Guía del usuario

AWS Certificate Manager

Version 1.0

AWS Certificate Manager: Guía del usuario

Table of Contents

¿Qué es AWS Certificate Manager?

AWS Certificate Manager (ACM) gestiona la complejidad de crear, almacenar y renovar los certificados y claves SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones. AWS Puede proporcionar certificados para sus servicios de AWS integrados, ya sea emitiéndolos directamente con ACM o importando certificados de terceros al sistema de administración de ACM. Los certificados de ACM pueden proteger nombres de dominio singulares, varios nombres de dominio específicos, dominios comodín o combinaciones de estos. Los certificados comodín de ACM pueden proteger un número ilimitado de subdominios. También puede exportar los certificados de ACM firmados por Autoridad de certificación privada de AWS para usarlos en cualquier parte de su PKI interna.

> **Note**
>
> El uso de ACM no se ha concebido para su uso en un servidor web independiente. Si desea configurar un servidor seguro independiente en una instancia de Amazon EC2, el siguiente tutorial contiene instrucciones: Configuración SSL/TLS en Amazon Linux 2023.

Temas

¿ACM es el servicio adecuado para mí?

AWS ofrece dos opciones a los clientes que implementen certificados X.509 administrados. Elija la que mejor se adapte a sus necesidades.

1. AWS Certificate Manager (ACM): este servicio es para clientes empresariales que necesitan una presencia web segura mediante TLS. Los certificados ACM se implementan a través de Elastic

Load Balancing CloudFront, Amazon, Amazon API Gateway y otros AWS servicios integrados. La aplicación más frecuente de este tipo es un sitio web público seguro con importantes requisitos de tráfico. ACM también simplifica la administración de la seguridad al automatizar la renovación de los certificados que vencen. Está en el lugar adecuado para este servicio.

2. Autoridad de certificación privada de AWS—Este servicio es para clientes empresariales que crean una infraestructura de clave pública (PKI) dentro de la AWS nube y está destinado al uso privado dentro de una organización. Con él Autoridad de certificación privada de AWS, puede crear su propia jerarquía de entidades de certificación (CA) y emitir certificados con ella para autenticar usuarios, ordenadores, aplicaciones, servicios, servidores y otros dispositivos. Los certificados emitidos por una CA privada no se pueden utilizar en Internet. Para obtener más información, consulte la Guía del usuario de Autoridad de certificación privada de AWS.

Características de los certificados de ACM

Los certificados públicos proporcionados por ACM tienen las características que se describen y en esta sección.

> **Note**
>
> Estas características se aplican solo a los certificados proporcionados por ACM. Puede que no se apliquen a los certificados que importe a ACM.

Entidad de certificación y jerarquía

Los certificados públicos que se solicitan a través de ACM se obtienen de Amazon Trust Services, una entidad de certificación (CA) pública administrada por Amazon. Las CA raíz de Amazon de la 1 a la 4 están firmadas de forma cruzada por una raíz más antigua denominada Starfield G2 Root Certificate Authority - G2. La raíz Starfield es de confianza en dispositivos Android a partir de las versiones posteriores a Gingerbread, y en iOS a partir de la versión 4.1. Las raíces de Amazon son de confianza en iOS a partir de la versión 11. Cualquier navegador, aplicación o sistema operativo que incluya las raíces de Amazon o Starfield confiará en los certificados públicos obtenidos de ACM.

Los certificados de hoja o entidad final que ACM emite a los clientes obtienen su autoridad de una CA raíz de Amazon Trust Services a través de alguna de las distintas CA intermedias. ACM asigna aleatoriamente una CA intermedia en función del tipo de certificado (RSA o ECDSA)

solicitado. Puesto que la CA intermedia se selecciona aleatoriamente después de generar la solicitud, ACM no proporciona información sobre la CA intermedia.

Confianza de navegadores y aplicaciones

Los certificados de ACM son de confianza para la mayoría de los principales navegadores, como Google Chrome, Microsoft Internet Explorer y Microsoft Edge, Mozilla Firefox y Apple Safari. Los navegadores que confían en los certificados de ACM muestran un icono de candado en la barra de estado o la barra de direcciones cuando se conectan por SSL/TLS a sitios que utilizan certificados de ACM. Los certificados de ACM también son de confianza para Java.

Rotación de CA intermedias y raíces

Con el fin de mantener una infraestructura de certificados resiliente y ágil, Amazon puede decidir en cualquier momento dejar de utilizar una CA intermedia sin previo aviso. Este tipo de cambios no afectan a los clientes. Para obtener más información, consulte la entrada de blog "Amazon introduces dynamic intermediate certificate authorities" (Amazon presenta las entidades de certificación intermedias dinámicas).

En el improbable caso de que Amazon deje de utilizar una CA raíz, el cambio se producirá tan pronto como lo requieran las circunstancias. Debido al gran impacto de este cambio, Amazon utilizará todos los mecanismos disponibles para notificar a los AWS clientes, incluido el AWS Health Dashboard correo electrónico a los propietarios de las cuentas y la comunicación con los administradores técnicos de cuentas.

Acceso a firewalls para revocación

Si un certificado de entidad final deja de ser de confianza, se revocará. El protocolo OCSP y las listas CRL son los mecanismos estándar que se utilizan para comprobar si un certificado se ha revocado o no. El protocolo OCSP y las listas CRL son los mecanismos estándar que se utilizan para publicar información sobre revocación. Es posible que los firewalls de algunos clientes necesiten reglas adicionales para permitir el funcionamiento de estos mecanismos.

Los siguientes ejemplos de patrones de caracteres comodín de URL se pueden utilizar para identificar tráfico de revocación. Un asterisco (*) representa uno o varios caracteres alfanuméricos, un signo de interrogación de cierre (?) representa un único carácter alfanumérico, y una almohadilla (#) representa un número.

- OCSP

```
http://ocsp.?????.amazontrust.com
```

```
http://ocsp.*.amazontrust.com
```

- CRL

```
http://crl.?????.amazontrust.com/?????.crl
```

```
http://crl.*.amazontrust.com/*.crl
```

Validación de dominio (DV)

Los certificados de ACM son validados por dominio. Es decir, el campo de asunto de un certificado de ACM identifica solo a un nombre de dominio. Cuando solicita un certificado de ACM, debe validar que usted es el propietario de todos los dominios que ha especificado en su solicitud, o bien que es quien los controla. Puede validar la titularidad a través del correo electrónico o DNS. Para obtener más información, consulte Validación por correo electrónico y Validación por DNS.

Periodo de validez

El periodo de validez de los certificados de ACM es de 13 meses (395 días).

Renovación e implementación administradas

ACM administra el proceso de renovación de los certificados de ACM y el aprovisionamiento de estos una vez renovados. La renovación automática puede ayudarle a evitar el tiempo de inactividad debido a certificados configurados incorrectamente, revocados o caducados. Para obtener más información, consulte Renovación administrada para certificados de ACM.

Varios nombres de dominio

Cada certificado de ACM debe incluir al menos un nombre de dominio completo (FQDN), pero puede agregar nombres adicionales si lo desea. Por ejemplo, cuando crea un certificado de ACM para `www.example.com`, puede agregar el nombre `www.example.net` si los clientes pueden acceder a su sitio utilizando cualquiera de los nombres. Lo mismo sucede con los dominios vacíos (también conocidos como ápex de zona o dominios desnudos). Es decir, puede solicitar un certificado de ACM para www.example.com y agregar el nombre example.com. Para obtener más información, consulte Solicitar un certificado público.

Nombres con comodines

ACM permite utilizar un asterisco (*) en el nombre de dominio para crear un certificado de ACM que contenga un nombre comodín que pueda proteger varios sitios en el mismo dominio. Por ejemplo, `*.example.com` protege `www.example.com` e `images.example.com`.

> **Note**
>
> Cuando solicita un certificado de comodín, el asterisco (*****) debe encontrarse en la posición más a la izquierda del nombre de dominio y solo puede proteger un nivel de subdominio. Por ejemplo, ***.example.com** puede proteger **login.example.com** y **test.example.com**, pero no puede proteger **test.login.example.com**. Tenga en cuenta también que ***.example.com** solo protege los subdominios de **example.com**. No protege el dominio desnudo o ápex (**example.com**). Sin embargo, puede solicitar un certificado que proteja una dominio desnudo o ápex y sus subdominios especificando varios nombres de dominio en su solicitud. Por ejemplo, puede solicitar un certificado que proteja **example.com** y ***.example.com**.

Algormos clave

Un certificado debe especificar un algoritmo y un tamaño de clave. Actualmente, ACM admite los siguientes algoritmos de clave pública (ECDSA) y el algoritmo de firma digital de curva elíptica (ECDSA). ACM puede solicitar la emisión de nuevos certificados a través de algoritmos marcados con un asterisco (*). Los algoritmos restantes solo son compatibles con los certificados importados.

> **Note**
>
> Al solicitar un certificado de PKI privado firmado por una CA AWS Private CA, la familia de algoritmos de firma especificada (RSA o ECDSA) debe coincidir con la familia de algoritmos de la clave secreta de la CA.

- RSA de 1024 bits (`RSA_1024`)
- RSA de 2048 bits (`RSA_2048`)*
- RSA de 3072 bits (`RSA_3072`)
- RSA de 4096 bits (`RSA_4096`)
- ECDSA de 256 bits (`EC_prime256v1`)*
- ECDSA de 384 bits (`EC_secp384r1`)*
- ECDSA de 521 bits (`EC_secp521r1`)

Las claves ECDSA son más pequeñas y ofrecen una seguridad comparable a la de las claves RSA, pero con una mayor eficiencia de computación. Sin embargo, ECDSA no es compatible con todos los clientes de red. La siguiente tabla, adaptada del NIST, muestra el nivel de seguridad representativo de RSA y ECDSA con claves de varios tamaños. Todos los valores se muestran en bits.

Comparación de la seguridad de algoritmos y claves

Nivel de seguridad	Tamaño de clave RSA	Tamaño de clave ECDSA
128	3072	256
192	7680	384
256	15360	512

El nivel de seguridad, entendido como una potencia de 2, está relacionado con la cantidad de intentos necesarios para romper el cifrado. Por ejemplo, se pueden recuperar tanto una clave RSA de 3072 bits como una clave ECDSA de 256 bits sin más de 2^{128} intentos.

Para obtener información que le ayude a elegir un algoritmo, consulte la entrada del AWS blog Cómo evaluar y utilizar los certificados ECDSA en. AWS Certificate Manager

> **Important**
>
> Tenga en cuenta que los servicios integrados solo permiten asociar a sus recursos los algoritmos y tamaños de clave que admiten. Además, la compatibilidad varía en función de si el certificado se importa a IAM o ACM. Para obtener más información, consulte la documentación de cada servicio.
>
> - Para Elastic Load Balancing, consulte Agentes de escucha de HTTPS para su Application Load Balancer.
> - Para ello CloudFront, consulte Protocolos y cifrados SSL/TLS compatibles.

