*How to Set Up an SSL Certificate for your application using AWS Certificate Manager(ACM)*

*Step 1: Prerequisites*

*Before starting, ensure you have the following :*

- *An AWS account with sufficient permissions to manage ACM and related services.*
- *A domain name registered through Rout 53 or any other domain registrar.*

*Step 2: Open AWS Certificate Manager*

1. *Log in to your AWS Management Console.*
2. *Navigate to Certificate Manager:*

- *Search for "Certificate Manager" in the search bar at the top of the console.*
- *Click on Certificate Manager under the Services section.*

*Step 3: Request a Certificate*

1. *Click the Request a certificate button.*
2. *Choose Request a public certificate (recommended for most applications).*
3. *Click Next.*

*Step 4: Specify Domain Names*

1. *Enter the domain name(s) you want the certificate to cover. For example:*
    - *example.com(your root domain)*
    - **.example.com(to include all subdomains like www.example.com or app.example.com).*
2. *Click Next .*

*Step 5: Choose Validation Method*

*AWS ACM requires you to validate ownership of your domain. You can choose one of two methods:*

*Option 1: DNS Validation (Recommended)*

1. *Select DNS validation and click Next.*
2. *AWS will provide a CNAME record that needs to be added to your domain's DNS settings.*

- *If you use Route 53, click Create a record in Route 53 to automatically add the required CNAME record.*
- *If you use another DNS provider, log in to your domain registrar and manually add the provided CNAME record.*

*Option 2: Email Validation*

1. *Select Email validation and click Next.*
2. *AWS will send validation emails to the domain's registered email addresses (e.g., admin@example.com, webmaster@example.com).*
3. *Check your email inbox, find the validation email, and follow the instructions to complete validation.*

*Step 6: Review and Submit*

1. *Review the information you entered :*
    - *Ensure all domain names are correct.*
    - *Confirm the validation method.*

2. *Click Confirm and Request.*

*Step 7: Validate the Domain*

*Depending on the validation method you  choose :*

- *For DNS validation, wait for the DNS changes to propagate(usually within a few minutes to a few hours).*
- *For Email Validation, click the link in the validation email to confirm ownership.*

*Once the validation is complete, the certificate's status will change to issue in ACM.*

*Step 8: Use the SSL Certificate*

*After the certificate is issued, you can associate it with your application. The steps vary depending on the service you use:*

***Option 1: For AWS Load Balancers (ALB/ELB)***

1. *Navigate to the **EC2** service and select **Load Balancers**.*
2. *Choose the load balancer you want to attach the certificate to.*
3. *Edit the **Listener** settings:*
    - *Add an HTTPS listener if one does not exist.*
    - *Select your ACM certificate from the drop-down menu.*
    - *Save the changes.*

***Option 2: For CloudFront Distributions***

1. *Navigate to the **CloudFront** service.*
2. *Choose the distribution you want to secure.*
3. *Edit the distribution's settings and select your ACM certificate under the **SSL Certificate** section.*
4. *Save the changes.*

***Option 3: For Other Services (e.g., API Gateway, Elastic Beanstalk)***

*Follow the specific service documentation to associate the SSL certificate with your application.*

## *Step 9: Test Your Application*

1. *Access your application via the HTTPS protocol (e.g., `https://example.com`).*
2. *Verify that the SSL certificate is active and the browser shows a secure connection.*