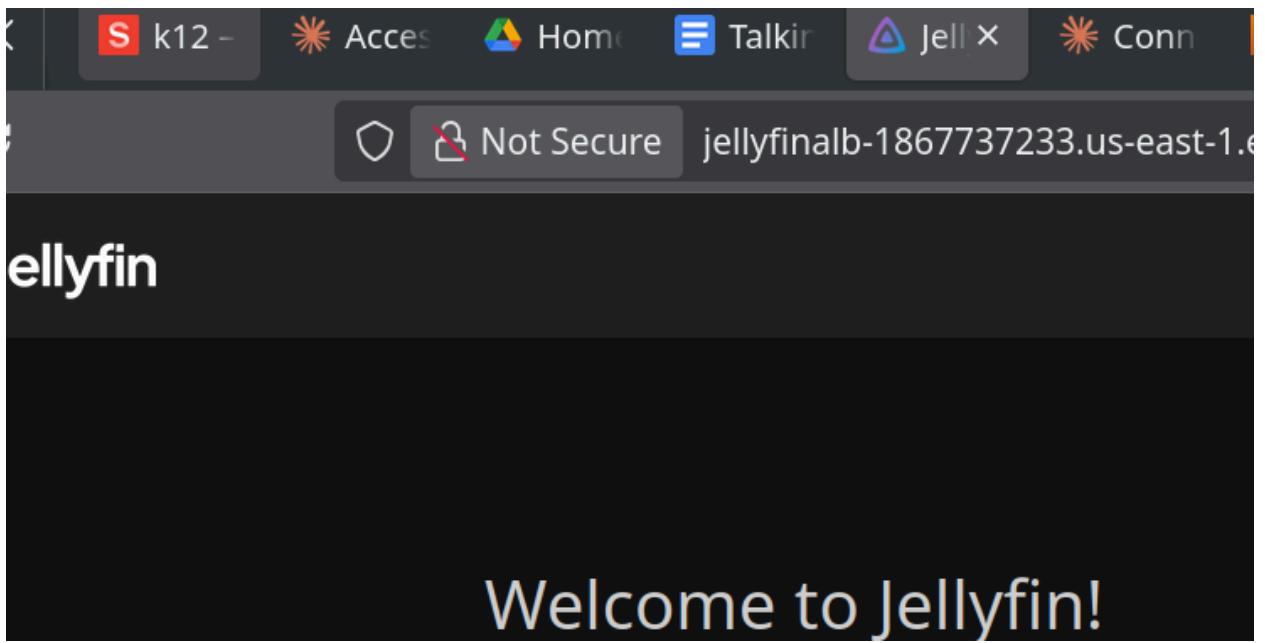


Add the default security group to the EC2, so that the ALB can send data to the EC2. This is because you can send data to other services in the same security group.

