AWS Configuration Guide

Overview

TRIOLL uses AWS services for game storage and delivery:

- **Cognito**: Anonymous authentication
- **S3**: Game file storage
- **CloudFront**: CDN (optional)

Current Configuration

```javascript
const AWS_CONFIG = {
    region: 'us-east-1',
    identityPoolId: 'us-east-1:c740f334-5bd2-43c6-85b9-48bfebf27268',
    gamesBucket: 'trioll-prod-games-us-east-1',
    apiEndpoint: 'https://4ib0hvu1xj.execute-api.us-east-1.amazonaws.com/prod'
};
```

S3 Bucket Structure

```
trioll-prod-games-us-east-1/
├── game-name-1234567890/
│   ├── index.html
│   ├── thumbnail.png
│   ├── manifest.json
│   ├── assets/
│   ├── js/
│   └── css/
└── another-game-0987654321/
    └── ...
```

Cognito Identity Pool

The identity pool allows anonymous users to upload games:

- No login required
- Temporary credentials
- Limited to S3 upload permissions

IAM Role Policy

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::trioll-prod-games-us-east-1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "public-read"
        }
      }
    }
  ]
}
```

Security Best Practices

1. **Never commit AWS credentials**
2. **Use Cognito for temporary credentials**
3. **Validate all file uploads**
4. **Set appropriate CORS headers**
5. **Monitor CloudWatch for unusual activity**

Troubleshooting

Upload Permissions Denied

- Check IAM role attached to Cognito Identity Pool
- Verify S3 bucket policy allows public-read ACL
- Check CORS configuration on S3 bucket

CORS Issues

Add this CORS configuration to S3 bucket:

```json
[
  {
    "AllowedHeaders": ["*"],
    "AllowedMethods": ["GET", "PUT", "POST", "HEAD"],
    "AllowedOrigins": ["*"],
    "ExposeHeaders": ["ETag"]
  }
]
```

Game Access Issues

- Ensure files are uploaded with `public-read` ACL

- Check CloudFront distribution if using CDN

- Verify index.html exists in game folder