**AWS ACM Interview Questions and Answers**

**Question:** What is AWS ACM?

**Answer:** AWS ACM is a service provided by Amazon Web Services that enables the provisioning, management, and deployment of SSL/TLS (Secure Sockets Layer/Transport Layer Security) certiﬁcates for use with AWS services and other external resources.

**Question:** What are the beneﬁts of using AWS ACM?

**Answer:** Some beneﬁts of using AWS ACM include:

* Simpliﬁed certiﬁcate management: ACM automates the process of certiﬁcate provisioning, renewal, and deployment, reducing manual effort and eliminating the need to manage certiﬁcates manually.
* Integration with AWS services: ACM seamlessly integrates with various AWS services, such as Elastic Load Balancing, Amazon CloudFront, and AWS Elastic Beanstalk, making it easier to deploy certiﬁcates for secure communication.
* Managed certiﬁcate renewals: ACM automatically handles certiﬁcate renewals, ensuring that certiﬁcates are always up to date and eliminating the risk of expired certiﬁcates.
* Highly available and scalable infrastructure: ACM's infrastructure is designed for high availability and scalability, ensuring reliable certiﬁcate management and deployment across AWS regions.
* Cost-effective: ACM is a free service, and you only pay for the AWS resources you use, such as load balancers or CloudFront distributions.

**Question:** How do you request a certiﬁcate using AWS ACM?

**Answer:** To request a certiﬁcate using AWS ACM, you need to follow these steps:

* Open the AWS Management Console and navigate to the ACM service.
* Click on "Request a certiﬁcate."
* Specify the domain names or subdomains for which you want to request a certiﬁcate.
* Choose a validation method: DNS validation or email validation.
* Conﬁgure the settings for the certiﬁcate, such as the key algorithm and the certiﬁcate options.
* Review and conﬁrm the request.
* Complete the validation process by following the provided instructions for DNS or email validation.

**Question:** How does AWS ACM handle certiﬁcate renewals?

**Answer:** AWS ACM automatically handles certiﬁcate renewals for you. When a certiﬁcate managed by ACM approaches its expiration date, ACM automatically renews it. You don't need to take any action for the renewal process. ACM replaces the expiring certiﬁcate with a new one and updates the associated resources, such as Elastic Load Balancers or

CloudFront distributions, with the new certiﬁcate.

**Question** 5: Can you import third-party certiﬁcates into AWS ACM?

**Answer:** No, AWS ACM only manages certiﬁcates that are issued by ACM itself or certiﬁcates that are provisioned through the ACM Private CA service. You cannot import third-party certiﬁcates into ACM. However, you can use

ACM-imported certiﬁcates with other AWS services such as CloudFront, but they will not beneﬁt from the automatic renewal and management features provided by ACM.

**Question** 6: How can you associate an ACM certiﬁcate with an AWS resource?

**Answer:** To associate an ACM certiﬁcate with an AWS resource, you can follow these steps:

* Open the AWS Management Console and navigate to the resource you want to associate the certiﬁcate with, such as an Elastic Load Balancer or CloudFront distribution.
* In the resource settings, look for the SSL/TLS conﬁguration or SSL certiﬁcate options.
* Select the ACM certiﬁcate you want to use from the list of available certiﬁcates.
* Save the conﬁguration changes.
* The resource will now use the selected ACM certiﬁcate for secure communication.

**Question** 7: Can you use ACM certiﬁcates outside of AWS?

**Answer:** Yes, you can export ACM certiﬁcates and use them outside of AWS. However, note that once you export an ACM certiﬁcate, it is no longer managed by ACM. You need to manually handle the certiﬁcate renewal and deployment

processes. Additionally, exported ACM certiﬁcates can only be used with services that support importing and using certiﬁcates from external sources.

**Question** 9: Can ACM certiﬁcates be used for both public and private resources?

**Answer:** Yes, ACM certiﬁcates can be used for both public and private resources. Public certiﬁcates can be used for resources that are publicly accessible over the internet, such as websites or APIs. Private certiﬁcates can be used for resources that are internal to your network, such as internal load balancers or private APIs.