Punycode

Se deben cumplir los siguientes requisitos de Punycode relativos a los Nombres de dominio internacionalizados:

1. Los nombres de dominio que empiecen con el patrón “<character><character>--” deben coincidir con “xn--”.
2. Los nombres de dominio que empiecen con “xn--” también deben ser nombres de dominio internacionalizados válidos.

Ejemplos de Punycode

Nombre del dominio	Cumple el n.° 1	Cumple el n.° 2	Permit	Nota
example.com	n/a	n/a	✓	No empieza con “<character><character>--”
a--ejemplo.com	n/a	n/a	✓	No empieza con “<character><character>--”
abc--ejemplo.com	n/a	n/a	✓	No empieza con “<character><character>--”
xn--xyz.com	Sí	Sí	✓	Nombre de dominio internacionalizado válido (se resuelve en 简.com)
xn--ejemplo.com	Sí	No	✗	No es un nombre de dominio internacionalizado válido
ab--ejemplo.com	No	No	✗	Debe empezar con “xn--”

Excepciones

Tenga en cuenta lo siguiente:

- ACM no proporciona certificados de validación extendida (EV) ni certificados de validación de organización (OV).
- ACM no proporciona certificados para nada más que los protocolos SSL/TLS.
- No puede utilizar certificados de ACM para el cifrado de correo electrónico.

- ACM no permite desactivar la renovación de certificados administrada de los certificados de ACM. Además, la renovación administrada no está disponible para los certificados que se importan a ACM.
- No se pueden solicitar certificados para nombres de dominio propiedad de Amazon, por ejemplo los que terminan en amazonaws.com, cloudfront.net o elasticbeanstalk.com.
- No se puede descargar la clave privada de un certificado de ACM.
- No puede instalar de manera directa certificados de ACM en su sitio web o aplicación de Amazon Elastic Compute Cloud (Amazon EC2). No obstante, sí puede utilizar su certificado con cualquier servicio integrado. Para obtener más información, consulte Servicios integrados con AWS Certificate Manager.

Regiones admitidas

Visite Regiones y puntos de enlace de AWS en Referencia general de AWS o la Tabla de regiones de AWS para ver la disponibilidad de regiones de ACM.

Los certificados en ACM son recursos regionales. Para usar un certificado con Elastic Load Balancing para el mismo nombre de dominio completo (FQDN) o conjunto de FQDN en más de una AWS región, debe solicitar o importar un certificado para cada región. Para los certificados proporcionados por ACM, esto significa que debe revalidar cada nombre de dominio en el certificado para cada región. No puede copiar un certificado de una región en otra.

Para utilizar un certificado ACM con Amazon CloudFront, debes solicitar o importar el certificado en la región EE.UU. Este (Norte de Virginia). Los certificados ACM de esta región que están asociados a una CloudFront distribución se distribuyen en todas las ubicaciones geográficas configuradas para esa distribución.

Servicios integrados con AWS Certificate Manager

AWS Certificate Manager admite un número creciente de AWS servicios. No puede instalar su certificado ACM o su Autoridad de certificación privada de AWS certificado privado directamente en su sitio web o aplicación AWS basados.

> **Note**
>
> Los certificados de ACM públicos se pueden instalar en instancias de Amazon EC2 conectadas a un Nitro Enclave, pero no a otras instancias de Amazon EC2. Para obtener

información sobre la configuración de un servidor web independiente en una instancia de Amazon EC2 no conectada a un Nitro Enclave, consulte Tutorial: Install a LAMP web server on Amazon Linux 2 o Tutorial: Install a LAMP web server with the Amazon Linux AMI.

Los certificados de ACM son compatibles con los siguientes servicios:

Elastic Load Balancing

Elastic Load Balancing distribuye de forma automática el tráfico entrante de aplicaciones entre varias instancias de Amazon EC2. Detecta las instancias en mal estado y redirige el tráfico hacia otras en buen estado, hasta que se restauren las instancias en mal estado. Elastic Load Balancing escala de forma automática su capacidad de gestión de solicitudes en respuesta al tráfico entrante. Para obtener más información sobre balanceadores de carga, consulte la Guía del usuario de Elastic Load Balancing.

En general, para distribuir contenido seguro a través de SSL/TLS, los balanceadores de carga requieren que los certificados SSL/TLS se instalen en el balanceador de carga o en la instancia backend de Amazon EC2. ACM se integra con Elastic Load Balancing para implementar certificados de ACM en el balanceador de carga. Para obtener más información, consulte Crear un Application Load Balancer.

Amazon CloudFront

Amazon CloudFront es un servicio web que acelera la distribución del contenido web dinámico y estático a los usuarios finales mediante la entrega del contenido desde una red mundial de ubicaciones periféricas. Cuando un usuario final solicita el contenido a través del cual estás publicando CloudFront, se redirige al usuario a la ubicación perimetral que ofrezca la latencia más baja. De este modo, se garantiza que el contenido se entrega con el máximo rendimiento posible. Si el contenido se encuentra actualmente en esa ubicación perimetral, CloudFront envíelo inmediatamente. Si el contenido no se encuentra actualmente en esa ubicación perimetral CloudFront , recupérelo del bucket o servidor web de Amazon S3 que haya identificado como la fuente de contenido definitiva. Para obtener más información al respecto CloudFront, consulta la Guía para CloudFront desarrolladores de Amazon.

Para ofrecer contenido seguro a través de SSL/TLS, es CloudFront necesario que los certificados SSL/TLS estén instalados en la distribución o en la CloudFront fuente de contenido respaldada. El ACM está integrado para implementar los certificados de ACM en la distribución. CloudFront CloudFront Para obtener más información, consulte la sección Obtener un certificado SSL/TLS.

> **Note**
>
> Para utilizar un certificado ACM CloudFront, debe solicitar o importar el certificado en la región EE.UU. Este (Virginia del Norte).

Amazon Cognito

Amazon Cognito ofrece autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Los usuarios pueden iniciar sesión directamente con tus Cuenta de AWS credenciales o a través de un tercero, como Facebook, Amazon, Google o Apple. Para obtener más información sobre Amazon Cognito, consulte la Guía para desarrolladores de Amazon Cognito.

Al configurar un grupo de usuarios de Cognito para usar un CloudFront proxy de Amazon, CloudFront puede implementar un certificado ACM para proteger el dominio personalizado. Si este es el caso, tenga en cuenta que debe eliminar la asociación del certificado CloudFront antes de poder eliminarlo.

AWS Elastic Beanstalk

Elastic Beanstalk le ayuda a implementar y administrar aplicaciones AWS en la nube sin preocuparse por la infraestructura que las ejecuta. AWS Elastic Beanstalk reduce la complejidad de la administración. Solo tiene que cargar la aplicación y Elastic Beanstalk gestionará de manera automática los detalles de aprovisionamiento de capacidad, balanceador de carga, escalado y monitoreo de estado. Elastic Beanstalk utiliza el servicio Elastic Load Balancing para crear un balanceador de carga. Para obtener más información sobre Elastic Beanstalk, consulte la Guía para desarrolladores de AWS Elastic Beanstalk.

Para elegir un certificado, debe configurar el balanceador de carga para su aplicación en la consola de Elastic Beanstalk. Para obtener más información, consulte Configuración del balanceador de carga del entorno Elastic Beanstalk para terminar HTTPS.

AWS App Runner

App Runner es un AWS servicio que proporciona una forma rápida, sencilla y rentable de implementar directamente desde el código fuente o una imagen de contenedor hasta una aplicación web escalable y segura en la AWS nube. No necesita aprender nuevas tecnologías, decidir qué servicio de cómputo usar ni saber cómo aprovisionar y configurar AWS los recursos. Para obtener más información sobre App Runner, consulte la Guía para desarrolladores de AWS App Runner.

Cuando asocia nombres de dominio personalizados con el servicio App Runner, crea internamente certificados que rastrean la validez del dominio. Están almacenados en ACM. App Runner conserva estos certificados durante siete días después de que el dominio se ha desasociado del servicio o después de que el servicio se ha eliminado. Todo este proceso está automatizado y no necesita agregar ni administrar ningún certificado. Para obtener más información, consulte Administración de nombres de dominio personalizados para un servicio de App Runner en la Guía para desarrolladores de AWS App Runner .

Amazon API Gateway

Con la proliferación de dispositivos móviles y el crecimiento del Internet de las cosas (IoT), es cada vez más habitual crear API que se puedan utilizar para obtener acceso a los datos e interactuar con los sistemas backend en AWS. Puede utilizar API Gateway para publicar, mantener, monitorear y proteger las API. Después de implementar la API en API Gateway, puede configurar un nombre de dominio personalizado para simplificar el acceso a él. Para configurar un nombre de dominio personalizado, debe proporcionar un certificado SSL/TLS. Puede utilizar ACM para generar o importar el certificado. Para obtener más información sobre Amazon API Gateway, consulte la Guía para desarrolladores de Amazon API Gateway.

AWS Nitro Enclaves

AWS Nitro Enclaves es una función de Amazon EC2 que le permite crear entornos de ejecución aislados, denominados enclaves, a partir de instancias de Amazon EC2. Los enclaves son máquinas virtuales independientes, reforzadas y altamente restringidas. Proporcionan solo conectividad de socket local segura con su instancia principal. No tienen almacenamiento persistente, acceso interactivo ni red externa. Los usuarios no pueden acceder por SSH a un enclave, y los procesos, aplicaciones o usuarios (incluidos los raíz o administradores) de la instancia principal no pueden acceder a los datos y las aplicaciones dentro del enclave.

Las instancias EC2 conectadas a Nitro Enclaves admiten certificados de ACM. Para obtener más información, consulte AWS Certificate Manager para Nitro Enclaves.

> **Note**
>
> No se pueden asociar certificados de ACM a una instancia EC2 que no esté conectada a un Nitro Enclave.

AWS CloudFormation

AWS CloudFormation le ayuda a modelar y configurar sus recursos de Amazon Web Services. Cree una plantilla que describa los AWS recursos que quiere usar, como Elastic Load Balancing o API Gateway. A continuación, AWS CloudFormation se encarga de aprovisionar y configurar para usted dichos recursos. No necesita crear y configurar AWS los recursos de forma individual ni averiguar qué depende de qué; se AWS CloudFormation encarga de todo eso. Los certificados ACM se incluyen como un recurso de plantilla, lo que significa que AWS CloudFormation puede solicitar certificados ACM que puede utilizar con AWS los servicios para habilitar conexiones seguras. Además, los certificados ACM se incluyen en muchos de AWS los recursos con los que puede configurarlos. AWS CloudFormation

Para obtener información general al respecto CloudFormation, consulte la Guía del AWS CloudFormation usuario. Para obtener información sobre los recursos de ACM compatibles con CloudFormation, consulte AWS::CertificateManager::Certificate.

Gracias a la potente automatización que ofrece AWS CloudFormation, es fácil superar la cuota de certificados, especialmente con AWS cuentas nuevas. Le recomendamos que siga las prácticas recomendadas de la ACM para AWS CloudFormation.

