AWS - Certificate Manager (ACM)

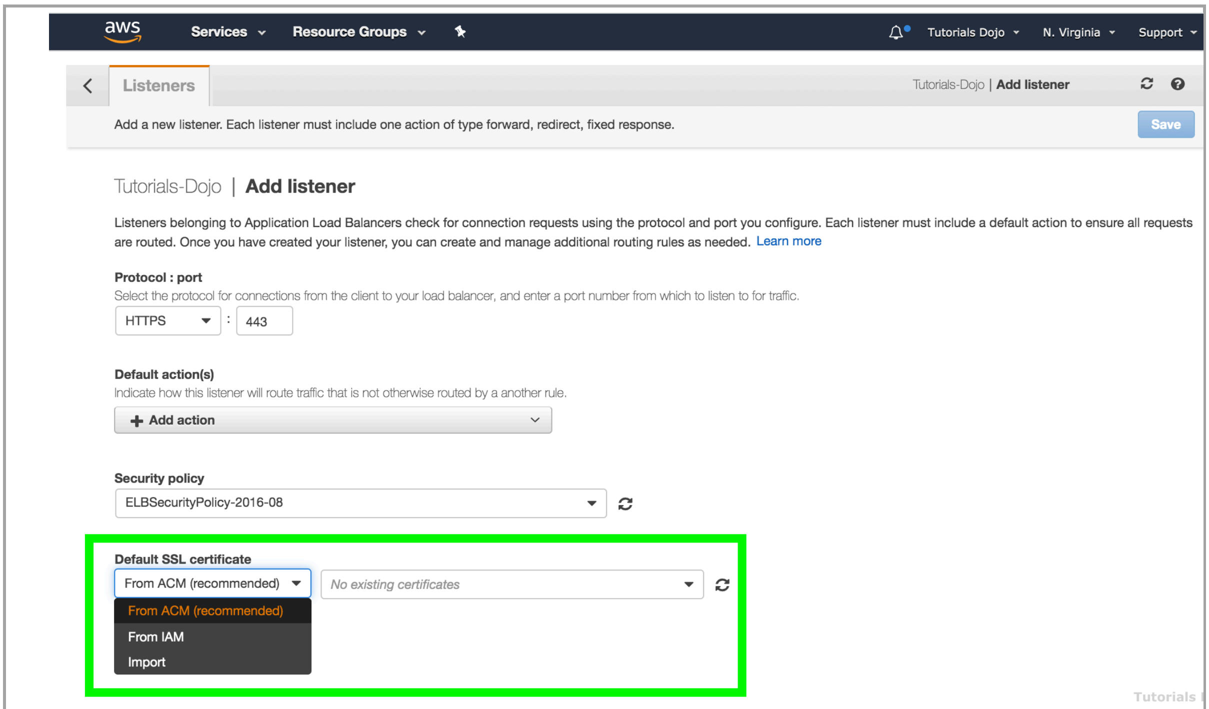
If you got your certificate from a third-party CA,

- import the certificate into ACM or
- upload it to the IAM certificate store.

Hence, **AWS Certificate Manager** and **IAM certificate store** are the correct answers.

AWS Certificate Manager

- AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.
- SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.
- AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.
- With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACM-integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals.
- It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally.
- **Public SSL/TLS certificates** provisioned through AWS Certificate Manager are free. You pay only for the AWS resources that you create to run your application.
- **For Private SSL/TLS certificates,** the ACM Private Certificate Authority (CA) is priced along two dimensions:
  - (1) You pay a monthly fee for the operation of each private CA until you delete it and
  - (2) you pay for the private certificates you issue each month.
- Public certificates generated from ACM can be used on
  - Amazon CloudFront,
  - Elastic Load Balancing, or
  - Amazon API Gateway
  - but not directly on EC2 instances, unlike private certificates.



Add a new listener. Each listener must include one action of type forward, redirect, fixed response.

Tutorials-Dojo | **Add listener**

Listeners belonging to Application Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. Once you have created your listener, you can create and manage additional routing rules as needed. Learn more

Protocol : port

Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen to for traffic.

HTTPS : 443

Default action(s)

Indicate how this listener will route traffic that is not otherwise routed by a another rule.

+ Add action

Security policy

ELBSecurityPolicy-2016-08

Default SSL certificate

From ACM (recommended) — No existing certificates

From ACM (recommended)
From IAM
Import

ACM Certificates : Elastic Load Balancing vs CloudFront

You can use the same SSL certificate from ACM in more than one AWS Region but it depends on whether you're using Elastic Load Balancing or Amazon CloudFront.

Elastic Load Balancing:

- To use a certificate with Elastic Load Balancing for the same site (the same fully qualified domain name, or FQDN, or set of FQDNs) in a different Region, you must request a new certificate for each Region in which you plan to use it.

CloudFront:

- To use an ACM certificate with Amazon CloudFront, you must request the certificate in the US East (N. Virginia) region.
- ACM certificates in this region that are associated with a CloudFront distribution are distributed to all the geographic locations configured for that distribution.