**Question:** What is the difference between ACM's managed renewal and private CA certiﬁcates?

**Answer:** ACM's managed renewal certiﬁcates are automatically renewed by ACM, while private CA certiﬁcates are issued by your own private certiﬁcate authority (CA) and require manual renewal. ACM's managed renewal certiﬁcates are suitable for most use cases and offer convenient automated renewal, while private CA certiﬁcates provide more control and ﬂexibility for organizations that want to manage their own certiﬁcate lifecycle.

**Question:** Can ACM certiﬁcates be used outside of AWS's infrastructure?

**Answer:** No, ACM certiﬁcates are primarily designed to be used within AWS's infrastructure. They are optimized for use with AWS services, such as Elastic Load Balancing and CloudFront. However, you can export ACM certiﬁcates and use them in some external services that support importing SSL/TLS certiﬁcates.

**Question:** Can ACM certiﬁcates be used with non-AWS resources?

**Answer:** Yes, ACM certiﬁcates can be used with non-AWS resources, but they need to be exported ﬁrst. You can export an ACM certiﬁcate and use it with external resources, such as servers hosted outside of AWS or with third-party services that support SSL/TLS certiﬁcates. However, note that once exported, the certiﬁcate will no longer beneﬁt from ACM's automatic renewal and management capabilities.

**Question:** What happens if an ACM certiﬁcate fails the automated renewal process?

**Answer:** If an ACM certiﬁcate fails the automated renewal process, ACM sends a notiﬁcation to the registered owner of the certiﬁcate. The owner can then take appropriate action to manually renew the certiﬁcate or investigate the reason for

the failure. It's important to ensure that the registered owner's contact information is up to date in order to receive renewal notiﬁcations.

**Question:** Can ACM manage wildcard certiﬁcates?

**Answer:** Yes, ACM can manage wildcard certiﬁcates, which allow you to secure multiple subdomains under a single domain with a single certiﬁcate. You can request a wildcard certiﬁcate by specifying "\*.example.com" as the domain name during the certiﬁcate request process. ACM will issue a certiﬁcate that covers all subdomains of "example.com" in a wildcard pattern.

**Question:** How does ACM handle the validation process for certiﬁcate issuance?

**Answer:** ACM offers two validation methods for certiﬁcate issuance: DNS validation and email validation. DNS validation requires you to add speciﬁc DNS records to your domain's DNS conﬁguration, while email validation involves sending validation emails to the domain owner or speciﬁc email addresses associated with the domain. The validation process

ensures that you have control over the domain for which you are requesting a certiﬁcate.

**Question:** Can ACM certiﬁcates be used in a multi-region architecture?

**Answer:** Yes, ACM certiﬁcates can be used in a multi-region architecture. ACM provides certiﬁcate availability in multiple AWS regions, allowing you to provision and manage certiﬁcates in each region independently. This enables you to deploy and manage certiﬁcates consistently across multiple regions to support global applications and architectures.

**Question:** Can ACM certiﬁcates be used with on-premises resources?

**Answer:** No, ACM certiﬁcates cannot be directly used with on-premises resources. ACM is designed for managing

certiﬁcates within the AWS ecosystem. However, you can export an ACM certiﬁcate and use it with on-premises resources if they support importing SSL/TLS certiﬁcates.

**Question:** Can I use AWS ACM certiﬁcates with an Amazon S3 bucket?

**Answer:** No, AWS ACM certiﬁcates cannot be directly used with Amazon S3 buckets. ACM certiﬁcates are primarily designed for use with AWS services like Elastic Load Balancing, CloudFront, and API Gateway. However, you can use a custom domain with CloudFront and associate an ACM certiﬁcate with it to provide secure access to your Amazon S3

content.