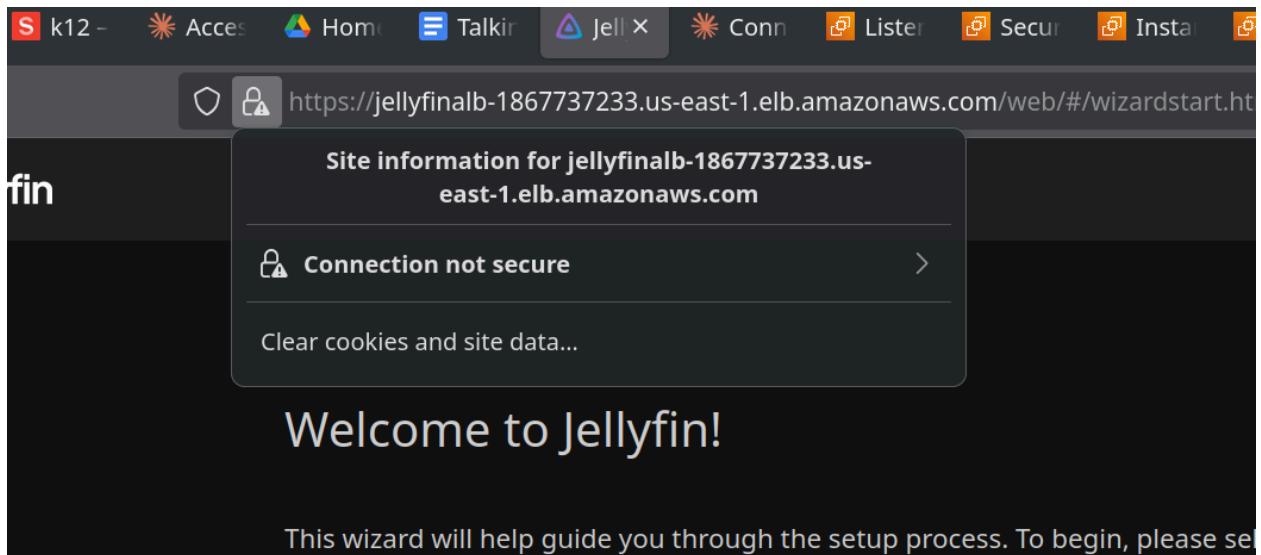


The screenshot shows the AWS CloudWatch Metrics console. At the top, there's a search bar with placeholder text "Find Metric by attribute or tag (case-sensitive)". Below it is a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. Three instances are listed: "JellyfinEC2Image" (selected), "MinecraftLog...", and "JellyfinEC2". The "Security" tab is selected in the navigation bar below the table. Under "Security details", it shows the IAM Role (empty), Owner ID (831926625893), and Launch time (Mon Mar 31 2025 04:55:04 GMT-0400 (Eastern Daylight Time)). Under "Security groups", two groups are listed: "sg-0cdd22001efbe957d (default)" and "sg-023c09592abc9ad1e (launch-wizard-4)". The "Inbound rules" section shows three rules with columns: Name, Security group rule ID, Port range, Protocol, Source, and Security groups. The rules are: "sgr-05209b61674ca652d" (All, All, sg-0cdd22001efbe957d, default), "sgr-0d1625c1ec282850d" (8096, TCP, 67.170.232.89/32, launch-wizard-4), and "sgr-02224990b2169c66f" (22, TCP, 0.0.0.0/0, launch-wizard-4).

Now try connecting to the ALB DNS. Make sure we use https:// by putting that in front of the dns. If it shows not secure, it's http.

