

Delay-Flow SCTE-35 Automated Insertion

CloudFormation Deployment Documentation

Architecture Overview

The deployment consists of two CloudFormation templates:

1. Cluster Template (`ecsClusterTemplate-delayFlow.json`): Creates the ECS cluster infrastructure
 2. Task Template (`ecsTaskTemplate-delayFlow.json`): Deploys the application containers and monitoring stack
- Download the two CloudFormation templates for Delay-Flow:
<https://alcflow-config.s3.us-east-2.amazonaws.com/1.0/CloudFormation/ecsClusterTemplate-delayFlow.json>
<https://alcflow-config.s3.us-east-2.amazonaws.com/1.0/CloudFormation/ecsTaskTemplate-delayFlow.json>

IAM Roles and Policies

Cluster Template IAM Roles

1. ECS Instance Role (`IAMRoleForECS`)
 - Purpose: Enables EC2 instances to join ECS cluster and access required AWS services
 - Managed Policies:
 - `AmazonEC2ContainerServiceforEC2Role`: Core ECS functionality
 - `AmazonSSMManagedInstanceCore`: Systems Manager access for management

Task Template IAM Roles

1. Monitoring Task Role (`MonitoringTaskRole`)
 - Purpose: Enables containers to access CloudWatch and marketplace metering
 - Key Permissions:
 - CloudWatch Logs access
 - ECR repository access
 - AWS Marketplace metering
 - SSM Parameter Store access
2. Task Execution Role (`TaskExecutionRole`)
 - Purpose: Enables ECS to pull container images and send logs
 - Key Permissions:

- ECR authentication
- CloudWatch Logs access
- Marketplace image pull access

Security Configuration

Network Security

1. Security Group Configuration:
 - SSH access (Port 22)
 - Grafana web interface (Port 3000)
 - RTP video input (Port 5004/UDP)
 - SRT video output (Port 5005/UDP)
 - All ports restricted to necessary CIDR ranges (as set by user)

Encryption Configuration

1. Grafana HTTPS:
 - Self-signed certificates generated during deployment
 - Certificate location: `/etc/grafana/certs/`
 - Key rotation: keys are generated at instance boot-up
2. Data Storage:
 - Prometheus data retention: 7 days, 1GB limit
 - CloudWatch Logs retention: 30 days

Network Architecture

1. VPC Requirements:
 - Public subnet required for video input/output
 - Elastic IP assigned for stable addressing
 - Host networking mode for optimal video performance
2. Container Communication:
 - Prometheus (Port 9090)
 - Prometheus Pushgateway (Port 9091)
 - Grafana (Port 3000)
 - Video streams (Ports 5004-5005)

AWS Service Quotas and Costs

Service Quotas

1. ECS Service Limits:
 - Tasks per service: 1
 - CPU units: 2048 (2 vCPU)
 - Memory: 4GB total
 - Grafana: 500MB

- Prometheus: 800MB
- Pushgateway: 500MB
- Delay-Flow: 2000MB

2. EC2 Instance Limits:

- Default t4g.medium specifications
- 2 vCPU, 4GB RAM
- EBS storage: 30GB

Cost Breakdown

1. EC2 Instance (t4g.medium):
 - On-demand pricing varies by region
 - ~\$30-40/month
2. EBS Storage:
 - 30GB gp2 volume
 - ~\$3/month
3. CloudWatch Logs:
 - 4 log groups with 30-day retention
 - Estimated ~\$5-10/month depending on log volume
4. Network Transfer:
 - Video streaming bandwidth costs
 - \$0.09/GB for outbound traffic

Monitoring Configuration

CloudWatch Logs

Four log groups with 30-day retention:

- /ecs/prometheus
- /ecs/pushgateway
- /ecs/grafana
- /ecs/alchemy-flow

Certificate Rotation

To rotate Grafana certificates:

Reboot the EC2 instance

Template Customization

Key environment variables to modify in task template. See the ‘Container Configuration’ document for more information:

```
{ "Name": "INPUT_IP", "Value": "127.0.0.1" },  
{ "Name": "INPUT_PORT", "Value": "5004" },  
{ "Name": "OUTPUT_IP", "Value": "127.0.0.1" },  
{ "Name": "OUTPUT_PORT", "Value": "5005" },  
{ "Name": "DELAY_SECONDS", "Value": "135" },  
{ "Name": "STREAM_PROTOCOL", "Value": "rtp" }
```

Upgrade information

Because the Delay-Flow container is configurable inside of `ecsTaskTemplate-delayFlow.json`, you can modify that script to point to a new version of Delay-Flow. Delete the CloudFormation task template task, and create a new one using the updated `ecsTaskTemplate-delayFlow.json`.

Please test individually on each channel and monitor the new version. Then, deploy it to more of your channels.

Troubleshooting Guide

1. Container Startup Issues:
 - Check CloudWatch Logs for each container
 - Verify ECS instance has sufficient resources
 - Confirm IAM roles have correct permissions
2. Network Connectivity:
 - Verify security group allows required ports
 - Check Elastic IP association
 - Confirm VPC routing configuration
3. Video Stream Issues:
 - Verify input/output ports match configuration
 - Check network bandwidth utilization
 - Monitor CloudWatch metrics for packet loss