🔐 AWS REKOGNITION SETUP GUIDE

Current Status

✅ **AWS Credentials**: Configured (Session-based)
❌ **IAM Permissions**: Missing Rekognition permissions
✅ **Region**: us-east-1
✅ **Integration**: Core Safety Loop implemented

📋 Required IAM Permissions

The current IAM role needs the following permissions for the Core Safety Loop to function:

1. Amazon Rekognition Permissions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rekognition:CreateCollection",
                "rekognition:DeleteCollection",
                "rekognition:ListCollections",
                "rekognition:DescribeCollection",
                "rekognition:IndexFaces",
                "rekognition:SearchFacesByImage",
                "rekognition:SearchFaces",
                "rekognition:DeleteFaces",
                "rekognition:ListFaces",
                "rekognition:DetectFaces",
                "rekognition:CompareFaces",
                "rekognition:DetectModerationLabels"
            ],
            "Resource": "*"
        }
    ]
}
```

2. S3 Permissions (for face image storage)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::safeplay-faces",
                "arn:aws:s3:::safeplay-faces/*"
            ]
        }
    ]
}
```

🔧 Setup Steps

Step 1: Update IAM Role Permissions

1. Go to AWS IAM Console
2. Find the role: `spark-permissions`
3. Add the above policies or create a custom policy
4. Attach the policy to the role

Step 2: Create S3 Bucket

```
aws s3 mb s3://safeplay-faces --region us-east-1
```

Step 3: Test Permissions

```
cd /home/ubuntu/safeplay-staging
node test-aws-config.js
```

Step 4: Initialize Face Collections

```
cd /home/ubuntu/safeplay-staging
node scripts/setup-face-collections.js
```

🏗️ Face Collection Structure

Collection Naming Convention

- **Format**: `safeplay-venue-{venueId}`

- **Example**: `safeplay-venue-123e4567-e89b-12d3-a456-426614174000`

Face Indexing Format

- **ExternalImageId**: `child-{childId}-{timestamp}`
- **Example**: `child-456e7890-e89b-12d3-a456-426614174001-1609459200000`

📊 Current Error Analysis

Error: `AccessDeniedException`
User: `arn:aws:sts::448970459817:assumed-role/spark-permissions/AbacusAIS3Session-user-code_policy_8e72b572e_bdsBx`
Action: `rekognition:ListCollections`
Resource: `arn:aws:rekognition:us-east-1:448970459817:collection/*`

Solution: Add Rekognition permissions to the `spark-permissions` role.

🎮 Demo Mode

Until AWS permissions are configured, the system runs in **Demo Mode**:
- ✅ Simulated face recognition events
- ✅ Real-time tracking dashboard
- ✅ Camera hardware integration
- ✅ WebSocket broadcasting
- ❌ Actual face recognition (requires AWS permissions)

🔄 Quick Permission Test

Run this command to test if permissions are working:

```
cd /home/ubuntu/safeplay-staging
node -e "
const { rekognitionClient } = require('./lib/aws/config.ts');
const { ListCollectionsCommand } = require('@aws-sdk/client-rekognition');

(async () => {
  try {
    const result = await rekognitionClient.send(new ListCollectionsCommand({}));
    console.log('✅ Rekognition permissions working!');
    console.log('Collections:', result.CollectionIds?.length || 0);
  } catch (error) {
    console.log('❌ Rekognition permissions needed');
    console.log('Error:', error.message);
  }
})();
"
```

⚡ Next Steps

1. **Configure IAM permissions** (see above)
2. **Create S3 bucket** for face storage
3. **Test permissions** with the test script
4. **Initialize face collections** for venues
5. **Deploy and test** the Core Safety Loop

📞 Support

If you need help with AWS configuration:
1. Check the IAM role permissions
2. Verify S3 bucket access
3. Run the permission test script
4. Contact AWS support if needed

The Core Safety Loop is ready to use once these permissions are configured!