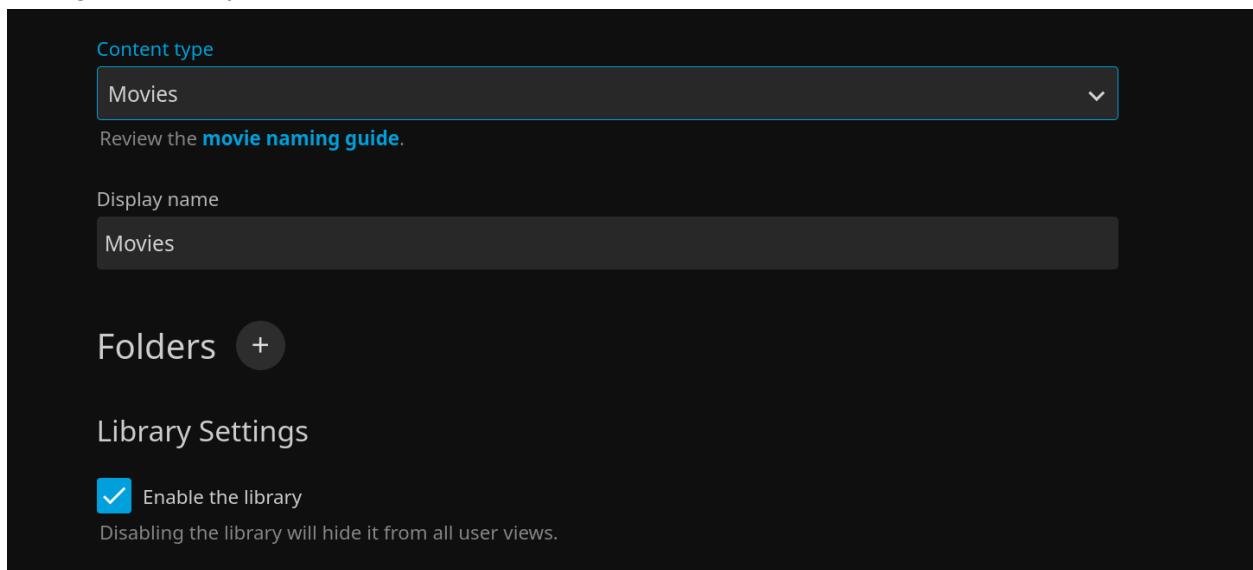


Example of https. Still says connection not secure though (because self signed cert)

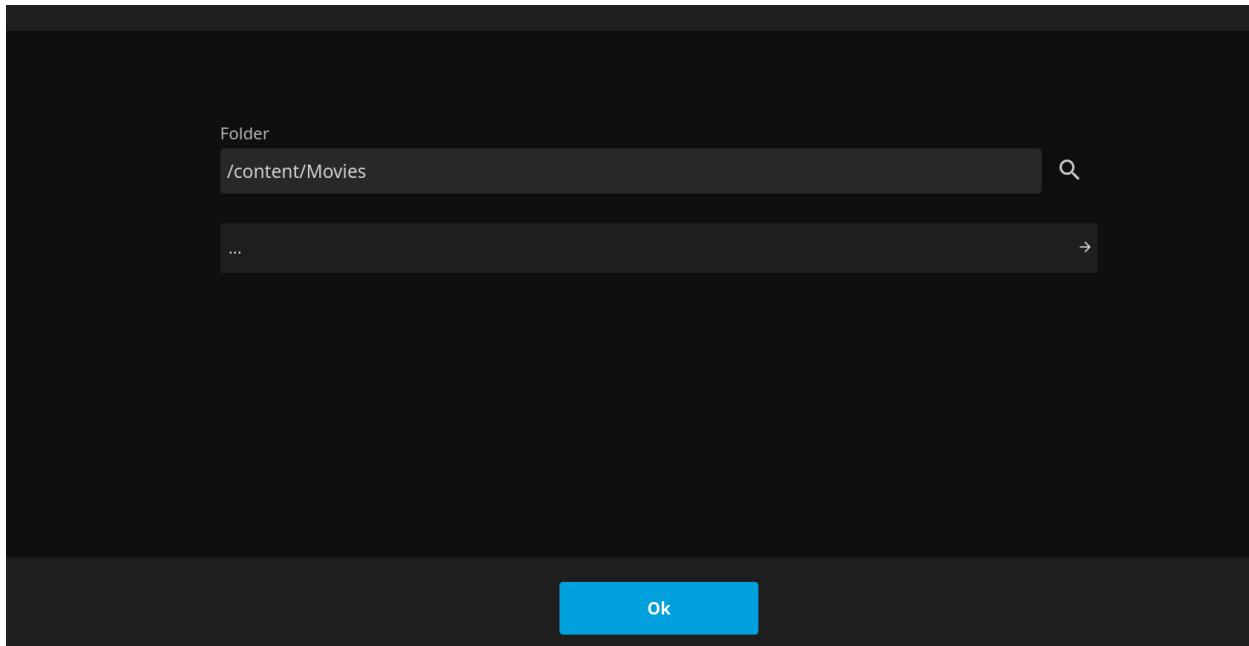


Now go through the process with https setup. Set up the admin credentials (Remember this!) Set up a movie folder when prompted to create a library.

Change content type to movies. Press plus button on Folders



Put in this path



Finish installation and login with admin and password credentials created earlier

## Creating S3 Bucket

We will use an S3 bucket to easily upload files and store the videos.

