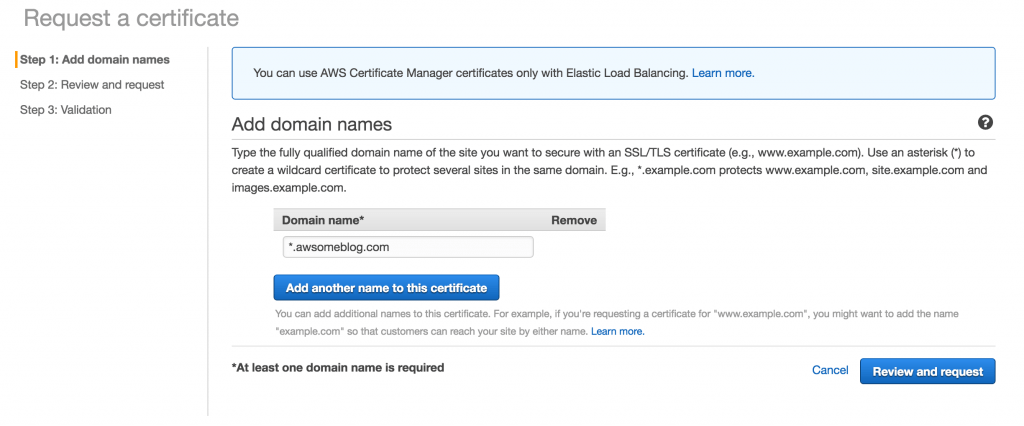
**AWS Certificate Manager**

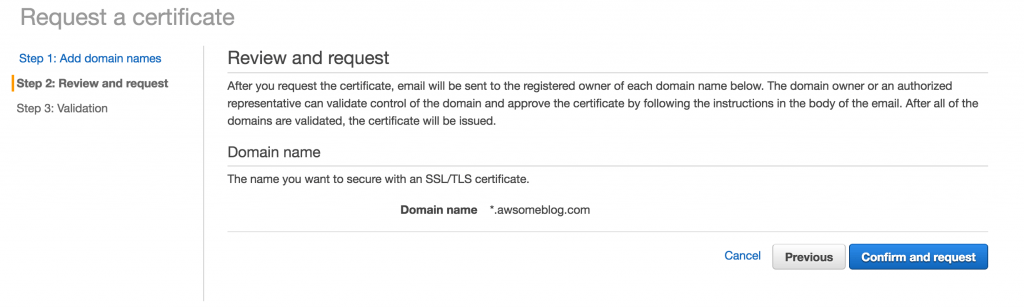
This week I will talk about AWS Certificate Manager, a simple service for our applications running on top of AWS. It is AWS-based because it only supports AWS ELB and Cloudfront. ACM helps us to request and manage our certificates easily ( for instance, it renews our certificates automatically) with some limitations ( the certificates are valid for 13 months, and some other [exceptions](http://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html) ).

Today I will request a certificate for my blog and configure it step by step. So let’s start…

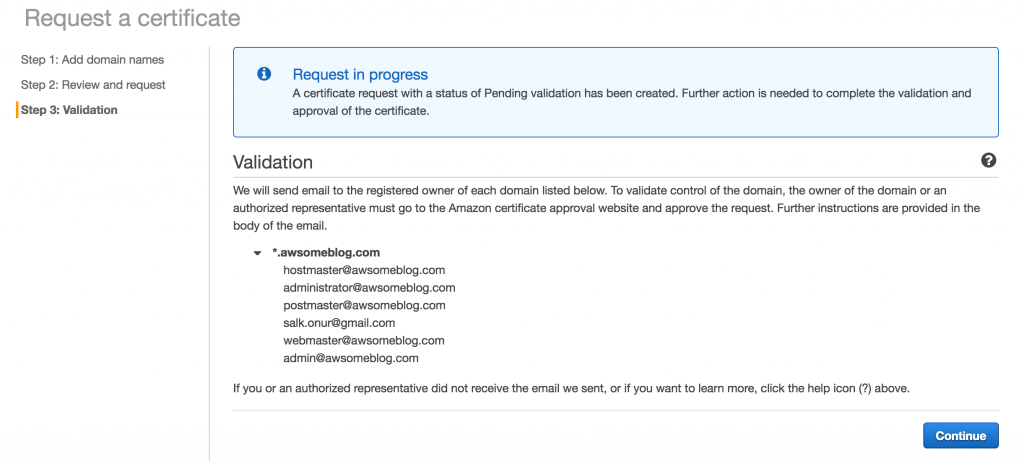
First, I request my certificate using ACM console. I add my domain name.