> **Note**
>
> Si crea un certificado ACM con AWS CloudFormation, la AWS CloudFormation pila permanece en el estado CREATE_IN_PROGRESS. Cualquier otra operación de pila se retrasa hasta que usted actúe según las instrucciones del correo electrónico de validación del certificado. Para obtener más información, consulte Recursos que no pueden estabilizarse durante una operación de pila de creación, actualización o eliminación.

AWS Amplify

Amplify es un conjunto de herramientas y funciones diseñadas específicamente que permite a los desarrolladores web y móviles de front-end crear aplicaciones completas de forma rápida y sencilla. AWS Amplify proporciona dos servicios: Amplify Hosting y Amplify Studio. Amplify Hosting proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor de pila completa con implementación continua. Amplify Studio es un entorno de desarrollo visual que simplifica la creación de aplicaciones web y móviles escalables de pila completa. Usa Studio para crear tu interfaz de usuario front-end con un conjunto de componentes

de ready-to-use interfaz de usuario, crea un backend de aplicaciones y, a continuación, conecta los dos. Para obtener más información sobre Amplify, consulte la Guía del usuario de AWS Amplify.

Si conecta un dominio personalizado con la aplicación, la consola de Amplify emite un certificado de ACM para protegerlo.

OpenSearch Servicio Amazon

Amazon OpenSearch Service es un motor de búsqueda y análisis para casos de uso como el análisis de registros, la supervisión de aplicaciones en tiempo real y el análisis del flujo de clics. Para obtener más información, consulta la Guía para desarrolladores OpenSearch de Amazon Service.

Al crear un clúster de OpenSearch servicios que contiene un dominio y un punto de conexión personalizados, puede usar ACM para aprovisionar el Application Load Balancer asociado con un certificado.

AWS Network Firewall

AWS Network Firewall es un servicio gestionado que facilita la implementación de protecciones de red esenciales para todas sus Amazon Virtual Private Clouds (VPC). Para obtener más información sobre Network Firewall, consulte la Guía para desarrolladores de AWS Network Firewall.

El firewall Network Firewall se integra con ACM para la inspección de TLS. Si utiliza la inspección de TLS en Network Firewall, debe configurar un certificado ACM para descifrar y volver a cifrar el tráfico SSL/TLS que pasa por su firewall. Para obtener información sobre cómo funciona Network Firewall con ACM para la inspección de TLS, consulte Requisitos para usar certificados SSL/TLS con configuraciones de inspección de TLS en la Guía para desarrolladores de AWS Network Firewall .

Sellos del sitio y logotipos de confianza

Amazon no proporciona un precinto del sitio ni permite que su marca comercial se utilice como tal:

- AWS Certificate Manager (ACM) no proporciona un sello de sitio seguro que pueda usar en su sitio web. Si desea utilizar un precinto del sitio, puede obtener uno de un proveedor de terceros. Le recomendamos que escoja un proveedor que evalúe y confirme la seguridad de sus prácticas de negocio o de la página web.

- Amazon no permite a su marca comercial o logotipo que sea utilizado como insignia de certificado, precinto de sitio o logotipo de confianza. Los sellos e insignias de este tipo pueden copiarse en sitios que no utilicen el servicio de ACM y es posible que sean utilizados de forma inadecuada para crear confianza con excusas falsas. Para proteger a nuestros clientes y la reputación de Amazon no permitimos que nuestra marca comercial y nuestro logotipo se utilicen de esta manera.

Cuotas

Las siguientes cuotas de servicio AWS Certificate Manager (ACM) se aplican a cada AWS región y por cuenta. AWS

Para ver qué cuotas se pueden ajustar, consulte la tacla de cuotas de ACM en la AWS Guía de referencia general. Para solicitar aumentos de cuota, cree un caso en el Centro de AWS Support.

Cuotas generales

Elemento	Cuota predeterminada
Número de certificados de ACM Los certificados vencidos y revocados siguen computándose para este total. Los certificados firmados por una entidad emisora de Autoridad de certificación privada de AWS origen no se incluyen en este total.	2 500
Número de certificados de ACM al año (últimos 365 días) Puede solicitar hasta el doble de su cuota de certificados de ACM por año, región y cuenta. Por ejemplo, si su cuota es 2500, puede solicitar hasta 5000 certificados de ACM al año en una región y cuenta determinadas. Solo puede tener 2500 certificados al mismo tiempo. Para solicitar 5000 certificados al año, debe eliminar 2500 durante el año para manteners	El doble de la cuota de su cuenta

Elemento	Cuota predeterminada
e dentro de la cuota. Si necesita más de 2500 certificados al mismo tiempo, contacte con el Centro de AWS Support. Los certificados firmados por una entidad emisora de Autoridad de certificación privada de AWS entidad emisora no se incluyen en este total.	
Número de certificados importadas	2.500
Número de certificados importados al año (últimos 365 días)	El doble de la cuota de su cuenta

Elemento	Cuota predeterminada
Número de nombres de dominio por certificado de ACM La cuota predeterminada es 10 nombres de dominio para cada certificado de ACM. Su cuota puede ser mayor. El primer nombre de dominio que envía se incluye como nombre común (CN) del asunto del certificado. Todos los nombres se incluyen en la extensión del nombre alternativo de asunto. Puede solicitar hasta 100 nombres de dominio. Para solicitar un aumento de la cuota, cree una solicitud en la consola Service Quotas para el servicio ACM. pero antes de hacerlo, lea la siguiente información para saber cómo añadir más nombres de dominio puede significar más trabajo administrativo para usted si usa la validación por correo electrónico. Para obtener más información, consulte Validación del dominio. La cuota del número de nombres de dominio por certificado de ACM se aplica solo a los certificados proporcionados por ACM. Esta cuota no se aplica a los certificados que se importan a ACM. Las secciones siguientes son aplicables solo a los certificados de ACM.	10

Elemento	Cuota predeterminada
Número de CA privadas ACM está integrado con AWS Private Certificate Authority ()Autoridad de certificación privada de AWS. Puede utilizar la consola de ACM o la API de ACM para solicitar certificados privados a una entidad de certificación (CA) privada existente alojada por. AWS CLI Autoridad de certificación privada de AWS Estos certificados se administran dentro del entorno de ACM y tienen las mismas restricciones que los certificados públicos emitidos por ACM. Para obtener más información, consulte Solicitud de un certificado PKI privado. También puede emitir certificados privados mediante el servicio independiente Autoridad de certificación privada de AWS . Para obtener más información, consulte el artículo sobre cómo emitir un certificado privado de entidad final. Una CA privada que se haya eliminado se tendrá en cuenta para la cuota hasta el final de su período de restauración. Para obtener más información, consulte Eliminación de una CA privada.	200
Número de certificados privados por CA (vida útil)	1 000 000

Cuotas de tarifas de API

Las siguientes cuotas de servicio se aplican a la API de ACM para cada región y cuenta. ACM aplica distintas limitaciones controladas a las solicitudes de API en función de la operación de la API. La limitación controlada significa que ACM rechaza una solicitud válida porque esta supera la cuota del número de solicitudes por segundo de la operación. Cuando se limita una solicitud de forma controlada, ACM devuelve un error `ThrottlingException`. En la siguiente tabla se muestra cada

operación de la API y la cuota en la que ACM limita de forma controlada las solicitudes de dicha operación.

> **Note**
>
> Además de las acciones de la API que se enumeran en la tabla de abajo, ACM también puede llamar a la acción `IssueCertificate` externa de Autoridad de certificación privada de AWS. Para obtener información sobre las cuotas up-to-date `IssueCertificate` tarifarias, consulte los puntos finales y las cuotas de. Autoridad de certificación privada de AWS

equests-per-second Cuota R para cada operación de la API de ACM

Llamada a la API	Solicitudes por segundo
`AddTagsToCertificate`	5
`DeleteCertificate`	10
`DescribeCertificate`	10
`ExportCertificate`	5
`GetAccountConfiguration`	1
`GetCertificate`	10
`ImportCertificate`	1
`ListCertificates`	8
`ListTagsForCertificate`	10
`PutAccountConfiguration`	1
`RemoveTagsFromCertificate`	5
`RenewCertificate`	5

Llamada a la API	Solicitudes por segundo
`RequestCertificate`	5
`ResendValidationEmail`	1
`UpdateCertificateOptions`	5

Para obtener más información, consulte Referencia de la API de AWS Certificate Manager.

Precios para AWS Certificate Manager

No se cobra un cargo adicional por los certificados SSL/TLS que gestione con AWS Certificate Manager. Solo paga por los AWS recursos que cree para ejecutar su sitio web o aplicación. Para obtener la información más reciente sobre los precios de ACM, consulte la página de precios de los AWS Certificate Manager servicios en el AWS sitio web.

Seguridad en AWS Certificate Manager

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Certificate Manager, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Certificate Manager (ACM). En los siguientes temas, se le mostrará cómo configurar ACM para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de ACM.

Temas

Protección de datos en AWS Certificate Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Certificate Manager. Como se describe en este modelo, AWS es responsable de proteger

la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con ACM o con otros dispositivos Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Seguridad para las claves privadas del certificado

Cuando solicita un certificado público, AWS Certificate Manager (ACM) genera un key pair de claves pública/privada. Sin embargo, en el caso de los certificados importados, es usted quien genera el par de claves. La clave pública pasa a formar parte del certificado. ACM almacena el certificado y su clave privada correspondiente, y usa AWS Key Management Service (AWS KMS) para ayudar a proteger la clave privada. El proceso ocurre de la siguiente manera:

1. La primera vez que solicita o importa un certificado en una AWS región, ACM crea un certificado gestionado AWS KMS key con el alias aws/acm. Esta clave de KMS es única en cada AWS cuenta y región. AWS
2. ACM utiliza esta clave KMS para cifrar la clave privada del certificado. ACM solo almacena una versión cifrada de la clave privada (ACM no almacena la clave privada como texto sin cifrar). ACM usa la misma clave KMS para cifrar las claves privadas de todos los certificados de una AWS cuenta y una región específicas AWS .
3. Al asociar el certificado con un servicio integrado en AWS Certificate Manager, ACM envía el certificado y la clave privada cifrada al servicio. También se crea una concesión AWS KMS que permite al servicio utilizar la clave KMS para descifrar la clave privada del certificado. Para obtener más información sobre las concesiones, consulte Uso de concesiones en la Guía para desarrolladores de AWS Key Management Service . Para obtener más información sobre los servicios compatibles con ACM, consulte Servicios integrados con AWS Certificate Manager.

   > **Note**
   >
   > Usted tiene el control de la AWS KMS concesión que se crea automáticamente. Si elimina esta concesión por cualquier motivo, pierde la funcionalidad de ACM para el servicio integrado.

4. Los servicios integrados utilizan la clave KMS para descifrar la clave privada. A continuación, el servicio utiliza el certificado y la clave privada descifrada (no cifrada) para establecer canales de comunicación segura (sesiones SSL/TLS) con sus clientes.
5. Cuando el certificado se desvincula de un servicio integrado, la concesión creada en el paso 3 se retira. Esto significa que el servicio no puede utilizar más la clave KMS para descifrar la clave privada del certificado.

Identity and Access Management para AWS Certificate Manager

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de ACM. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en ACM.

