**Project Documentation: Auto-Stop Untagged EC2 Instances Using AWS Lambda**

**Overview**

This AWS Lambda function automatically stops or terminates EC2 instances that are launched without mandatory tags. It enhances cloud governance by enforcing tagging policies and preventing resource sprawl and untracked costs.

**Objective**

Ensure that all EC2 instances launched in the AWS account are properly tagged with required metadata (e.g., Name, Owner, Environment). If any instance is found without the required tags, the Lambda function automatically stops or terminates it shortly after launch.

**Architecture**

The architecture consists of the following components:  
- EC2 instance launch  
- EventBridge rule that triggers on instance state change  
- AWS Lambda function that checks for required tags  
- If tags are missing, the instance is stopped



**Required Tags**

You can define required tags such as:  
- Name  
- Owner  
- Environment

**Implementation Steps**

1. Create an IAM role for Lambda with permissions to describe, stop, and terminate EC2 instances.
2. Create a Lambda function that inspects the tags of a newly launched EC2 instance.
3. Define a list of required tags within the Lambda function.
4. If any of the required tags are missing, stop or terminate the EC2 instance.
5. Create an EventBridge rule that triggers the Lambda function on EC2 instance state changes (specifically when entering the 'running' state).
6. Test the solution by launching EC2 instances with and without the required tags.

**Security Considerations**

- Use least privilege principle for IAM roles.  
- Monitor Lambda logs using CloudWatch Logs.  
- Consider adding SNS notifications for stopped or terminated instances.

**Future Enhancements**

- Add configurable required tags via environment variables.  
- Notify via email (SNS) when untagged instances are stopped.  
- Support for other resources like RDS, Lambda, etc.