**Question:** How does ACM manage the private keys associated with the certiﬁcates?

**Answer:** ACM does not provide direct access to the private keys associated with the certiﬁcates it manages. The private keys are securely stored and managed by AWS Key Management Service (KMS). ACM takes care of the certiﬁcate

provisioning and renewal processes, while KMS handles the secure storage and management of the private keys.

**Question:** Can I import my existing SSL/TLS certiﬁcates into AWS ACM?

**Answer:** No, AWS ACM does not support importing existing SSL/TLS certiﬁcates. ACM manages its own certiﬁcates or certiﬁcates issued by the ACM Private CA service. If you have existing certiﬁcates from another provider, you would need to request new certiﬁcates through ACM or ACM Private CA.

**Question:** Can I use ACM certiﬁcates with AWS Lambda functions?

**Answer:** ACM certiﬁcates cannot be directly associated with AWS Lambda functions. However, you can use API Gateway in front of your Lambda functions and associate an ACM certiﬁcate with the custom domain in API Gateway. This way, the request from the client to the Lambda function will be secured using the ACM certiﬁcate.

**Question:** Can I use ACM certiﬁcates with AWS CloudFormation?

**Answer:** Yes, you can use ACM certiﬁcates with AWS CloudFormation. You can deﬁne an

AWS::CertiﬁcateManager::Certiﬁcate resource in your CloudFormation template to request an ACM certiﬁcate. This allows you to automate the provisioning of ACM certiﬁcates along with your other AWS resources in a CloudFormation stack.

**Question:** Can I share ACM certiﬁcates across AWS accounts?

**Answer:** No, ACM certiﬁcates cannot be shared across AWS accounts. ACM certiﬁcates are speciﬁc to the AWS account in which they are created. If you need to use an ACM certiﬁcate in another AWS account, you would need to request a new

certiﬁcate in that account or consider exporting the certiﬁcate and using it in the target account.

**Question:** Can ACM certiﬁcates be used for client-side encryption?

**Answer:** No, ACM certiﬁcates are primarily designed for server-side encryption, such as securing web servers, load

balancers, or content delivery networks. For client-side encryption scenarios, such as encrypting data before uploading it to S3, you would typically use AWS Key Management Service (KMS) for managing encryption keys.

**Question:** Can ACM certiﬁcates be used for code signing?

**Answer:** No, ACM certiﬁcates cannot be used for code signing. ACM certiﬁcates are speciﬁcally intended for securing network communication between servers and clients. For code signing purposes, you would need to use a different type of certiﬁcate, such as those provided by a certiﬁcate authority specialized in code signing.

**Question:** How does ACM handle certiﬁcate revocation?

**Answer:** ACM does not provide a direct certiﬁcate revocation mechanism. Instead, ACM focuses on automated certiﬁcate renewal to ensure that certiﬁcates remain valid and up to date. If a certiﬁcate needs to be revoked, you would typically handle it through the certiﬁcate authority or provider that issued the certiﬁcate.

**Question:** Can ACM certiﬁcates be used with self-managed infrastructure?

**Answer:** No, ACM certiﬁcates are designed to be used with AWS services and cannot be directly used with self-managed infrastructure. However, you can export an ACM certiﬁcate and manually conﬁgure it for use with your self-managed infrastructure if it supports importing SSL/TLS certiﬁcates.

**Question:** Can I request a wildcard certiﬁcate for multiple levels of subdomains with ACM?

**Answer:** No, ACM does not support requesting wildcard certiﬁcates for multiple levels of subdomains. ACM wildcard certiﬁcates only cover a single level of subdomains. If you need to secure multiple levels of subdomains, you would need

to request separate wildcard certiﬁcates for each level.

**Question:** How does ACM handle certiﬁcate expiration notiﬁcations?

**Answer:** ACM sends expiration notiﬁcations to the registered owners of certiﬁcates via email. The notiﬁcations are sent to the email addresses associated with the AWS account that requested the certiﬁcate. It's essential to ensure that the registered owner's email addresses are up to date to receive timely expiration notiﬁcations.