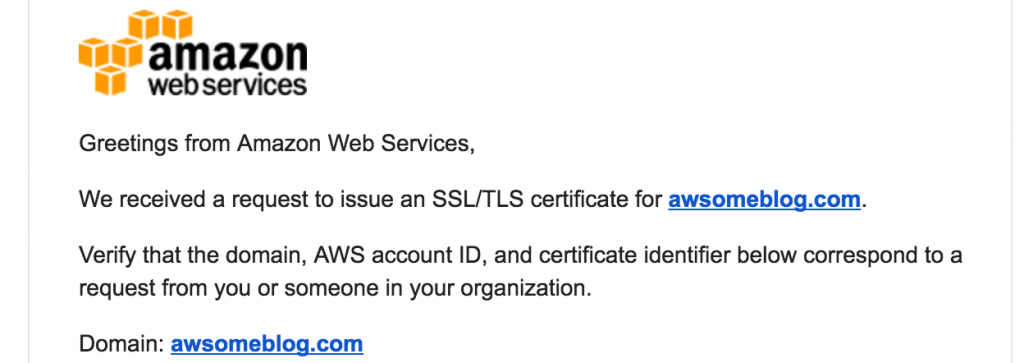
I review and confirm my request.



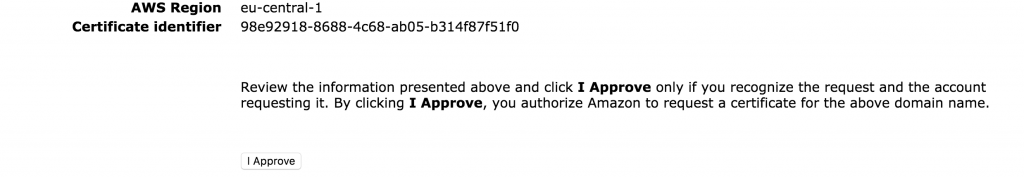
AWS automatically sends an email to verify the owner of the domain.



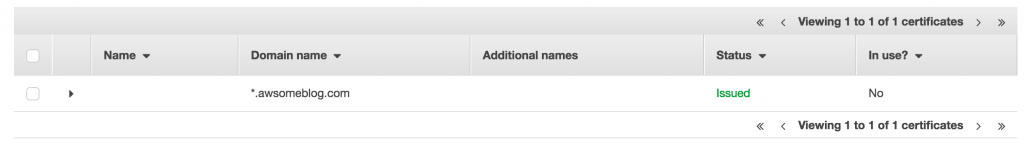
And I check the if the email has arrived.



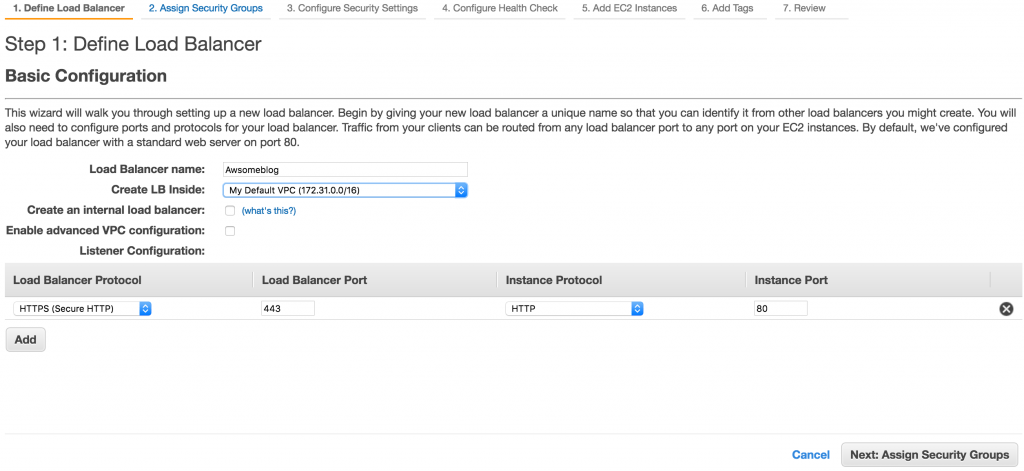
I approve and authorize AWS to request a certificate for my domain.



