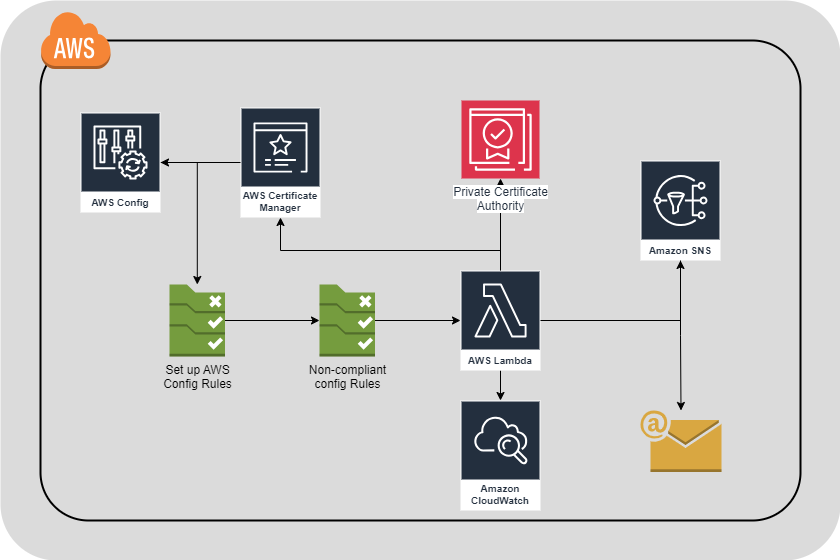
**Automating ACM Certificate Requests Using AWS Config & Lambda**

****

**Objective**

This document outlines the process to automatically request a new **Private ACM Certificate** with the latest **Private CA** using **AWS Config, AWS Lambda, and SNS Notifications**.

**Components Involved**

1. **AWS Config Rule**: Monitors ACM certificates and identifies expiring ones.
2. **AWS Lambda Function**: Requests a new certificate with the latest Private CA.
3. **Amazon SNS (Simple Notification Service)**: Sends notifications upon successful or failed requests.
4. **AWS CloudWatch Logs**: Stores execution logs for auditing and debugging.

**Step 1: Create an AWS Lambda Function**

**1.1 Create the Lambda Function**

1. **Go to AWS Lambda**.
2. Click **Create function**.
3. Choose **Author from scratch**.
4. **Function name**: aps-acm-cert-renewal.
5. **Runtime**: Python 3.8+.
6. **Execution Role**:
   * Create a new role or use an existing one.
   * Attach the necessary IAM policy (see Step 3).
7. Click **Create function**.

**1.2 Add the Python Code**

1. Open the **Lambda function**.
2. Copy and paste the following Python script:
3. Click **Deploy**.

**Step 2: Configure AWS Config Rule**

1. **Go to AWS Config** > **Rules**.
2. Click **Create Rule**.
3. Choose **Custom rule**.
4. **Enter Rule Name**: acm-cert-renewal.
5. **Trigger Type**: Periodic.
6. **Execution Frequency**: 12 hours.
7. Select **AWS Lambda Function** > Choose aps-acm-cert-renewal.
8. Click **Save**.

**Step 3: IAM Permissions for Lambda**

Attach the following IAM policy to the Lambda execution role:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"acm:ListCertificates",

"acm:DescribeCertificate",

"acm:RequestCertificate"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"acm-pca:ListCertificateAuthorities",

"acm-pca:DescribeCertificateAuthority"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": "sns:Publish",

"Resource": "arn:aws:sns:region:account-id:ACM\_Cert\_Request\_Notifications"

}

]

}

**✅ Summary**

* **AWS Config Rule** detects expiring **private** ACM certificates.
* **Lambda function** requests a new certificate with the **latest Private CA**.
* **SNS notifications** send success & failure alerts.
* **CloudWatch Logs** provide execution tracking.
* **IAM policies** ensure security & access control.

**Now, ACM private certificate requests are fully automated!**