Usuario de servicio: si utiliza el servicio de ACM para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de ACM para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en ACM, consulte Solución de problemas de AWS Certificate Manager identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de ACM en su empresa, es probable que tenga acceso completo a ACM. Su trabajo consiste en determinar a qué características y recursos de

ACM deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con ACM, consulte ¿Cómo AWS Certificate Manager funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a ACM. Para consultar ejemplos de políticas basadas en identidades de ACM que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para AWS Certificate Manager.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener

información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una

política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites

de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Certificate Manager funciona con IAM

Antes de utilizar IAM para administrar el acceso a ACM, conozca qué características de IAM se pueden utilizar con ACM.

Funciones de IAM que puede utilizar con AWS Certificate Manager

Característica de IAM	Soporte de ACM
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No

Característica de IAM	Soporte de ACM
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan ACM y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades de ACM

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones.

No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de ACM

Para ver ejemplos de políticas basadas en identidades de ACM, consulte Ejemplos de políticas basadas en la identidad para AWS Certificate Manager.

Políticas basadas en recursos de ACM

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas de ACM

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de ACM, consulte Acciones definidas por AWS Certificate Manager en la Referencia de autorizaciones de servicio.

Las acciones de políticas de ACM utilizan el siguiente prefijo antes de la acción:

```
acm
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "acm:action1",
      "acm:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidades de ACM, consulte Ejemplos de políticas basadas en la identidad para AWS Certificate Manager.

Recursos de políticas de ACM

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de ACM y sus ARN, consulte Recursos definidos por AWS Certificate Manager en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Certificate Manager.

Para ver ejemplos de políticas basadas en identidades de ACM, consulte Ejemplos de políticas basadas en la identidad para AWS Certificate Manager.

Claves de condición de política de ACM

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de ACM, consulte Claves de condición para AWS Certificate Manager en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Certificate Manager.

Para ver ejemplos de políticas basadas en identidades de ACM, consulte Ejemplos de políticas basadas en la identidad para AWS Certificate Manager.

ACL en ACM

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con ACM

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar

etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con ACM

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de ACM

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de ACM

Compatible con roles de servicio	No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de ACM. Edite los roles de servicio solo cuando ACM proporcione orientación para hacerlo.

Roles vinculados a servicios de ACM

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Certificate Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de ACM. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por ACM, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS Certificate Manager en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de ACM
- Cómo permitir a los usuarios consultar sus propios permisos

- Enumeración de certificados
- Recuperación de un certificado
- Importación de un certificado
- Eliminación de un certificado

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de ACM en su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de ACM

Para acceder a la AWS Certificate Manager consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de ACM de su Cuenta de AWS propiedad. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de ACM, adjunte también la política *AWSCertificateManagerReadOnly* AWS gestionada por ACM a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Enumeración de certificados

La siguiente política permite a un usuario crear una lista de todos los certificados de ACM en la cuenta de usuario.

```
{
            "Version":"2012-10-17",
            "Statement":[
            {
            "Effect":"Allow",
            "Action":"acm:ListCertificates",
            "Resource":"*"
            }
            ]
```

```
            }
```

> **Note**
>
> Este permiso es necesario para que los certificados ACM aparezcan en Elastic Load Balancing y en CloudFront las consolas.

Recuperación de un certificado

La siguiente política permite a un usuario recuperar un certificado de ACM específico.

```
{
            "Version":"2012-10-17",
            "Statement":{
            "Effect":"Allow",
            "Action":"acm:GetCertificate",
            "Resource":"arn:aws:acm:region:account:certificate/certificate_ID"
            }
            }
```

Importación de un certificado

La siguiente política le permite a un usuario importar un certificado.

```
{
            "Version":"2012-10-17",
            "Statement":{
            "Effect":"Allow",
            "Action":"acm:ImportCertificate",
            "Resource":"arn:aws:acm:region:account:certificate/certificate_ID"
            }
            }
```

Eliminación de un certificado

La siguiente política permite a un usuario eliminar un certificado de ACM específico.

```
{
            "Version":"2012-10-17",
```

```
"Statement":{
"Effect":"Allow",
"Action":"acm:DeleteCertificate",
"Resource":"arn:aws:acm:region:account:certificate/certificate_ID"
}
}
```

Permisos de la API de ACM: referencia de recursos y acciones

Cuando configure el control de acceso y escriba políticas de permisos que se pueden asociar a un usuario o rol de IAM, puede utilizar la siguiente tabla como referencia. La primera columna de la tabla enumera cada operación de la API de AWS Certificate Manager. Usted especifica acciones en un elemento `Action` de la política. El resto de columnas proporcionan información adicional:

Puede utilizar los elementos de la política de IAM en sus políticas de ACM para expresar condiciones. Para ver una lista completa, consulte Claves disponibles en la Guía del usuario de IAM.

> **Note**
>
> Para especificar una acción, use el prefijo `acm:` seguido del nombre de operación de la API (por ejemplo, `acm:RequestCertificate`).

Permisos y operaciones de la API de ACM

Operaciones de la API de ACM	Permisos requeridos (operaciones de API)	Recursos
AddTagsToCertificate	`acm:AddTagsToCertificate`	`arn:aws:acm: region:account:certificate/ certificate_ID`
DeleteCertificate	`acm:DeleteCertificate`	`arn:aws:acm: region:account:certificate/ certificate_ID`
DescribeCertificate	`acm:DescribeCertificate`	`arn:aws:acm: region:account:certificate/ certificate_ID`

Operaciones de la API de ACM	Permisos requeridos (operaciones de API)	Recursos
ExportCertificate	`acm:ExportCertificate`	`arn:aws:acm:` *region*`:` *account*`:certificate/` *certificate_ID*
GetAccountConfiguration	`acm:GetAccountConfiguration`	`*`
GetCertificate	`acm:GetCertificate`	`arn:aws:acm:` *region*`:` *account*`:certificate/` *certificate_ID*

ImportCertificate	`acm:ImportCertificate`	`arn:aws:acm:` *region*`:` *account*`:certificate/*`
		o bien
		`*`

ListCertificates	`acm:ListCertificates`	`*`
ListTagsForCertificate	`acm:ListTagsForCertificate`	`arn:aws:acm:` *region*`:` *account*`:certificate/` *certificate_ID*
PutAccountConfiguration	`acm:PutAccountConfiguration`	`*`
RemoveTagsFromCertificate	`acm:RemoveTagsFromCertificate`	`arn:aws:acm:` *region*`:` *account*`:certificate/` *certificate_ID*

Operaciones de la API de ACM	Permisos requeridos (operaciones de API)	Recursos

RequestCertificate	`acm:RequestCertificate`	`arn:aws:acm: region:account:certificate/*`
		
		o bien
		
		`*`

ResendValidationEmail	`acm:ResendValidationEmail`	`arn:aws:acm: region:account:certificate/ certificate_ID`
UpdateCertificateOptions	`acm:UpdateCertificateOptions`	`arn:aws:acm: region:account:certificate/ certificate_ID`

Políticas administradas de AWS para AWS Certificate Manager

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas por AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWSCertificateManagerReadOnly

Esta política proporciona acceso de solo lectura a los certificados de ACM; permite a los usuarios describir, enumerar y recuperar certificados de ACM.

```
{
"Version":"2012-10-17",
"Statement":{
    "Effect":"Allow",
    "Action":[
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:GetCertificate",
        "acm:ListTagsForCertificate",
        "acm:GetAccountConfiguration"
    ],
    "Resource":"*"
}
}
```

Para ver esta política administrada por AWS en la consola, visite https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly.

AWSCertificateManagerFullAccess

Esta política proporciona acceso completo a todas las acciones y recursos de ACM.

```
{
"Version":"2012-10-17",
"Statement":[
    {
        "Effect":"Allow",
        "Action":[
            "acm:*"
        ],
        "Resource":"*"
```

```
    },
    {
        "Effect":"Allow",
        "Action":"iam:CreateServiceLinkedRole",
        "Resource":"arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
        "Condition":{
            "StringEquals":{
                "iam:AWSServiceName":"acm.amazonaws.com"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:GetRole"
        ],
        "Resource":"arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
    ]
}
```

Para ver esta política administrada por AWS en la consola, visite https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess.

Actualizaciones de ACM en las políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para ACM debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página Historial de documentos de ACM.

Cambio	Descripción	Fecha
Se ha agregado compatibilidad con `GetAccoun`	La política `AWSCertificateManagerReadOn`	3 de marzo de 2021

Cambio	Descripción	Fecha
`tConfiguration` a la política AWSCertificateManagerReadOnly.	`ly` ahora incluye permiso para llamar a la acción de la API `GetAccountConfiguration` .	
ACM comienza el seguimiento de cambios	ACM comienza el seguimiento de cambios de las políticas administradas por AWS.	3 de marzo de 2021

Uso de claves de condición con ACM

AWS Certificate Manager utiliza claves de condición de AWS Identity and Access Management (IAM) para limitar el acceso a las solicitudes de certificados. Con las claves de condición de las políticas de IAM o las políticas de control de servicio (SCP), puede crear solicitudes de certificados que se ajusten a las directrices de su organización.

> **Note**
>
> Combine las claves de condición de ACM con las claves de condición globales de AWS, como `aws:PrincipalArn`, para restringir aún más las acciones a usuarios o roles específicos.

Condiciones compatibles con ACM

Operaciones de la API de ACM y condiciones compatibles

Clave de condición	Operaciones de la API de ACM compatibles	Tipo	Descripción
`acm:ValidationMethod`	RequestCertificate	Cadena (`EMAIL`, `DNS`)	Filtra las solicitudes en función del método de validación de ACM

Clave de condición	Operaciones de la API de ACM compatibles	Tipo	Descripción
`acm:DomainNames`	RequestCertificate	ArrayOfString	Filtra en función de los nombres de dominio en la solicitud de ACM
`acm:KeyAlgorithm`	RequestCertificate	Cadena	Filtra las solicitudes en función del tamaño y algoritmo de clave de ACM
`acm:CertificateTransparencyLogging`	RequestCertificate	Cadena (`ENABLED`, `DISABLED`)	Filtra las solicitudes en función de la preferencia de registro de transparencia del certificado de ACM
`acm:CertificateAuthority`	RequestCertificate	ARN	Filtra las solicitudes en función de las entidades de certificación en la solicitud de ACM

Ejemplo 1: Restringir el método de validación

La siguiente política deniega las solicitudes de certificados nuevas mediante el método de Validación por correo electrónico, excepto en el caso de una solicitud que se realiza mediante el rol `arn:aws:iam::123456789012:role/AllowedEmailValidation`.

```
{
    "Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
```

```
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "StringLike" : {
                "acm:ValidationMethod":"EMAIL"
            },
            "ArnNotLike": {
                "aws:PrincipalArn": [ "arn:aws:iam::123456789012:role/
AllowedEmailValidation"]
            }
        }
    }
}
```

Ejemplo 2: Evitar los dominios comodín

La siguiente política deniega cualquier solicitud de certificado de ACM nueva que utilice dominios comodín.