**Question:** Can I use ACM certiﬁcates with AWS Elastic Beanstalk?

**Answer:** Yes, you can use ACM certiﬁcates with AWS Elastic Beanstalk. When conﬁguring your Elastic Beanstalk

environment, you can associate an ACM certiﬁcate with the custom domain of your application. This ensures secure communication between your application and the users accessing it.

**Question:** Can ACM certiﬁcates be used with CloudFormation stack sets?

**Answer:** Yes, you can use ACM certiﬁcates with CloudFormation stack sets. Stack sets allow you to create, update, or delete CloudFormation stacks across multiple accounts and regions. When deﬁning the CloudFormation template for a stack set, you can include an ACM certiﬁcate resource to provision a certiﬁcate in each targeted account and region.

**Question:** What happens to ACM certiﬁcates when deleting an AWS account?

**Answer:** When you delete an AWS account, the associated ACM certiﬁcates are also deleted. It's important to make sure that you have backups or copies of any essential certiﬁcates before deleting an AWS account to avoid data loss or disruption to your services.

**Question:** Can ACM manage certiﬁcates for wildcard domains?

**Answer:** Yes, ACM can manage certiﬁcates for wildcard domains. You can request a wildcard certiﬁcate by specifying "\*.example.com" as the domain name during the certiﬁcate request. ACM will issue a certiﬁcate that covers all

subdomains of "example.com" in a wildcard pattern.

**Question:** Can I request a certiﬁcate from ACM for an IP address instead of a domain name?

**Answer:** No, ACM only issues certiﬁcates for domain names and not IP addresses. Certiﬁcates issued by ACM require a domain name validation process to ensure the requester has control over the domain for which the certiﬁcate is being issued.

**Question:** How does ACM ensure the security and privacy of certiﬁcates?

**Answer:** ACM ensures the security and privacy of certiﬁcates by encrypting the private keys using AWS Key Management Service (KMS). ACM also implements robust security measures to protect the conﬁdentiality and integrity of certiﬁcate data, following industry best practices and compliance standards.

**Question:** You are setting up a web application on AWS and need to secure it with an SSL/TLS certiﬁcate. Which service can you use to provision and manage the SSL/TLS certiﬁcate automatically?

**Answer:** You can use AWS ACM (Amazon Certiﬁcate Manager) to provision and manage the SSL/TLS certiﬁcate automatically. ACM integrates with various AWS services like Elastic Load Balancing, CloudFront, and API Gateway to simplify the process of deploying and managing certiﬁcates.

**Question:** You have a highly available web application deployed across multiple AWS regions. How can you ensure consistent SSL/TLS certiﬁcate management across all regions?

**Answer:** You can leverage ACM's multi-region support to ensure consistent SSL/TLS certiﬁcate management across multiple AWS regions. ACM provides certiﬁcate availability in multiple regions, allowing you to provision and manage certiﬁcates in each region independently while ensuring consistent security across your application's global architecture.

**Question:** Your organization operates a private certiﬁcate authority (CA) and wants to use its own certiﬁcates for securing applications on AWS. How can you integrate your private CA with AWS services?

**Answer:** You can use ACM Private CA to integrate your private CA with AWS services. ACM Private CA allows you to operate a private CA within AWS and issue private certiﬁcates for use within your organization. You can then import these certiﬁcates into ACM and use them with AWS services like Elastic Load Balancing, CloudFront, or API Gateway.

**Question:** You have a web application running on EC2 instances behind an Elastic Load Balancer (ELB). How can you secure the communication between the ELB and the EC2 instances using ACM?

**Answer:** You can secure the communication between the ELB and the EC2 instances using ACM by requesting an SSL/TLS certiﬁcate from ACM and associating it with the ELB. ACM will automatically provision and manage the certiﬁcate, ensuring secure communication between the ELB and the EC2 instances.