Create the S3 bucket. Remember, bucket must be unique (globally too, across all users)

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The first step, 'General configuration', is selected. It includes fields for 'Bucket name' (set to 'jellyfinmediak12stem'), 'AWS Region' (set to 'US East (N. Virginia) us-east-1'), and 'Bucket type' (set to 'General purpose'). The second step, 'Object Ownership', is shown below, with the 'ACLs disabled (recommended)' option selected. A tooltip for this option states: 'All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.' A preview section on the right shows the bucket's ARN and a 'Spectacle' icon.

keep all default settings

Create a folder called Movies/

Delete

Actions ▾

Create folder



or others to access your objects, you'll need to explicitly grant them permissions. Learn more ↗

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

**Objects (1)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) ↗ to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#) ↗

Find objects by prefix

Name	Type	Last modified	Size	Storage class
Movies/	Folder	-	-	-

Actions ▾ Create folder Upload

Upload your video of choice in the movies folder

#### Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#) ↗

Drag and drop files and folders you want to upload here, or choose Add files or Add folder.

#### Files and folders (1 total, 21.0 MB)

All files and folders in this table will be uploaded.

Remove

Add files

Add folder

#### Destination Info

##### Destination

s3://jellyfinmediak12stem/Movies/ ↗

##### Destination details

Bucket settings that impact new objects stored in the specified destination.

## Syncing -> Creating an IAM Role

We need to create an IAM role to allow the EC2 to sync with the S3 bucket.

Go to IAM dashboard and create a new role.

Identity and Access Management (IAM)			
Roles (13) <small>Info</small>			
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.			
<input type="text"/> Search			
Role name	Trusted entities	Last activity	▼
<a href="#">AWSServiceRoleForAPIGateway</a>	AWS Service: ops.apigateway (Service)	24 days ago	
<a href="#">AWSServiceRoleForEc2InstanceConnect</a>	AWS Service: ec2-instance-connect (Service)	20 hours ago	
<a href="#">AWSServiceRoleForElasticLoadBalancing</a>	AWS Service: elasticloadbalancing (Service)	9 hours ago	
<a href="#">AWSServiceRoleForGlobalAccelerator</a>	AWS Service: globalaccelerator (Service)	-	
<a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds (Service-Linked Role)	14 minutes ago	
<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linked Role)	-	
<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service)	-	
<a href="#">EC2SystemsManagerRole</a>	AWS Service: ec2	-	
<a href="#">FormPostInsertRDS-role-ebrpu38p</a>	AWS Service: lambda	6 days ago	

IAM > Roles > Create role

Step 3  
Name, review, and create

**Trusted entity type**

- AWS service  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy  
Create a custom trust policy to enable others to perform actions in this account.

### Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

#### Service or use case

EC2

Choose a use case for the specified service.

#### Use case

EC2

Use the s3readonly policy. Name the role something reasonable.

The screenshot shows the 'Add permissions' step of the IAM role creation wizard. On the left, a navigation bar indicates 'Step 1 Select trusted entity', 'Step 2 Add permissions' (which is selected), and 'Step 3 Name, review, and create'. The main area is titled 'Add permissions' with a sub-section 'Permissions policies (1/1046)'. A search bar shows 's3' and a filter dropdown set to 'All types'. Below is a table with columns 'Policy name', 'Type', and 'Description'. One row, 'AmazonS3ReadOnlyAccess', is highlighted with a blue border.

## Name, review, and create

This section shows 'Role details'. The 'Role name' field contains 'JellyfinEC2Reader'. The 'Description' field contains 'Allows EC2 instances to call AWS services on your behalf.' Both fields have character limits and examples provided.