```
{
    "Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition": {
            "ForAnyValue:StringLike": {
                "acm:DomainNames": [
                    "${*}.*"
                ]
            }
        }
    }
}
```

Ejemplo 3: Restringir los dominios de certificados

La siguiente política deniega cualquier solicitud de certificado de ACM nueva para dominios que no terminen con `*.amazonaws.com`.

```
{
    "Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition": {
            "ForAnyValue:StringNotLike": {
                "acm:DomainNames": ["*.amazonaws.com"]
            }
        }
    }
}
```

La política podría restringirse aún más a subdominios específicos. Esta política solo permitiría solicitudes en las que cada dominio coincida con al menos uno de los nombres de dominio condicionales.

```
{
    "Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition": {
            "ForAllValues:StringNotLike": {
                "acm:DomainNames": ["support.amazonaws.com", "developer.amazonaws.com"]
            }
        }
    }
}
```

Ejemplo 4: Restringir los algoritmos de clave

La siguiente política utiliza la clave de condición `StringNotLike` para permitir solo los certificados que se soliciten con el algoritmo de clave ECDSA de 384 bits (`EC_secp384r1`).

```
{
    "Version":"2012-10-17",
        "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "StringNotLike" : {
                "acm:KeyAlgorithm":"EC_secp384r1"
            }
        }
    }
}
```

La siguiente política utiliza la clave de condición `StringLike` y el comodín `*` coincidente para evitar las solicitudes de certificados nuevos en ACM con cualquier algoritmo de clave RSA.

```
{
    "Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "StringLike" : {
                "acm:KeyAlgorithm":"RSA*"
            }
        }
    }
}
```

Ejemplo 5: Restringir la entidad de certificación

La siguiente política solo permitiría las solicitudes de certificados privados mediante el ARN de la entidad de certificación privada (PCA) proporcionado.

```
{
    "Version":"2012-10-17",
```

```
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "StringNotLike": {
                "acm:CertificateAuthority":" arn:aws:acm-
pca:region:account:certificate-authority/CA_ID"
            }
        }
    }
}
```

Esta política utiliza la condición `acm:CertificateAuthority` para permitir solo las solicitudes de certificados de confianza públicos que emite Amazon Trust Services. Configurar el ARN de la entidad de certificación en `false` evita las solicitudes de certificados privados de la PCA.

```
{
"Version":"2012-10-17",
    "Statement":{
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "Null" : {
                "acm:CertificateAuthority":"false"
            }
        }
    }
}
```

Uso de un rol vinculado a servicios (SLR) con ACM

AWS Certificate Manager utiliza un rol vinculado a un servicio AWS Identity and Access Management (IAM) para permitir la renovación automática de los certificados ACM gestionados. Un rol vinculado a servicios (SLR) es un rol de IAM que se encuentra vinculado directamente a un servicio de ACM. ACM ha predefinido los SLR y estos incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

El SLR simplifica la configuración de ACM y usted ya no tendrá que agregar de forma manual los permisos necesarios para la firma de certificados sin supervisión. ACM define los permisos de este SLR y, a menos que se defina de otro modo, solo ACM puede asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten SLR, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Elija la opción Yes (Sí) con un enlace para ver la documentación de SLR para ese servicio.

Permisos de SLR para ACM

ACM utiliza un SLR denominado política de rol de servicio de Amazon Certificate Manager.

La AWSServiceRoleForCertificateManager SLR confía en los siguientes servicios para asumir la función:

- `acm.amazonaws.com`

La política de permisos del rol permite que ACM realice las siguientes acciones en los recursos especificados:

- Acciones: `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` en "*"

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un SLR. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

> **Important**
>
> ACM podría avisarle que no puede determinar si existe un SLR en su cuenta. Si ya se ha concedido el permiso `iam:GetRole` necesario al SLR de ACM para su cuenta, el aviso no se repetirá después de crearse el SLR. Si se repite, es posible que usted o el administrador de su cuenta tengan que conceder el permiso `iam:GetRole` a ACM o asociar la cuenta a la política `AWSCertificateManagerFullAccess` administrada por ACM.

Creación del SLR para ACM

No será necesario crear de forma manual el SLR que utiliza ACM. Al emitir un certificado ACM mediante la AWS Management Console, la AWS CLIAPI o la AWS API, ACM crea la SLR automáticamente la primera vez que elige una CA privada para firmar el certificado.

Si recibe mensajes que indican que ACM no puede determinar si existe una SLR en su cuenta, es posible que su cuenta no haya concedido el permiso de lectura necesario. Autoridad de certificación privada de AWS Esto no impedirá instalar el SLR y aún podrá emitir certificados, pero ACM no podrá renovar los certificados de forma automática hasta que resuelva el problema. Para obtener más información, consulte Problemas con el rol vinculado a servicios (SLR) de ACM.

> **Important**
>
> Este SLR puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizabas el servicio ACM antes del 1 de enero de 2017, cuando comenzó a admitir cámaras réflex, ACM creó el AWSServiceRoleForCertificateManager rol en tu cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este SLR y necesita crearlo de nuevo, utilice cualquiera de los siguientes métodos:

- En la consola de IAM, elija Role, Create role y Certificate Manager para crear un nuevo rol con el caso de CertificateManagerServiceRolePolicyuso.
- Con la API de IAM CreateServiceLinkedRoleo el AWS CLI comando correspondiente create-service-linked-role, cree una SLR con el nombre del `acm.amazonaws.com` servicio.

Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM.

Edición del SLR para ACM

ACM no permite editar el rol vinculado al AWSServiceRoleForCertificateManager servicio. Después de crear un SLR, no puede cambiar el nombre porque varias entidades pueden hacer referencia a él. Sin embargo, sí puede editar la descripción del rol con IAM. Para más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación del SLR para ACM

Por lo general, no es necesario eliminar la SLR. AWSServiceRoleForCertificateManager Sin embargo, puedes eliminar el rol manualmente mediante la consola de IAM, la AWS CLI o la AWS API. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con los SLR de ACM

ACM admite el uso de cámaras réflex en todas las regiones en las que están disponibles tanto ACM como yo. Autoridad de certificación privada de AWS Para obtener más información, consulte Regiones y puntos de conexión deAWS.

Nombre de la región	Identidad de la región	Compatibilidad en ACM
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
Asia Pacífico (Mumbai)	ap-south-1	Sí
Asia Pacífico (Osaka)	ap-northeast-3	Sí
Asia Pacífico (Seúl)	ap-northeast-2	Sí
Asia Pacífico (Singapur)	ap-southeast-1	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí
Asia Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (Central)	ca-central-1	Sí
Europa (Frankfurt)	eu-central-1	Sí
Europa (Zúrich)	eu-central-2	Sí

Nombre de la región	Identidad de la región	Compatibilidad en ACM
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (París)	eu-west-3	Sí
América del Sur (São Paulo)	sa-east-1	Sí
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	Sí
AWS GovCloud (EE. UU.-Este) Este	us-gov-east-1	Sí

Solución de problemas de AWS Certificate Manager identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con ACM e IAM.

Temas

- No tengo autorización para realizar una acción en ACM
- No tengo autorización para solicitar un certificado en ACM
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de ACM

No tengo autorización para realizar una acción en ACM

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `acm:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 acm:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `acm:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No tengo autorización para solicitar un certificado en ACM

Si recibe este error, el administrador de ACM o PKI ha establecido reglas que le impiden solicitar el certificado en su estado actual.

El siguiente ejemplo de error se produce cuando un usuario de IAM intenta utilizar la consola para solicitar un certificado mediante opciones configuradas por el administrador de la organización con una `DENY`.

```
User: arn:aws:sts::account::ID: is not authorized to perform: acm:RequestCertificate
on resource: arn:aws:acm:region:account:certificate/*
with an explicit deny in a service control policy
```

En este caso, la solicitud se debe volver a realizar de forma que esté en línea con las políticas que estableció el administrador. O bien, se debe actualizar la política para permitir la solicitud del certificado.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a ACM.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en ACM. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de ACM

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si ACM admite estas características, consulte ¿Cómo AWS Certificate Manager funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro Cuenta de AWS de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca del uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Resiliencia en AWS Certificate Manager

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de

disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Certificate Manager

Como servicio gestionado, AWS Certificate Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a ACM a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Obtener acceso programático a ACM

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario. • Para obtener AWS información sobre los SDK, las herramientas y AWS las API, consulte la autenticación del IAM Identity Center en la Guía de referencia de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener información AWS sobre los SDK y las herramientas, consulte

¿Qué usuario necesita acceso programático?	Para	Mediante
		Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para ver AWS las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Prácticas recomendadas

Las mejores prácticas son recomendaciones que pueden ayudarle a utilizar AWS Certificate Manager (AWS Certificate Manager) de forma más eficaz. Las siguientes prácticas recomendadas se basan en experiencias reales de clientes de ACM actuales.

Temas

- Separación a nivel de cuenta
- AWS CloudFormation
- Asignación de certificados
- Validación del dominio
- Agregar o eliminar nombres de dominio
- Cancelación del registro de transparencia de certificados
- Encienda AWS CloudTrail

Separación a nivel de cuenta

Utilice la separación a nivel de cuenta en sus políticas para controlar quién puede acceder a los certificados a nivel de cuenta. Guarde sus certificados de producción en cuentas distintas a las de sus certificados de pruebas y desarrollo. Si no puedes usar la separación a nivel de cuenta, puedes restringir el acceso a funciones específicas negando cualquier `kms:CreateGrant` acción

en tus políticas. Esto limita los roles de una cuenta que pueden firmar certificados a un nivel superior. Para obtener información sobre las subvenciones, incluida la terminología sobre las subvenciones, consulte las subvenciones AWS KMS en la Guía para AWS Key Management Service desarrolladores.

Si desea un control más detallado que restringir el uso `kms:CreateGrant` por cuenta, puede limitarlo `kms:CreateGrant` a certificados específicos mediante las claves de EncryptionContext condición kms:. Especifique `arn:aws:acm` como clave y el valor del ARN que se va a restringir. El siguiente ejemplo de política impide el uso de un certificado específico, pero permite otros.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "VisualEditor0",
           "Effect": "Deny",
           "Action": "kms:CreateGrant",
           "Resource": "*",
           "Condition": {
               "StringEquals": {
                   "kms:EncryptionContext:aws:acm:arn": "arn:aws:acm:us-
east-1:111122223333:certificate/b26def74-1234-4321-9876-951d4c07b197"
               }
           }
       }
   ]
}
```

AWS CloudFormation

Con AWS CloudFormation él puede crear una plantilla que describa los AWS recursos que desea utilizar. AWS CloudFormation a continuación, aprovisiona y configura esos recursos por usted. AWS CloudFormation puede aprovisionar recursos compatibles con ACM, como Elastic Load Balancing CloudFront, Amazon y Amazon API Gateway. Para obtener más información, consulte Servicios integrados con AWS Certificate Manager.