**Question:** Your organization has a requirement to rotate SSL/TLS certiﬁcates periodically. How can you achieve automated certiﬁcate rotation with ACM?

**Answer:** ACM automatically handles the certiﬁcate renewal process, ensuring that certiﬁcates are automatically rotated. ACM manages the certiﬁcate lifecycle, including the renewal process, eliminating the need for manual intervention in certiﬁcate rotation.

**Question:** You have a web application hosted on CloudFront that needs to support multiple subdomains. How can you obtain a wildcard certiﬁcate for all subdomains using ACM?

**Answer:** To obtain a wildcard certiﬁcate for all subdomains using ACM, you can request a wildcard certiﬁcate by specifying "\*.example.com" as the domain name during the certiﬁcate request process. ACM will issue a certiﬁcate that covers all subdomains of "example.com" in a wildcard pattern.

**Question:** Your company is launching a new API that needs to be secured with SSL/TLS encryption. How can you conﬁgure API Gateway to use ACM certiﬁcates?

**Answer:** You can conﬁgure API Gateway to use ACM certiﬁcates by associating an ACM certiﬁcate with a custom domain name in API Gateway. This ensures that API Gateway uses the ACM certiﬁcate for SSL/TLS encryption when serving

requests to the API.

**Question:** Your organization is migrating an on-premises web application to AWS. The application currently uses an SSL/TLS certiﬁcate from a third-party CA. How can you migrate and manage the certiﬁcate using ACM?

**Answer:** ACM does not support importing existing SSL/TLS certiﬁcates. In this case, you can request a new certiﬁcate from ACM and conﬁgure it for use with your migrated web application. It's important to plan the migration process carefully to minimize any disruption during the transition to the new ACM certiﬁcate.

**Question:** You have a web application hosted on an EC2 instance running in a VPC (Virtual Private Cloud). How can you secure the communication between the client and the EC2 instance using ACM?

**Answer:** ACM does not directly secure communication between the client and an EC2 instance. However, you can use other AWS services like Elastic Load Balancer or CloudFront in front of your EC2 instances. You can associate an ACM certiﬁcate with the load balancer or CloudFront distribution to enable secure communication between the client and the EC2 instance.

**Question:** You have a serverless application built with AWS Lambda functions and exposed through an API Gateway. How can you secure the API Gateway endpoint using ACM?

**Answer:** To secure the API Gateway endpoint using ACM, you can associate an ACM certiﬁcate with a custom domain name in API Gateway. This ensures that the API Gateway endpoint is served over HTTPS using the ACM certiﬁcate,

providing secure communication between the client and the API Gateway.

**Question:** Your organization wants to implement a multi-tier architecture for a scalable web application. How can you manage SSL/TLS certiﬁcates across different tiers using ACM?

**Answer:** ACM certiﬁcates can be managed separately for each tier of the architecture. You can provision ACM certiﬁcates for each tier, such as load balancers, web servers, and microservices. ACM will handle the certiﬁcate renewal and management automatically for each tier, ensuring secure communication between the components.

**Question:** You are building a global website with traﬃc distributed across multiple regions. How can you ensure consistent SSL/TLS certiﬁcate management for all regions using ACM?

**Answer:** ACM offers a global infrastructure that enables consistent SSL/TLS certiﬁcate management across multiple

regions. By provisioning ACM certiﬁcates in each region where your website operates, you can ensure consistent security across all regions while beneﬁting from ACM's automatic certiﬁcate renewal and management.

**Question:** Your application requires client-side SSL/TLS authentication to verify the identity of the clients. Can you use ACM for client-side SSL/TLS authentication?

**Answer:** No, ACM does not support client-side SSL/TLS authentication. ACM is primarily designed for server-side

SSL/TLS certiﬁcate management. For client-side authentication, you would typically use other mechanisms such as AWS Cognito or a custom authentication solution.

**Question:** Your organization has a requirement to secure communication between internal services running on EC2 instances. Can you use ACM for securing internal service-to-service communication?