## Step 1: Select trusted entities

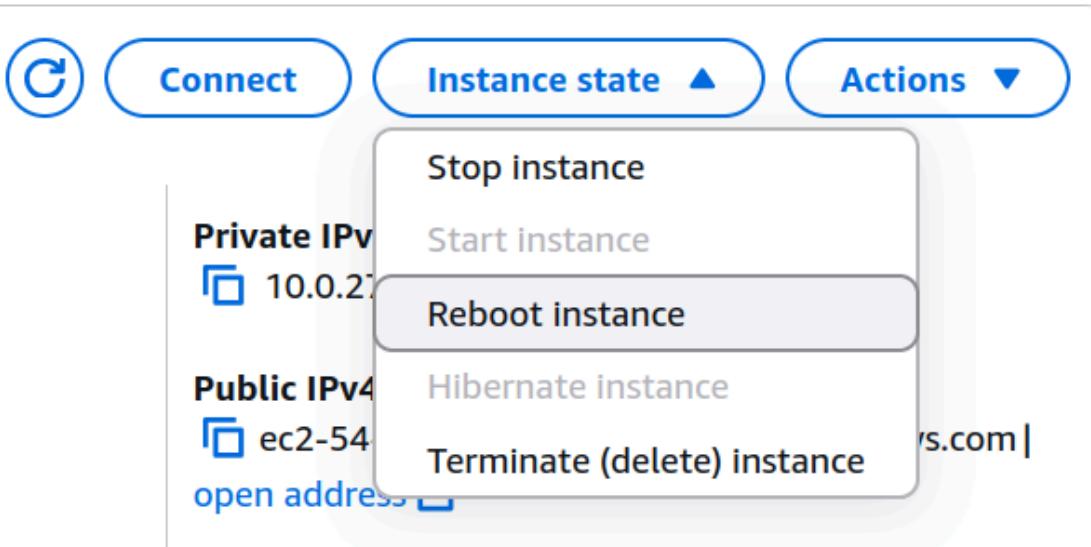
Edit

This section shows the 'Trust policy' field, which contains a JSON snippet:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "sts:AssumeRole"
8     }
9   ]
}
```

## Add the role to the EC2 instance

This section shows the 'Instance summary for i-0d6f0155437f01754 (JellyfinEC2Image)'. It displays various instance details like Public IP, Instance state, and Hostname type. On the right, a vertical 'Actions' menu is open, showing options such as Connect, Manage instance state, Instance settings, Networking, Security, Image and templates, and Monitor and troubleshoot. The 'Modify IAM role' option is also listed under the Actions menu.



## Sync bucket

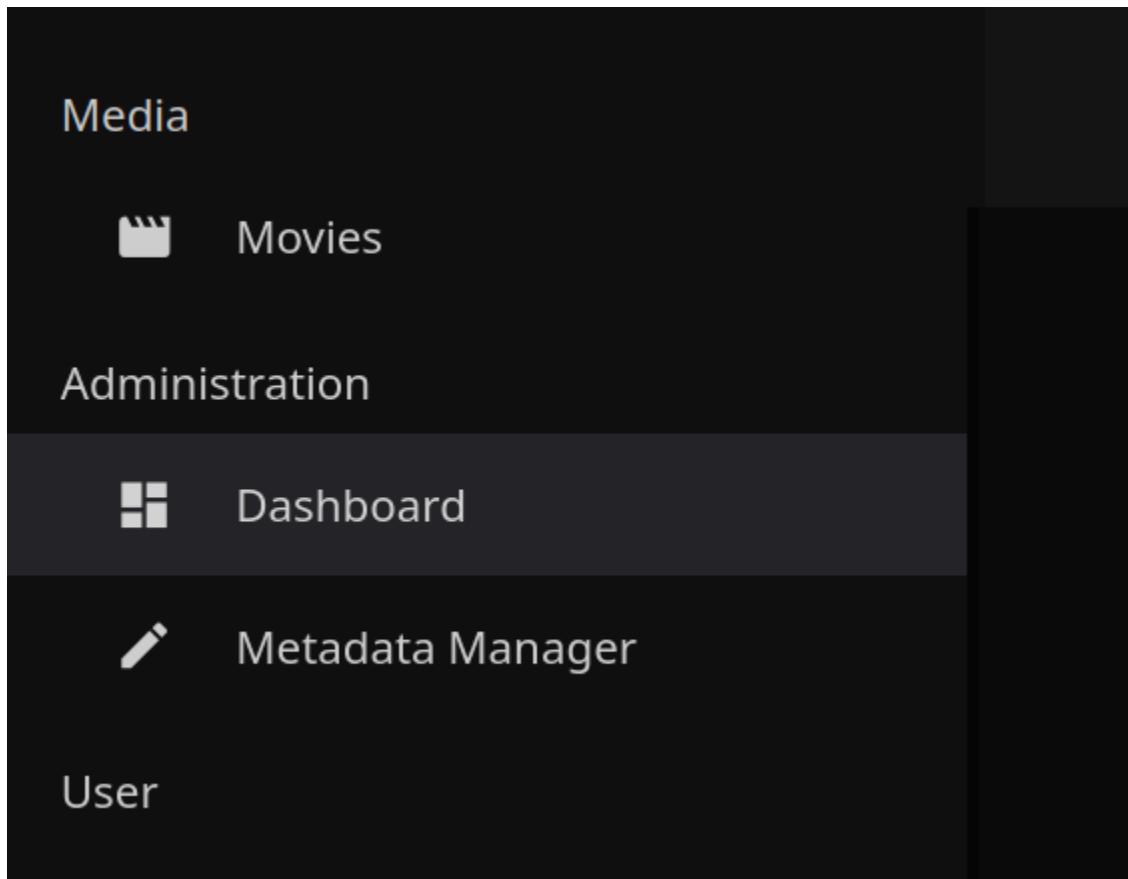
Sync your bucket by going through these commands