Hence, the correct answer is the option that says: **In each new AWS Region, request for SSL/TLS certificates using the AWS Certificate Manager for each FQDN. Associate the new certificates to the corresponding Application Load Balancer of the same AWS Region.**

Benefits

Free public certificates for ACM-integrated services

With AWS Certificate Manager, there is no additional charge for provisioning public or private SSL/TLS certificates you use with ACM-integrated services, such as Elastic Load Balancing and API Gateway. You pay for the AWS resources you create to run your application. For private certificates, ACM Private CA provides you the ability to pay monthly for the service and certificates you create. You pay less per certificate as you create more private certificates.

Managed certificate renewal

AWS Certificate Manager manages the renewal process for the certificates managed in ACM and used with ACM-integrated services, such as Elastic Load Balancing and API Gateway. ACM can automate renewal and deployment of these certificates. With ACM Private CA APIs, ACM enables you to automate creation and renewal of private certificates for on-premises resources, EC2 instances, and IoT devices.

IAM Certificate Store

- To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS *server certificate*.
- For certificates in a Region supported by AWS Certificate Manager (ACM), we recommend that you use ACM to provision, manage, and deploy your server certificates.
- In unsupported Regions, you must use IAM as a certificate manager.

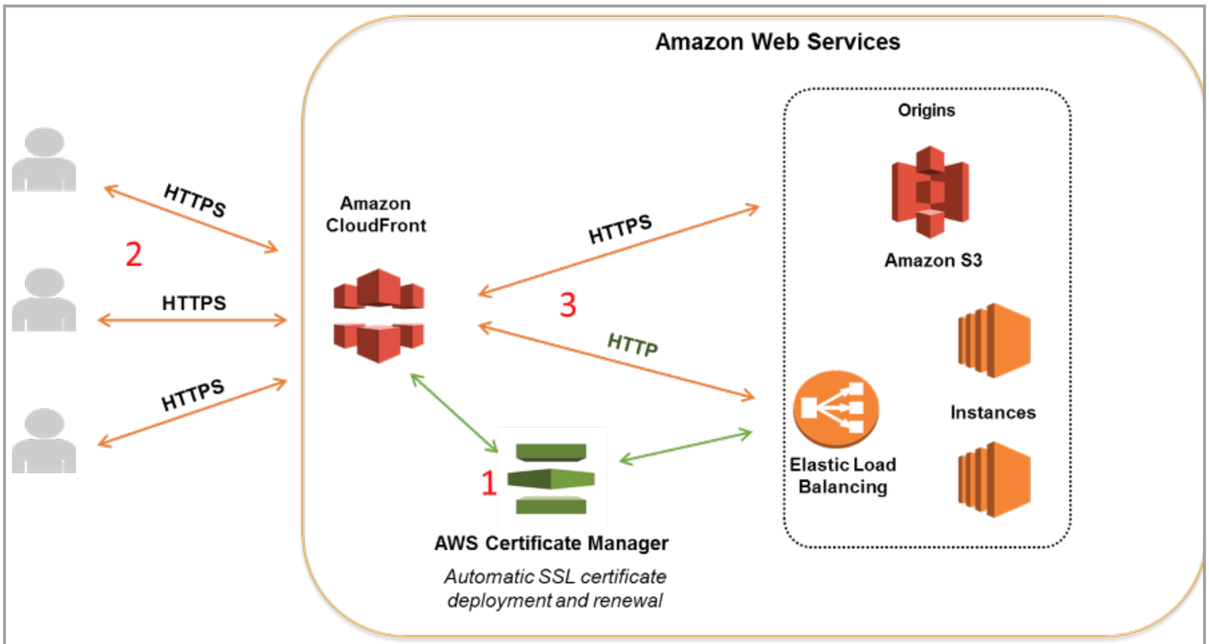
```
aws iam upload-server-certificate --server-certificate-name ExampleCertificate
                          --certificate-body file://Certificate.pem
                          --certificate-chain file://CertificateChain.pem
                          --private-key file://PrivateKey.pem
```

```
aws iam get-server-certificate --server-certificate-name ExampleCertificate
```

```
aws iam list-server-certificates
```

```
aws iam update-server-certificate --server-certificate-name ExampleCertificate
                          --new-server-certificate-name CloudFrontCertificate
                          --new-path /cloudfront/
```

```
aws iam delete-server-certificate --server-certificate-name ExampleCertificate
```



- ACM lets you import third-party certificates from the ACM console, as well as programmatically.
- If ACM is not available in your region, use AWS CLI to upload your third-party certificate to the IAM certificate store.

Reference:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html#cnames-and-https-uploading-certificates

Check out this Amazon CloudFront Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-amazon-cloudfront/

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

https://tutorialsdojo.com/aws-cheat-sheet-aws-certified-solutions-architect-associate/

References:

https://aws.amazon.com/certificate-manager/faqs/

https://aws.amazon.com/certificate-manager/