**Answer:** ACM is primarily designed for securing communication between clients and AWS services, such as load

balancers and API Gateway. For securing internal service-to-service communication on EC2 instances, you can use other mechanisms such as self-signed certiﬁcates, OpenSSL, or third-party certiﬁcate authorities.

**Question:** You are deploying a containerized application on AWS using Amazon Elastic Container Service (ECS). How can you secure the communication between the load balancer and the containers using ACM?

**Answer:** You can secure the communication between the load balancer and the containers in Amazon ECS by associating an ACM certiﬁcate with the load balancer. ACM will automatically handle the certiﬁcate provisioning and renewal,

ensuring secure communication between the load balancer and the ECS containers.

**Question:** Your organization is using AWS CloudFormation to manage the infrastructure as code. How can you include ACM certiﬁcates in your CloudFormation templates?

**Answer:** In CloudFormation templates, you can deﬁne an AWS::CertiﬁcateManager::Certiﬁcate resource to request an ACM certiﬁcate. This allows you to automate the provisioning of ACM certiﬁcates as part of your infrastructure deployment using CloudFormation.

**Question:** Your organization is planning to deploy a web application on AWS that requires SSL/TLS encryption. How can you ensure that the ACM certiﬁcate is automatically renewed before it expires?

**Answer:** ACM takes care of certiﬁcate renewal automatically. It monitors the expiration date of certiﬁcates and initiates

the renewal process in advance. You don't have to manually renew the certiﬁcates or worry about their expiration, as ACM handles it seamlessly for you.

**Question:** You have an application load balancer (ALB) distributing traﬃc to multiple EC2 instances. Can you use a single ACM certiﬁcate for multiple ALBs in different regions?

**Answer:** ACM certiﬁcates are region-speciﬁc. If you have ALBs in different regions, you'll need to request separate ACM certiﬁcates for each region. However, ACM makes it easy to manage and renew these certiﬁcates centrally, ensuring consistent security across your distributed application.

**Question:** Your organization is using Amazon CloudFront to deliver content globally. How can you associate an ACM certiﬁcate with your CloudFront distribution?

**Answer:** To associate an ACM certiﬁcate with your CloudFront distribution, you can request an ACM certiﬁcate and specify the domain name(s) you want to secure. Once the certiﬁcate is issued, you can select it as the custom SSL

certiﬁcate for your CloudFront distribution. CloudFront will automatically handle the SSL/TLS termination using the ACM certiﬁcate.

**Question:** You are migrating an existing application to AWS that currently uses a certiﬁcate from another certiﬁcate authority (CA). Can you import the existing certiﬁcate into ACM?

**Answer:** ACM does not support importing existing certiﬁcates. If you have an existing certiﬁcate from another CA, you'll

need to request a new certiﬁcate from ACM. However, you can import an ACM certiﬁcate to other AWS services like Elastic Load Balancing, CloudFront, or API Gateway.

**Question:** Your organization has a requirement to store and manage private keys separately from ACM. Is it possible to export private keys from ACM?

**Answer:** No, ACM does not provide an option to export private keys. ACM manages the private keys securely within the AWS infrastructure and allows you to use the certiﬁcates with supported AWS services. If you need direct access to

private keys, you may consider using other certiﬁcate management solutions.

**Question:** Your application is using AWS Elastic Beanstalk for deployment. Can you use ACM certiﬁcates with Elastic Beanstalk?

**Answer:** Yes, you can use ACM certiﬁcates with Elastic Beanstalk. When conﬁguring your Elastic Beanstalk environment, you can associate an ACM certiﬁcate with the custom domain name of your application. Elastic Beanstalk will automatically deploy and manage the certiﬁcate for secure communication.

**Question:** Your organization wants to implement a strict security policy that requires certiﬁcates to have a minimum key length. Can you specify the key length for ACM certiﬁcates?

**Answer:** ACM automatically generates the private key and the corresponding public key for the certiﬁcates it issues. You cannot specify the key length directly through ACM. However, ACM uses industry-standard encryption algorithms and

ensures robust security for the certiﬁcates it manages.