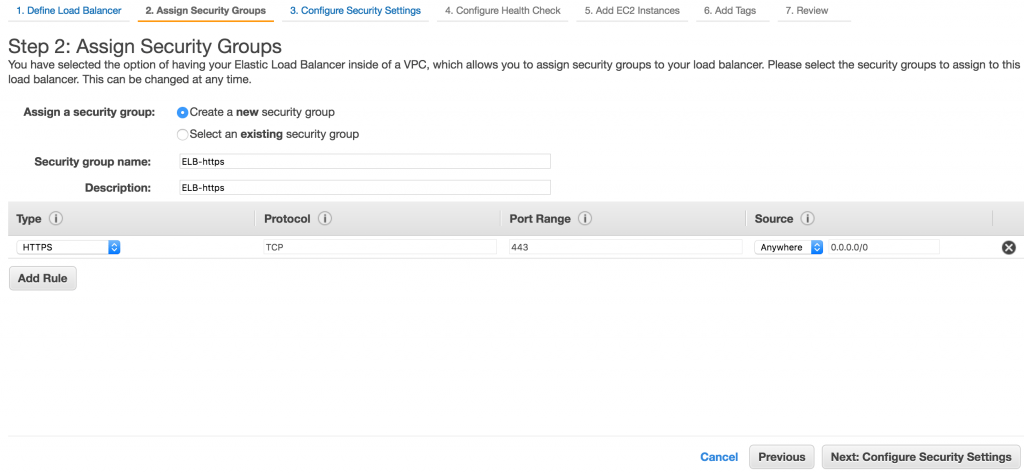
Finally my certificate is issued. ( After that I also issued another certificate for awsomeblog.com and www.awsomeblog.com )



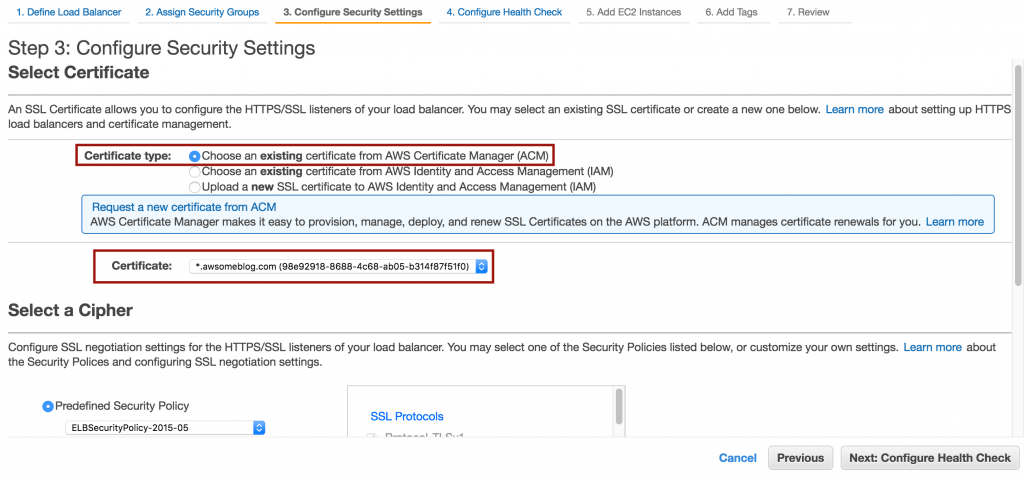
My next step is creating an ELB for my blog. I configure HTTPS for listener.



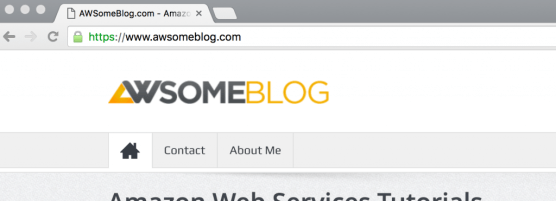
I create a security group that listens on port 443.



For the last step, I select “Choose an existing certificate from AWS Certificate manager” as certificate type and select my issued certificate.



As soon as my instance pass the health check of ELB, my blog is started to serve on HTTPS. ( I also need to configure wordpress, nginx etc settings on my server but this is not related to AWS )



As you see, requesting a certificate via ACM and configuring the ELB is very easy. I hope you find it useful. If you have any questions or comments, please feel free to write and don’t forget to share this post please.