```
sudo apt update  
sudo snap install aws-cli --classic  
  
sudo -u jellyfin aws s3 sync s3://your-bucket-name/ /content/  
example: sudo -u jellyfin aws s3 sync s3://jellyfinmediak12stem/ /content/
```

The video should now show up in your folders.

## Refresh Jellyfin

Go to the administrator panel and refresh the library for jellyfin to find the files



SERVER VERSION

10.10.6

**Web version**

10.10.6 (c335a)

**Build version**

10.10.6

**Scan All Libraries**

**Restart**

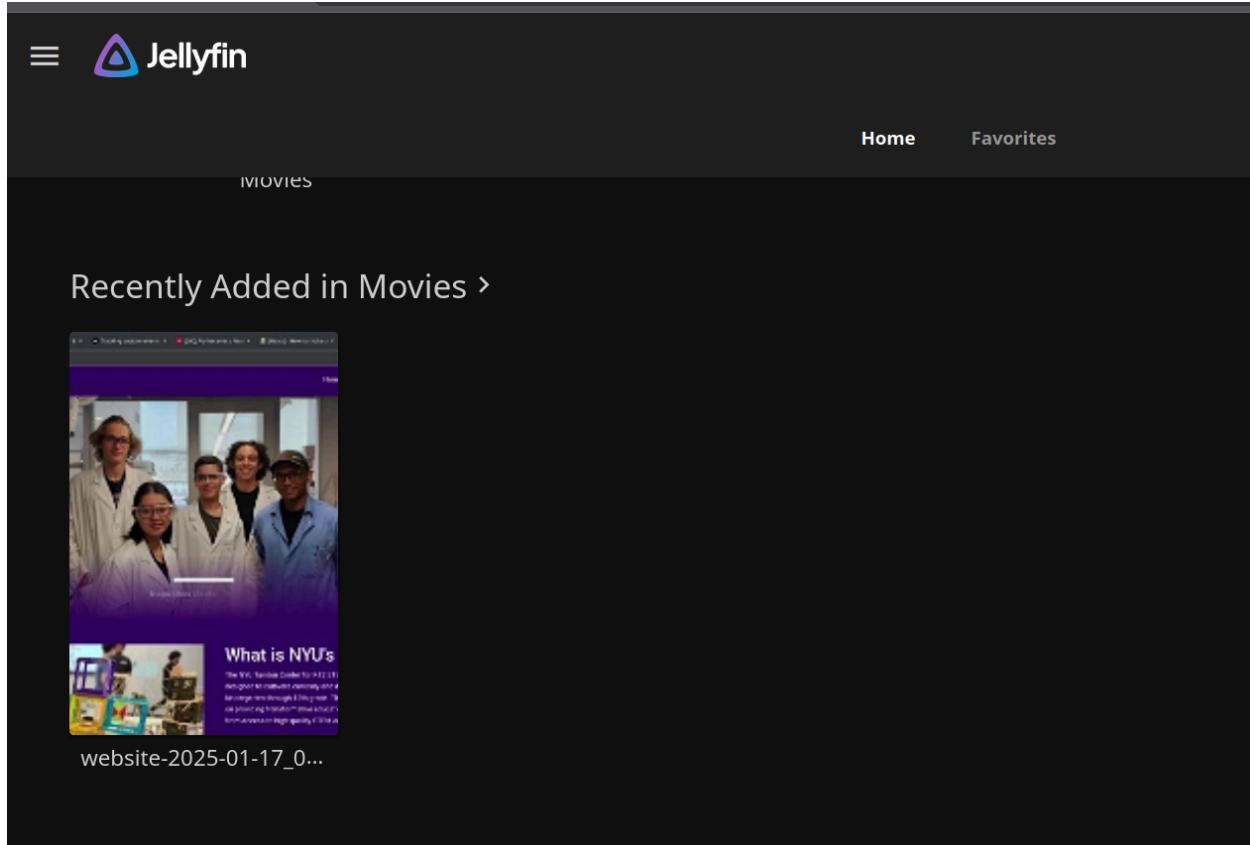
**Shutdown**

Active Devices >



Firefox

Jellyfin Web 10.10.6



## Creating an Image

Let's create an Image of the server we just made (to save the work and also to create copies later)

d6f0155437f01754

**Instance summary for i-0d6f0155437f01754 (JellyfinEC2Image)** [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 address
i-0d6f0155437f01754	54.197.88.22   <a href="#">open address</a>	10.0.27.161
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-54-197-81-161.ec2.internal   <a href="#">open address</a>
Hostname type	Private IP DNS name (IPv4 only)	Create image
IP name: ip-10-0-27-161.ec2.internal	ip-10-0-27-161.ec2.internal	Create template from instance
Answer private resource DNS name	Instance type	Launch more like this
-	t2.micro	Elastic IP addresses
Auto-assigned IP address	VPC ID	AWS Compute Optimizer finding
54.197.88.22 [Public IP]	vpc-039305848ac3e5f0d (JellyfinVPC-vpc)	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>
IAM Role	Subnet ID	Auto Scaling Group name
JellyfinEC2S3Reader	subnet-0794f1c1c64c4f493 (JellyfinVPC-subnet-public2-us-east-1b)	-

**Create image** [Info](#)

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

**Instance ID**  
i-0d6f0155437f01754 (JellyfinEC2Image)

**Image name**  
JellyfinServerImage  
Maximum 127 characters. Can't be modified after creation.

**Image description - optional**  
Image description  
Maximum 255 characters

**Reboot instance**  
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