**Question:** Your application needs to support older web browsers that do not support the latest encryption standards. Can you choose the encryption algorithm and compatibility settings for ACM certiﬁcates?

**Answer:** ACM uses industry-standard encryption algorithms and conﬁgurations by default. The supported encryption algorithms and compatibility settings are automatically determined based on industry best practices and browser compatibility. ACM ensures that the certiﬁcates it issues are compatible with a wide range of web browsers.

**Question:** Your organization wants to enable HTTP to HTTPS redirection for your website. Can you conﬁgure this redirection using ACM?

**Answer:** ACM does not provide built-in functionality for HTTP to HTTPS redirection. To enable HTTP to HTTPS redirection, you would typically conﬁgure this at the web server level or use services like Amazon CloudFront or Elastic Load Balancing to handle the redirection.

**Question:** Your application is using multiple subdomains for different functionalities. How can you obtain separate ACM certiﬁcates for each subdomain?

**Answer:** You can request individual ACM certiﬁcates for each subdomain by specifying the subdomain as the domain name during the certiﬁcate request process. ACM allows you to manage multiple certiﬁcates, making it easy to secure and manage certiﬁcates for each subdomain separately.

**Question:** Your organization wants to implement a custom domain for the AWS Management Console using ACM. Is this possible?

**Answer:** No, ACM is not designed to secure the AWS Management Console or other AWS services directly. ACM is

primarily used to secure applications running on AWS infrastructure. To secure the AWS Management Console, you would typically use other methods such as AWS Identity and Access Management (IAM) and secure access policies.

**Question:** You have an existing application hosted on an EC2 instance, and you want to secure it using an ACM certiﬁcate. How can you associate an ACM certiﬁcate with the EC2 instance?

**Answer:** ACM certiﬁcates cannot be directly associated with individual EC2 instances. ACM is designed to work with AWS services like Elastic Load Balancing, CloudFront, and API Gateway. To secure an application hosted on an EC2 instance, you would typically use other methods such as manually installing an SSL/TLS certiﬁcate on the web server running on

the EC2 instance.

**Question:** Your organization wants to automate the issuance and renewal of certiﬁcates for its infrastructure. Can you programmatically interact with ACM?

**Answer:** Yes, you can programmatically interact with ACM using the AWS SDKs, AWS CLI, or AWS APIs. You can automate the certiﬁcate issuance and renewal process, as well as perform other operations such as listing certiﬁcates, requesting certiﬁcate validation, and managing certiﬁcate revocation.

**Question:** Your organization is using AWS CloudFormation for infrastructure deployment. How can you provision an ACM certiﬁcate using CloudFormation?

**Answer:** In AWS CloudFormation, you can use the AWS::CertificateManager::Certificate resource type to provision an ACM certiﬁcate. You can specify the domain name, validation method, and other properties as part of the CloudFormation template to automate the provisioning of ACM certiﬁcates along with your infrastructure.

**Question** Your application needs to support internationalized domain names (IDNs) with non-ASCII characters. Can you use ACM to secure IDNs?

**Answer:** Yes, ACM supports internationalized domain names (IDNs) with non-ASCII characters. You can request an ACM certiﬁcate for an IDN by specifying the appropriate domain name during the certiﬁcate request process. ACM will issue a certiﬁcate that supports the speciﬁed IDN, allowing you to secure applications with non-ASCII domain names.

**Question:** Your organization is using AWS CloudTrail for logging and monitoring. Does ACM integrate with AWS CloudTrail to log certiﬁcate-related events?

**Answer:** Yes, ACM integrates with AWS CloudTrail. ACM logs certiﬁcate-related events, such as certiﬁcate issuance,

renewal, and deletion, to AWS CloudTrail. You can use CloudTrail logs to track and monitor ACM certiﬁcate activities and maintain an audit trail of certiﬁcate-related events.