# Multi-Region AWS Services Auto-Tagging Infrastructure

## Overview

This documentation outlines the steps for setting up auto-tagging for AWS services created across multiple AWS regions. The solution utilizes AWS CloudTrail, AWS Lambda, AWS IAM Roles, and AWS EventBridge services to enable centralized logging and tagging of the infrastructure.

## Components

* **AWS CloudTrail:** Captures all API calls for creation events across all regions.
* **AWS Lambda:** Contains the python code for tagging.
* **AWS IAM Role:** Manages permissions for the Lambda function to tag various resources.
* **Amazon EventBridge:** Routes multi-region creation events to the centralized Lambda function.

## Architecture

* **Multi-Region CloudTrail:** Set up to track multi-region creation events. Deployed in the central region(us-east-1).
* **Centralized Lambda Function**: This triggers upon specific creation events and tags the newly created resources.
* **IAM Role for Lambda**: Grants the lambda function necessary permissions to tag resources.
* **Custom Event Bridge Bus**: Setup to trigger the lambda function on creation event API calls.
* **EventBridge Rules**: Set up in each AWS region to detect and forward events to the Custom Event Bus

A screenshot of a computer

Description automatically generated

## Procedures

## Step 1: Set Up Multi-Region CloudTrail

## A new CloudTrail was created and configured to apply to all regions, ensuring that any creation event is captured.

## CloudTrail: BIFX-auto-tagging

## Step 2: Create Centralized Lambda Function

## A Lambda function was created in a central AWS region(us-east-1). This function is responsible for tagging new resources based on the events received.

## Lambda: bifx-autotag-lambda

## Step 3: Configure IAM Role for Lambda

## An IAM role with the necessary permissions was created to allow the Lambda function to tag S3 resources across different regions. The permission set provided is:

## AWSCloudTrail\_ReadOnlyAccess

## AWSLambdaBasicExecutionRole

## A custom tagging policy: This policy contains all the tagging permissions for specific services.

## IAM Role: allow-s3-access-to-quilt-role

## Step 4: Create a custom event bus in the Central Region (us-east-1)

## A custom event bus was configured in the central region which accepts events forwarded from any event bus throughout any region in the account. This helps in mapping events forwarded from other regions to the central auto-tagging lambda function.

## A resource-based policy is attached to this custom event bus that accepts events from any event bus throughout the account.

## A rule is configured in this bus that forwards all creation events captured on this bus to the central lambda function. It keeps track of the below event pattern.

## Event Source: AWS Service

## AWS Service: S3, ec2, rds, lambda, dynamodb, elasticfilesystem, ecs

## Event Pattern: AWS API Call via CloudTrail

## Event Type Specification: Specific Operation(s) = All create events under the above services

## The target of this rule is the central lambda function (bifx-autotag-lambda).

## Step 5: Set Up EventBridge Rules to Route S3 Events from all the desired regions

## EventBridge rules were established in each AWS region on the default event bus to capture the S3 bucket creation events and forward them to the central event bus.

## Event Source: AWS Service

## AWS Service: S3, ec2, rds, lambda, dynamodb, elasticfilesystem, ecs

## Event Pattern: AWS API Call via CloudTrail

## Event Type Specification: Specific Operation(s) = All create events under the above services

## Target of the event bridge rule on the default event bus is the custom “central event bus”. Either an existing execution role or a new execution role (first time setup) can be attached.

## Step 6: Testing the Setup

## The auto-tagging feature was verified by inspecting the “CreatedBy” tag of the newly created S3 bucket.

## CloudWatch Logs were monitored under the “bifx-autotag-lambda” log group to ensure that the Lambda function is triggered and executed without errors.

## A screenshot of a bucket overview Description automatically generated