Si suele AWS CloudFormation crear y eliminar rápidamente varios entornos de prueba, le recomendamos que no cree un certificado ACM independiente para cada entorno. Al hacerlo, se agotará rápidamente la cuota de certificados. Para obtener más información, consulte Cuotas. En su lugar, cree un certificado comodín que abarque todos los nombres de dominio que utilice para

las pruebas. Por ejemplo, si crea repetidamente certificados de ACM para nombres de dominio que varían en función solo de un número de versión, como `<version>.service.example.com`, cree un único certificado comodín para `<*>.service.example.com`. Incluya el certificado comodín en la plantilla que AWS CloudFormation utilice para crear el entorno de prueba.

Asignación de certificados

La fijación de certificados, en ocasiones denominada fijación de SSL, es un proceso que puede utilizar en su aplicación para validar un host remoto asociando dicho host directamente con su clave pública o certificado X.509 en lugar de hacerlo con una jerarquía de certificados. La aplicación, por tanto, utiliza la asignación para omitir la validación de la cadena de certificados SSL/TLS. El proceso de validación típico de SSL comprueba las firmas en toda la cadena de certificados del certificado de la entidad de certificación (CA) raíz hasta los certificados de CA subordinados, si hay alguno. También comprueba el certificado del host remoto en la parte inferior de la jerarquía. Su aplicación puede en su lugar asignar el certificado para el host remoto para indicar que solo dicho certificado y no el certificado raíz o cualquier otro de la cadena es de confianza. Puede añadir el certificado o la clave pública del host remoto a la aplicación durante el desarrollo. Asimismo, la aplicación puede añadir el certificado o clave cuando se conecta por primera vez al host.

> **Warning**
>
> Recomendamos que su aplicación no asigne un certificado de ACM. ACM realiza Renovación administrada para certificados de ACM para renovar de forma automática sus certificados SSL/TLS emitidos por Amazon antes de que venzan. Para renovar un certificado, ACM genera un nuevo par de claves pública y privada. Si su aplicación asigna el certificado de ACM y este se renueva correctamente con una nueva clave pública, es posible que la aplicación no se conecte al dominio.

Si decide fijar un certificado, las siguientes opciones no obstaculizan que su aplicación se conecte a su dominio:

- Importe su propio certificado a ACM y, a continuación, asigne la aplicación al certificado importado. ACM no intenta renovar de forma automática los certificados importados.
- Si utiliza un certificado público, fije su aplicación a todos los certificados raíz de Amazon disponibles. Si utiliza un certificado privado, fije su aplicación al certificado raíz de la CA.

Validación del dominio

Antes de que la autoridad de certificación (CA) de Amazon pueda emitir un certificado para tu sitio, AWS Certificate Manager (ACM) debe comprobar que eres el propietario o el control de todos los dominios que especificaste en tu solicitud. Puede realizar la verificación mediante el correo electrónico o DNS. Para obtener más información, consulte Validación por DNS y Validación por correo electrónico.

Agregar o eliminar nombres de dominio

No se pueden agregar ni eliminar nombres de dominio de un certificado de ACM existente. En su lugar, debe solicitar un certificado nuevo con la lista de nombres de dominio revisada. Por ejemplo, si el certificado tiene cinco nombres de dominio y desea añadir cuatro más, debe solicitar un certificado nuevo con los nueve nombres de dominio. Al igual que con cualquier certificado nuevo, debe validar la titularidad de todos los nombres de dominio de la solicitud, incluidos los que ya se habían validado para el certificado original.

Si utiliza la validación por correo electrónico, recibe hasta ocho mensajes de correo electrónico de validación para cada dominio, y deberá actuar sobre al menos uno de ellos en un plazo de 72 horas. Por ejemplo, si solicita un certificado con cinco nombres de dominio, recibirá hasta 40 mensajes de validación y deberá actuar sobre al menos cinco de ellos en un plazo de 72 horas. A medida que la cantidad de nombres de dominio de la solicitud de certificado aumente, aumentará también el trabajo necesario para validar la titularidad de los dominios mediante el correo electrónico.

Si en cambio utiliza la validación por DNS, solo debe escribir un nuevo registro de DNS en la base de datos para el FQDN que desea validar. ACM envía el registro que se debe crear y posteriormente consulta la base de datos para determinar si se ha agregado el registro. La inclusión del registro constata que usted es el propietario o controla el dominio. En el ejemplo anterior, si solicita un certificado con cinco nombres de dominio, debe crear cinco registros de DNS. Le recomendamos que utilice la validación por DNS cuando sea posible.

Cancelación del registro de transparencia de certificados

> **Important**
>
> Independientemente de las acciones que lleve a cabo para desactivar el registro de transparencia de certificados, el certificado aún puede ser registrado por cualquier cliente o persona que tenga acceso al punto de enlace público o privado al que vincula el certificado.

Sin embargo, el certificado no contendrá una marca temporal de certificado firmada (SCT). Solo la CA emisora puede integrar una SCT en un certificado.

Desde el 30 de abril de 2018, Google Chrome ya no confía en los certificados SSL/TLS públicos que no estén en un registro de transparencia de certificados. Por lo tanto, a partir del 24 de abril de 2018, la CA de Amazon comenzó a publicar todos los nuevos certificados y las renovaciones al menos en dos registros públicos. Una vez que un certificado se ha registrado, no se puede eliminar. Para obtener más información, consulte Registro de transparencia de certificados.

El registro se realiza automáticamente cuando se solicita o se renueva un certificado, pero puede optar por no hacerlo. Entre los motivos más comunes para hacerlo se incluyen las preocupaciones por la seguridad y privacidad. Por ejemplo, el registro de nombres de dominio de host internos ofrece a los posibles atacantes información sobre las redes internas que de otro modo no sería pública. Además, el registro podría filtrar los nombres de productos y sitios web nuevos o que todavía no se han publicado.

Para inhabilitar el registro de transparencia cuando solicite un certificado, utilice el `options` parámetro del AWS CLI comando request-certificate o la operación de la RequestCertificateAPI. Si su certificado se emitió antes del 24 de abril de 2018 y quiere asegurarse de que no se registre durante la renovación, puede usar el update-certificate-optionscomando o la operación de UpdateCertificateOptionsAPI para excluirlo.

Limitaciones

- No puede utilizar la consola para habilitar o desactivar el registro de transparencia.
- No puede cambiar el estado del registro después de que un certificado entra en su periodo de renovación, normalmente 60 días antes del vencimiento del certificado. No se generan mensajes de error si falla un cambio de estado.

Una vez que un certificado se ha registrado, no se puede eliminar del registro. En ese momento, la cancelación no tendrá ningún efecto. Si desactiva el registro al solicitar un certificado y después elige volver a activarlo, el certificado no se registrará hasta que no se renueve. Si desea que el certificado se registre inmediatamente, le recomendamos que emita uno nuevo.

En el siguiente ejemplo se muestra cómo utilizar el comando request-certificate para deshabilitar la transparencia del certificado cuando se solicita un certificado nuevo.

```
aws acm request-certificate \
--domain-name www.example.com \
--validation-method DNS \
--options CertificateTransparencyLoggingPreference=DISABLED \
```

El comando anterior muestra el ARN del nuevo certificado.

```
{
    "CertificateArn": "arn:aws:acm:region:account:certificate/certificate_ID"
}
```

Si ya tiene un certificado y no quiere que se registre cuando se renueve, utilice el update-certificate-optionscomando. Este comando no devuelve ningún valor.

```
aws acm update-certificate-options \
--certificate-arn arn:aws:acm:region:account:\
certificate/certificate_ID \
--options CertificateTransparencyLoggingPreference=DISABLED
```

Encienda AWS CloudTrail

Active el CloudTrail registro antes de empezar a usar ACM. CloudTrail le permite supervisar sus AWS despliegues recuperando un historial de las llamadas a las AWS API de su cuenta, incluidas las llamadas a las API realizadas a través de la consola de AWS administración, los AWS SDK y los Amazon Web AWS Command Line Interface Services de nivel superior. También puede identificar qué usuarios y cuentas llamaron a las API de ACM, la dirección IP de origen desde la que se realizaron las llamadas así como el momento en que se efectuaron. Puede CloudTrail integrarlas en las aplicaciones mediante la API, automatizar la creación de rutas para su organización, comprobar el estado de las rutas y controlar la forma en que los administradores activan y desactivan el inicio de CloudTrail sesión. Para obtener más información, consulte Crear un registro de seguimiento. Vaya a Utilizándolo con CloudTrail AWS Certificate Manager a fin de consultar ejemplos de registros de seguimiento para acciones de ACM.

Configuración

Con AWS Certificate Manager (ACM), puede aprovisionar y administrar los certificados SSL/TLS para sus sitios web y aplicaciones basados. AWS Puede utilizar ACM; para crear o importar un certificado y luego administrarlo. Debe usar otros AWS servicios para implementar el certificado en su sitio web o aplicación. Para obtener más información sobre los servicios integrados con ACM, consulte Servicios integrados con AWS Certificate Manager. En las siguientes secciones se tratan los pasos necesarios para poder utilizar ACM.

Temas

Inscríbase en un Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Registrar un nombre de dominio

Un nombre de dominio completo (FQDN) es el nombre único de una organización o individuo en Internet, seguido de una extensión de dominio de nivel superior como, por ejemplo, .com o .org. Si aún no tiene un nombre de dominio registrado, puede registrar uno a través de Amazon Route 53 o cualquier otro registrador comercial. Lo normal es dirigirse al sitio web del registrador y solicitar un nombre de dominio. El registrador consulta WHOIS para determinar si el FQDN solicitado está disponible. Si lo está, el registrador suele enumerar los nombres relacionados cuyas extensiones de dominio difieran y ofrece la oportunidad de adquirir cualquiera de los disponibles. El registro suele durar un periodo determinado antes su renovación como, por ejemplo, uno o dos años.

Para obtener más información sobre el registro de nombres de dominio con Amazon Route 53, consulte Registro de nombres de dominio mediante Amazon Route 53 en la Guía del desarrollador de Amazon Route 53.

(Opcional) Configuración del correo electrónico para el dominio

> **Note**
>
> Los siguientes pasos solo son necesarios si utiliza la validación por correo electrónico para constatar que usted es el propietario del FQDN (nombre de dominio completo) que ha especificado en su solicitud de certificado, o bien que es quien lo controla. Antes de emitir un certificado, ACM requiere que valide que es el propietario del dominio o bien que lo controla. Puede utilizar la validación por correo electrónico o la validación por DNS. Para obtener

más información sobre la validación por correo electrónico, consulte Validación por correo electrónico.

Si no puede editar su configuración de DNS, recomendamos que utilice la validación de dominios de DNS en lugar de la validación por correo electrónico. La validación por DNS elimina la necesidad de configurar el correo electrónico para el nombre de dominio. Para obtener más información sobre la validación por DNS, consulte Validación por DNS.

Base de datos WHOIS

La base de datos WHOIS contiene la información de contacto del dominio. Para validar su identidad, ACM envía un correo electrónico a las siguientes tres direcciones en WHOIS. Debe asegurarse de que su información de contacto es pública o que el correo electrónico que se envía a una dirección oculta se reenvía a su dirección de correo electrónico real.

