

coturn setup in AWS EC2 instance

Overview

It may be useful to deploy a [TURN server](#) for users to publish and play streams with media ports closed on users side. If internal TURN server is not enough for some reasons, and it is not desirable to deploy a separate AWS EC2 instance for this task, or the server should be used in [autoscaling group](#), the [coturn](#) server can be deployed in the same instance with WCS.

WCS EC2 instance deploying

Deploy AWS EC2 WCS instance as described [here](#). Add TCP port 443 to security group while launching the instance.

Inbound rules					Edit inbound rules	
Type	Protocol	Port range	Source	Description - optional		
Custom TCP	TCP	9091	0.0.0.0/0	-		
Custom TCP	TCP	8888	0.0.0.0/0	-		
Custom UDP	UDP	30000 - 33000	0.0.0.0/0	-		
Custom TCP	TCP	1935	0.0.0.0/0	-		
Custom TCP	TCP	554	0.0.0.0/0	-		
SSH	TCP	22	0.0.0.0/0	-		
Custom TCP	TCP	8443 - 8445	0.0.0.0/0	-		
Custom TCP	TCP	3478	0.0.0.0/0	-		
Custom UDP	UDP	1935	0.0.0.0/0	-		
HTTPS	TCP	443	0.0.0.0/0	-		
Custom TCP	TCP	8080 - 8084	0.0.0.0/0	-		

WCS configuration

Add the following parameter to [flashphoner.properties](#) file

```
rtc_ice_add_local_interface=true
```

and restart WCS.

coturn installation and configuration

1. Install coturn from `epel-release` repository

```
sudo amazon-linux-extras install epel
sudo yum install coturn
```

2. Set the following parameters in coturn configuration file `/etc/coturn/turnserver.conf`

```
# Listen port 443
listening-port=443
# Listen on internal IP only
listening-ip=172.31.xx.xxx
# Set up external IP option as coturn manual recommends
external-ip=54.75.x.xxx/172.31.xx.xxx
# Set user and password
user=username:password
# Set the domain
realm=yourdomain.com
# Disable UDP listener
no-udp
# SSL certificate and key
cert=/etc/pki/coturn/public/cert.pem
cert=/etc/pki/coturn/private/cert.key
```

Leave the rest of coturn parameters by default

3. Add the following parameter to `[Service]` section of the `/lib/systemd/system/coturn.service` file to allow coturn to listen TCP port 443

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

4. Launch coturn

```
sudo systemctl start coturn
```

Testing

Open Firewall Traversal Streaming example page in Chrome browser, set your server name and port 443 to `TURN server` field, set username and password you configured in coturn settings, then publish and play a stream

Firewall Traversal Streaming

Local



96ee



Stop

Player



96ee

Stop

PUBLISHING

WCS Server

wss://test3.flashphoner.com

Turn Server

turn:test3.flashphoner.com:

Username of turn server

flashphoner

Credential of turn server

coM77EMrV7Cwhyah

Force relay



Disconnect

ESTABLISHED

PLAYING