**Instance volumes**

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/sda1	Create new snapshot ...	8	EBS General Purpose ...	3000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

## Launching an EC2 instance with more Oomph (Do it yourself)

You can now use this image to launch instances that are stronger. The current t2.micro can only support direct play on very small videos. It will **LAG** on bigger videos like 1080p and 4k videos with multiple people watching at once. That's why we can use the image to create an instance that is exactly the same, but running with better hardware. We can also put it behind a private subnet now, if you automate the syncing, so that you don't have to interact with the server anymore.

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | **My AMIs** | Quick Start

Owned by me |  Shared with me

[Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

JellyfinServerImage ami-021c36a3c4035f78c 2025-04-01T04:29:16.000Z	Virtualization: hvm	ENAv2 enabled: true	Root device type: ebs	Boot mode: uefi-preferred
--------------------------------------------------------------------------	---------------------	---------------------	-----------------------	---------------------------

Description

-

Architecture      AMI ID

x86\_64      ami-021c36a3c4035f78c

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t3.medium	All generations
Family: t3    2 vCPU    4 GiB Memory    Current generation: true	On-Demand SUSE base pricing: 0.0979 USD per Hour
On-Demand Windows base pricing: 0.06 USD per Hour	On-Demand Linux base pricing: 0.0416 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0451 USD per Hour	On-Demand RHEL base pricing: 0.0704 USD per Hour

[Compare instance types](#)

End

Make sure to delete/stop and resources you are not using. Things to note:

- Your EBS storage volume is not automatically deleted when terminating the EC2. You have to manually delete it
- Your ALB must be deleted, it cannot be just turned off
-