- Titularidad del dominio
- Contacto técnico
- Contacto administrativo

(Opcional) Configuración de un registro de CAA

Si lo desea, puede configurar un registro DNS de autorización de la autoridad de certificación (CAA) para especificar que AWS Certificate Manager (ACM) puede emitir un certificado para su dominio o subdominio. Después de validar el dominio, ACM verifica la presencia de un registro de CAA para asegurarse de que puede emitir un certificado para usted. Puede elegir no configurar ningún registro de CAA para su dominio si no desea habilitar la comprobación de CAA.

Un registro de CAA contiene los siguientes campos de datos:

flags

Especifica si ACM admite el valor del campo tag (etiqueta). Establezca este valor en 0.

etiqueta

El campo tag puede tener uno de los siguientes valores. Tenga en cuenta que el campo iodef se omite actualmente.

issue

Indica que la CA de ACM especificada en el campovalue (valor) tiene autorización para emitir un certificado para su dominio o subdominio.

issuewild

Indica que la CA de ACM; especificada en el campovalue (valor) tiene autorización para emitir un certificado comodín para su dominio o subdominio. Un certificado comodín se aplica al dominio o subdominio y a todos sus subdominios.

value

El valor de este campo depende del valor del campo tag. Debe incluir este valor entre comillas ("").

Cuando tag es issue

El campo value contiene el nombre de dominio de la CA. Este campo puede contener el nombre de una CA que no sea una CA de Amazon. Sin embargo, si no dispone de un registro de CAA que especifique una de las siguientes cuatro CA de Amazon, ACM no puede emitir un certificado para su dominio o subdominio:

- amazon.com
- amazontrust.com
- awstrust.com
- amazonaws.com

El campo value también puede contener un punto y coma (;) para indicar que no se debe permitir a la CA emitir un certificado para su dominio o subdominio. Utilice este campo si en algún momento decide que ya no desea que se le emita un certificado para un dominio determinado.

Cuando tag es issuewild

El campo value es igual que cuando tag es issue salvo que el valor se aplica a los certificados comodín.

Cuando hay un registro de CAA issuewild que no incluye ningún valor CA de ACM, ACM no puede emitir ningún comodín. Si no hay ningún registro issuewild, pero sí un registro issue de CAA para ACM, ACM puede emitir los comodines.

Example Ejemplos de registros de CAA

En los siguientes ejemplos, su nombre de dominio aparece primero seguido del tipo de registro (CAA). El campo flags siempre es 0. El campo tags puede ser issue o issuewild. Si el campo es issue y escribe el nombre de dominio de un servidor de CA en el campo value, el registro de CAA indica que el servidor especificado tiene permiso para emitir el certificado solicitado. Si escribe un punto y coma ";" en el campo value, el registro de CAA indica que ninguna CA tiene permiso para emitir un certificado. La configuración de los registros de CAA varía en función del proveedor de DNS.

```
Domain       Record type  Flags  Tag      Value
example.com.   CAA            0        issue      "SomeCA.com"
```

```
Domain       Record type  Flags  Tag      Value
example.com.   CAA            0        issue      "amazon.com"
```

```
Domain       Record type  Flags  Tag      Value
example.com.   CAA            0        issue      "amazontrust.com"
```

```
Domain       Record type  Flags  Tag      Value
example.com.   CAA            0        issue      "awstrust.com"
```

```
Domain       Record type  Flags  Tag      Value
example.com.   CAA            0        issue      "amazonaws.com"
```

```
Domain       Record type  Flags  Tag      Value
example.com    CAA            0        issue      ";"
```

Para obtener más información sobre cómo agregar o modificar registros de DNS, contacte con el proveedor de DNS. Route 53 admite registros de CAA. Si Route 53 es su proveedor de DNS, consulte Formato de CAA para obtener más información sobre la creación de un registro.

Emisión y administración de certificados

Los certificados de ACM se pueden utilizar para establecer comunicaciones seguras a través de Internet o de una red interna. Puede solicitar un certificado de confianza pública directamente a ACM (un “certificado de ACM”) o importar un certificado de confianza pública emitido por un tercero. También se admiten certificados autofirmados. Para aprovisionar la PKI interna de su organización, puede emitir certificados de ACM firmados por una entidad de certificación privada (CA) creada y administrada por Autoridad de certificación privada de AWS. La CA puede residir en su cuenta o compartirse con usted desde otra cuenta.

> **Note**
>
> Los certificados de ACM públicos se pueden instalar en instancias de Amazon EC2 conectadas a un Nitro Enclave, pero no a otras instancias de Amazon EC2. Para obtener información sobre la configuración de un servidor web independiente en una instancia de Amazon EC2 no conectada a un Nitro Enclave, consulte Tutorial: Install a LAMP web server on Amazon Linux 2 o Tutorial: Install a LAMP web server with the Amazon Linux AMI.

> **Note**
>
> Dado que los certificados firmados por una CA privada no son de confianza de forma predeterminada, los administradores deben instalarlos en los almacenes de confianza del cliente.

Para empezar a emitir certificados, inicie sesión en la consola AWS de administración y abra la consola ACM en https://console.aws.amazon.com/acm/home. Si aparece la página de introducción, elija Get Started (Comenzar). De lo contrario, elija Certificate Manager o Private CAs (CA privadas) en el panel de navegación izquierdo.

Temas

- Descripción de certificados de ACM
- Eliminar certificados administrados por ACM
- Instalar certificados de ACM

Solicitar un certificado público

En las siguientes secciones, se explica cómo utilizar la consola de ACM o AWS CLI cómo solicitar un certificado de ACM público. Después de solicitar un certificado público, debe realizar uno de los procedimientos descritos en Validación de la propiedad del dominio.

Los certificados de ACM privados siguen el estándar X.509 y están sujetos a las siguientes restricciones:

- Nombres: se deben utilizar nombres de asunto que cumplan con el DNS. Para obtener más información, consulte Nombres de dominio.
- Algoritmo: para el cifrado, el algoritmo de clave privada del certificado debe ser RSA de 2048 bits, ECDSA de 256 bits o ECDSA de 384 bits.
- Vencimiento: cada certificado tiene una validez de 13 meses (395 días).
- Renovación: ACM intenta renovar un certificado privado automáticamente después de 11 meses.

Si tiene problemas al solicitar un certificado, consulte Solución de problemas de solicitudes de certificados.

Para solicitar un certificado para una PKI privada mediante Autoridad de certificación privada de AWS, consulte. Solicitud de un certificado PKI privado

> **Note**
>
> Los administradores pueden utilizar las Políticas de clave condicional de ACM para controlar la forma en que los usuarios finales emiten certificados nuevos. Estas claves condicionales permiten imponer restricciones a los dominios, los métodos de validación y los demás atributos relacionados con una solicitud de certificado.

> **Note**
>
> A menos que elija desactivarlos, los certificados ACM de confianza pública se registrarán automáticamente al menos en dos bases de datos de transparencia de los certificados. Actualmente no puede utilizar la consola para desactivarlo. Debe usar la API AWS CLI o ACM. Para obtener más información, consulte Cancelación del registro de transparencia de certificados. Para obtener información general sobre los registros de transparencia, consulte Registro de transparencia de certificados.

Temas

Solicitar un certificado público mediante la consola

Para solicitar un certificado público de ACM (consola)

1. Inicie sesión en la consola AWS de administración y abra la consola ACM en https://console.aws.amazon.com/acm/home.

   Elija Request a certificate (Solicitar un certificado).
2. En la sección Domain names (Nombres de dominio) escriba el nombre de dominio.

   Puede utilizar un nombre de dominio completo (FQDN), tal como **`www.example.com`**, o un nombre de dominio desnudo o ápex, tal como **`example.com`**. También puede utilizar un asterisco (**`*`**) como comodín en la posición más a la izquierda para proteger varios nombres de sitio del mismo dominio. Por ejemplo, **`*.example.com`** protege a **`corp.example.com`** y a **`images.example.com`**. El nombre comodín aparecerá en el campo Subject (Sujeto) y en la extensión Subject Alternative Name (Nombre alternativo de sujeto) del certificado de ACM.

   Cuando solicita un certificado de comodín, el asterisco (**`*`**) debe encontrarse en la posición más a la izquierda del nombre de dominio y solo puede proteger un nivel de subdominio. Por ejemplo, **`*.example.com`** puede proteger a **`login.example.com`** y a **`test.example.com`**, pero no puede proteger a **`test.login.example.com`**. Tenga en cuenta también que **`*.example.com`** solo protege los subdominios de **`example.com`**. No protege el dominio desnudo o ápex (**`example.com`**). Para proteger ambos, consulte el siguiente paso.

> **Note**
>
> En conformidad con RFC 5280, la longitud del nombre de dominio (técnicamente, el nombre común) que ingrese en este paso no puede superar los 64 octetos (caracteres), incluidos los puntos. Cada nombre alternativo de sujeto (SAN) posterior que proporcione, como en el siguiente paso, puede tener una longitud de hasta 253 octetos.

Para agregar otro nombre, elija Add another name to this certificate (Agregar otro nombre a este certificado) y escriba el nombre en el cuadro de texto. Esto resulta útil para proteger tanto los dominios desnudos como los ápex (por ejemplo, **`example.com`**) y sus subdominios (por ejemplo, **`*.example.com`**).

3. En la sección Validation method (Método de validación) elija DNS validation (Validación DNS) (opción recomendada) o Email validation (Validación por correo electrónico), según sus necesidades.

> **Note**
>
> Si no puede editar su configuración de DNS, recomendamos que utilice la validación de dominios de DNS en lugar de la validación por correo electrónico. La validación por DNS presenta varios beneficios con respecto a la validación por correo electrónico. Consulte Validación por DNS.

Antes de que ACM emita un certificado, valida que usted es el propietario o controla los nombres de dominio incluidos en la solicitud de certificado. Puede utilizar la validación por correo electrónico o la validación por DNS.

Si elige la validación por correo electrónico, ACM envía un correo electrónico de validación a tres direcciones de contacto registradas en la base de datos WHOIS y hasta cinco direcciones comunes de administración del sistema para cada nombre de dominio. Usted o un representante autorizado debe responder a uno de estos mensajes de correo electrónico. Para obtener más información, consulte Validación por correo electrónico.

Si utiliza la validación por DNS, solo tiene que agregar un registro CNAME proporcionado por ACM en la configuración de DNS. Para obtener más información sobre la validación por DNS, consulte Validación por DNS.

4. En la sección Key algorithm (Algoritmos clave), elija uno de los tres algoritmos disponibles:

   - RSA 2048 (predeterminado)
   - ECDSA P 256
   - ECDSA P 384

   Para obtener información que le ayude a elegir un algoritmo, consulte Algormos clave la entrada del AWS blog Cómo evaluar y utilizar los certificados ECDSA en. AWS Certificate Manager

5. En la página Tags (Etiquetas), puede etiquetar el certificado si así lo desea. Las etiquetas son pares clave-valor que sirven como metadatos para identificar y organizar los recursos. AWS Para obtener una lista de los parámetros de etiquetas de ACM e instrucciones sobre cómo agregar etiquetas a los certificados después de su creación, consulte Etiquetar certificados de AWS Certificate Manager.

   Cuando termine de agregar etiquetas, elija Request (Solicitar).

