**Implementation Plan for ACM Certificate Automation Effort**

**Objectives:**

1. Automate ACM certificate management processes.
2. Enable proactive certificate expiration management using custom email notifications for 30, 60, and 90 days before expiration.
3. Implement auto-renewal of ACM certificates.
4. Automate the process of swapping certificates in Load Balancers and EC2 instances, followed by deletion of old certificates.

**Sprint Breakdown**

**Sprint 17.1: Infrastructure Setup, Notifications, and Base Automation**

**Activities:**

1. Create and configure AWS resources for ACM automation.
   * IAM roles and policies for Lambda, SNS, ACM, EC2, and Load Balancers.
   * S3 bucket for storing logs and configurations.
2. Develop a script to fetch ACM certificates and check expiration dates.
   * Identify ACM certificates using AWS CLI/SDK.
   * Filter certificates expiring within 30, 60, and 90 days.
3. Implement the first notification system using SNS and Lambda:
   * Set up a generic SNS topic for certificate expiration alerts.
   * Configure email subscriptions for the SNS topic.
   * Write Lambda function to send notifications for certificates expiring in 30, 60, and 90 days.
4. Unit testing of Lambda and SNS integration.

**User Stories:**

* As an admin, I want an S3 bucket to store ACM certificate logs securely.
* As a DevOps engineer, I need IAM policies to grant specific permissions to ACM, SNS, and Lambda.
* As a system, I want to identify certificates expiring within a certain period to send timely alerts.
* As an admin, I want notifications via email when certificates are nearing expiration.

**Deliverables:**

* IAM roles/policies configured.
* S3 bucket for logs.
* Basic Lambda-SNS notification flow for 30, 60, and 90-day alerts.

**Sprint 17.2: Auto-Renewal and Enhanced Functionality**

**Activities:**

1. Implement auto-renewal for ACM certificates:
   * Use AWS Certificate Manager’s renewal feature for eligible certificates.
   * Develop a Lambda function to monitor and ensure renewal status.
   * Log renewal activities in S3 and CloudWatch.
2. Extend Lambda function for enhanced notification capabilities:
   * Include certificate details (ARN, domain, expiration date) in email notifications.
   * Optimize for scalability and reusability.
3. Customize email notifications.
   * Format emails for clarity and actionability.
   * Include direct links to the ACM console for manual renewal if required.
4. Implement logging and error handling:
   * Ensure all actions (success/failure) are logged in CloudWatch and S3.
   * Handle edge cases like renewal failures or unsupported certificates.
5. Integration testing for Lambda, ACM, and SNS workflows.

**User Stories:**

* As an admin, I want certificates to renew automatically before expiration to reduce manual effort.
* As a developer, I need the Lambda function to handle both notifications and renewal processes.
* As a system, I want to log all actions for traceability and debugging.

**Deliverables:**

* Auto-renewal process for ACM certificates.
* Customized and formatted email notifications.
* CloudWatch and S3-based logging for audit purposes.

**Sprint 17.3: Certificate Swapping and Finalization**

**Activities:**

1. Automate certificate swapping in Load Balancers:
   * Develop a script to identify and replace expired/expiring certificates in ALB/ELB.
   * Verify the replacement process to ensure no downtime.
2. Automate certificate swapping in EC2 instances:
   * Use SSH or Systems Manager to update certificates on EC2 instances.
   * Validate the configuration post-replacement.
3. Delete old certificates after a successful swap:
   * Implement a cleanup process to remove old certificates from ACM.
   * Log deletion activities for auditing.
4. Implement monitoring and metrics:
   * Use CloudWatch to track notification delivery metrics, renewal status, and swapping activities.
   * Set up dashboards for monitoring Lambda execution and SNS message delivery.
5. Document the automation process:
   * Create comprehensive runbooks and operational guides.
   * Include steps for extending or modifying the solution.
6. Conduct user training and knowledge transfer sessions:
   * Train relevant teams on managing and troubleshooting the system.
7. Perform final end-to-end testing.
   * Simulate expiration, renewal, and swapping scenarios to verify all functionalities.
8. Production deployment and validation.
   * Deploy the solution in production and validate with real ACM certificates.

**User Stories:**

* As an admin, I want certificates to be swapped automatically in Load Balancers and EC2 instances to ensure continuous service.
* As a DevOps engineer, I need old certificates to be deleted after successful replacement to maintain a clean environment.
* As an operations team member, I want a dashboard to monitor the automation system.

**Deliverables:**

* Automated certificate swapping in Load Balancers and EC2 instances.
* Cleanup process for old certificates.
* CloudWatch dashboard for monitoring.
* Final documentation and runbooks.
* Knowledge transfer and training sessions.
* Validated production deployment.

**Summary of User Stories Across Sprints**

1. IAM roles and policies for secure resource access.
2. Notification system for expiring certificates using SNS and Lambda.
3. Auto-renewal of ACM certificates.
4. Automated certificate swapping in Load Balancers and EC2 instances.
5. Cleanup of old certificates post-replacement.
6. Comprehensive documentation and operational readiness.

**Custom Email Notifications (SNS + Lambda):**

* **Lambda Implementation:**
  + Triggered by a CloudWatch schedule.
  + Fetch all ACM certificates.
  + Identify certificates expiring in 30, 60, and 90 days.
  + Format email notifications.
  + Publish notifications to SNS.
* **SNS Setup:**
  + Create topics for certificate alerts.
  + Add email subscribers (e.g., operations team).
* **Email Content:**
  + Subject: "Certificate Expiration Alert: "
  + Body:
    - Certificate ARN and domain name.
    - Expiration date.
    - Link to ACM console for renewal.

By following this updated plan, the ACM Certificate Automation effort will cover notifications, auto-renewal, certificate swapping, and cleanup, ensuring a seamless and automated certificate management process.