6. Una vez procesada la solicitud, la consola regresa a la lista de certificados, donde se muestra la información sobre el nuevo certificado.

   Un certificado recibe el estado Pending validation (Validación pendiente) al solicitarse, a menos que falle por alguno de los motivos expuestos en el tema de solución de problemas Error en la solicitud de certificado. ACM intenta repetidamente validar un certificado durante 72 horas y, a continuación, se agota el tiempo de espera. Si un certificado muestra el estado Error o Validation timed out (Tiempo de espera de validación agotado), elimine la solicitud, corrija el problema con Validación por DNS o Validación por correo electrónico e inténtelo de nuevo. Si se supera la validación, el certificado recibe el estado Issued (Emitido).

   > **Note**
   >
   > Según cómo haya ordenado la lista, es posible que un certificado que esté buscando no esté visible de inmediato. Puede hacer clic en el triángulo negro de la derecha para cambiar el orden. También puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha.

Solicitar un certificado público mediante la CLI

Utilice el comando request-certificate para solicitar un nuevo certificado público de ACM en la línea de comandos. Los valores opcionales del método de validación son DNS y EMAIL (Correo electrónico). Los valores opcionales del algoritmo clave son RSA_2048 (el predeterminado si el parámetro no se proporciona explícitamente), EC_prime256v1 y EC_secp384r1.

```
aws acm request-certificate \
--domain-name www.example.com \
--key-algorithm EC_Prime256v1 \
--validation-method DNS \
--idempotency-token 1234 \
--options CertificateTransparencyLoggingPreference=DISABLED
```

Este comando devuelve el nombre de recurso de Amazon (ARN) del nuevo certificado público.

```
{
    "CertificateArn": "arn:aws:acm:Region:444455556666:certificate/certificate_ID"
}
```

Solicitud de un certificado PKI privado

Si tiene acceso a una CA privada existente creada por Autoridad de certificación privada de AWS, ACM puede solicitar un certificado adecuado para su uso en su PKI privada. La CA puede residir en su cuenta o compartirse con usted desde otra cuenta. Para obtener información sobre la creación de una CA privada, consulte el artículo Crear Private Certificate Authority.

De manera predeterminada, no se confía en los certificados firmados por una CA privada, y ACM no admite ningún tipo de validación para ellos. En consecuencia, un administrador debe tomar medidas para instalarlos en los almacenes de confianza de los clientes de su organización.

Los certificados de ACM privados siguen el estándar X.509 y están sujetos a las siguientes restricciones:

- Nombres: se deben utilizar nombres de asunto que cumplan con el DNS. Para obtener más información, consulte Nombres de dominio.
- Algoritmo: para el cifrado, el algoritmo de clave privada del certificado debe ser RSA de 2048 bits, ECDSA de 256 bits o ECDSA de 384 bits.

> **Note**
>
> La familia de algoritmos de firma especificada (RSA o ECDSA) debe coincidir con la familia de algoritmos de la clave secreta de la entidad de certificación.

- Vencimiento: cada certificado tiene una validez de 13 meses (395 días). La fecha de finalización del certificado de la CA de firma debe ser posterior a la fecha de finalización del certificado solicitado, ya que, de lo contrario, la solicitud del certificado producirá un error.
- Renovación: ACM intenta renovar un certificado privado automáticamente después de 11 meses.

La CA privada utilizada para firmar los certificados de entidad final está sujeta a sus propias restricciones:

- La CA debe tener el estado de Activa.
- El algoritmo de clave privada de la CA debe ser RSA 2048 o RSA 4096.

> **Note**
>
> A diferencia de los certificados de confianza pública, los certificados firmados por una CA privada no requieren validación.

Temas

Configurar el acceso a una CA privada

Puede utilizar Autoridad de certificación privada de AWS para firmar sus certificados de ACM en cualquiera de estos dos casos:

- Cuenta única: la CA firmante y el certificado ACM emitido residen en la misma AWS cuenta.

Para permitir la emisión y las renovaciones de una única cuenta, el administrador de Autoridad de certificación privada de AWS debe conceder permiso a la entidad principal del servicio de ACM para crear, recuperar y enumerar certificados. Esto se hace mediante la acción de la Autoridad de certificación privada de AWS API CreatePermissiono el AWS CLI comando create-permission. El propietario de la cuenta asigna estos permisos a un usuario, grupo o rol de IAM responsable de emitir certificados.

- Cuenta cruzada: la CA firmante y el certificado ACM que se emite residen en AWS cuentas diferentes, y el acceso a la CA se ha concedido a la cuenta en la que reside el certificado.

  Para permitir la emisión y renovación entre cuentas, el Autoridad de certificación privada de AWS administrador debe adjuntar a la CA una política basada en recursos mediante la acción de la Autoridad de certificación privada de AWS API o el comando put-policy. PutPolicyAWS CLI La política especifica las entidades principales de otras cuentas a las que se permite el acceso limitado a la CA. Para obtener más información, consulte Utilización de una política con base en recursos con ACM Private CA.

  El escenario entre cuentas también requiere que ACM configure un rol vinculado a servicios (SLR) para interactuar como entidad principal con la política de PCA. ACM crea el SLR automáticamente mientras emite el primer certificado.

  ACM podría avisarle que no puede determinar si existe un SLR en su cuenta. Si ya se ha concedido el permiso `iam:GetRole` necesario al SLR de ACM para su cuenta, el aviso no se repetirá después de crearse el SLR. Si se repite, es posible que usted o el administrador de su cuenta tengan que conceder el permiso `iam:GetRole` a ACM o asociar la cuenta a la política `AWSCertificateManagerFullAccess` administrada por ACM.

  Para obtener más información, consulte Utilización de un rol vinculado a servicios con ACM.

> **Important**
>
> Su certificado ACM debe estar asociado activamente a un AWS servicio compatible para que pueda renovarse automáticamente. Para obtener información sobre los recursos que admite ACM, consulte Servicios integrados con AWS Certificate Manager.

Solicitar un certificado PKI privado mediante la consola de ACM

1. Inicie sesión en la consola AWS de administración y abra la consola ACM en https://console.aws.amazon.com/acm/home.

   Elija Request a certificate (Solicitar un certificado).
2. En la página Request certificate (Solicitar certificado), elija Request a private certificate (Solicitar un certificado privado) y Next (Siguiente) para continuar.
3. En la sección Certificate authority details (Detalles de la entidad de certificación), haga clic en el menú Certificate authority (Entidad de certificación) y elija una de las CA privadas disponibles. Si la CA se comparte desde otra cuenta, el ARN aparece precedido por la información de propiedad.

   Se muestran detalles sobre la CA para ayudarlo a verificar que haya elegido la correcta:

   - Propietario
   - Tipo
   - Nombre común (NC)
   - Organización (O)
   - Unidad organizativa (UO)
   - Nombre del país (C)
   - Estado o provincia
   - Nombre de la localidad
4. En la sección Domain names (Nombres de dominio) escriba el nombre de dominio. Puede utilizar un nombre de dominio completo (FQDN), tal como **`www.example.com`**, o un nombre de dominio desnudo o ápex, tal como **`example.com`**. También puede utilizar un asterisco (**`*`**) como comodín en la posición más a la izquierda para proteger varios nombres de sitio del mismo dominio. Por ejemplo, **`*.example.com`** protege a **`corp.example.com`** y a **`images.example.com`**. El nombre comodín aparecerá en el campo Subject (Sujeto) y en la extensión Subject Alternative Name (Nombre alternativo de sujeto) del certificado de ACM.

   > **Note**
   >
   > Cuando solicita un certificado de comodín, el asterisco (**`*`**) debe encontrarse en la posición más a la izquierda del nombre de dominio y solo puede proteger un nivel de subdominio. Por ejemplo, **`*.example.com`** puede proteger a **`login.example.com`**

y a **test.example.com**, pero no puede proteger a **test.login.example.com**. Tenga en cuenta también que ***.example.com** solo protege los subdominios de **example.com**. No protege el dominio desnudo o ápex (**example.com**). Para proteger ambos, consulte el siguiente paso

De manera opcional, elija Add another name to this certificate (Agregar otro nombre a este certificado) y escriba el nombre en el cuadro de texto. Esto resulta útil para autenticar tanto los dominios desnudos como los ápex (por ejemplo, **example.com**) y sus subdominios (por ejemplo, ***.example.com**).

5. En la sección Key algorithm (Algoritmos clave), elija uno de los tres algoritmos disponibles:

   - RSA 2048 (predeterminado)
   - ECDSA P 256
   - ECDSA P 384

   Para obtener información que le ayude a elegir un algoritmo, consulteAlgormos clave.

6. En la sección Tags (Etiquetas), puede etiquetar el certificado si así lo desea. Las etiquetas son pares clave-valor que sirven como metadatos para identificar y organizar los recursos. AWS Para obtener una lista de los parámetros de etiquetas de ACM e instrucciones sobre cómo agregar etiquetas a los certificados después de su creación, consulte Etiquetar certificados de AWS Certificate Manager.

7. En la sección Certificate renewal permissions (Permisos de renovación de certificados), confirme el aviso sobre los permisos de renovación de certificados. Estos permisos permiten la renovación automática de los certificados PKI privados que firma con la CA seleccionada. Para obtener más información, consulte Utilización de un rol vinculado a servicios con ACM.

8. Después de proporcionar toda la información requerida, elija Request (Solicitar). La consola regresa a la lista de certificados, donde puede ver el nuevo certificado.

> **Note**
>
> Según cómo haya ordenado la lista, es posible que un certificado que esté buscando no esté visible de inmediato. Puede hacer clic en el triángulo negro de la derecha para cambiar el orden. También puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha.

Solicitar un certificado PKI privado mediante la CLI

Utilice el comando request-certificate para solicitar un certificado privado en ACM.

> **Note**
>
> Al solicitar un certificado de PKI privado firmado por una CA AWS Private CA, la familia de algoritmos de firma especificada (RSA o ECDSA) debe coincidir con la familia de algoritmos de la clave secreta de la CA.

```
aws acm request-certificate \
--domain-name www.example.com \
--idempotency-token 12563 \
--certificate-authority-arn arn:aws:acm-pca:Region:444455556666:\
certificate-authority/CA_ID
```

Este comando devuelve el nombre de recurso de Amazon (ARN) del certificado privado nuevo.

```
{
    "CertificateArn": "arn:aws:acm:Region:444455556666:certificate/certificate_ID"
}
```

En la mayoría de los casos, ACM adjunta automáticamente un rol vinculado a servicios (SLR) a la cuenta la primera vez que utiliza una CA compartida. El SLR habilita la renovación automática de los certificados de la entidad final emitida. Para comprobar si el SLR está presente, puede consultar IAM con el siguiente comando:

```
aws iam get-role --role-name AWSServiceRoleForCertificateManager
```

Si el SLR está presente, el resultado del comando debe tener el siguiente aspecto:

```
{
   "Role":{
      "Path":"/aws-service-role/acm.amazonaws.com/",
      "RoleName":"AWSServiceRoleForCertificateManager",
      "RoleId":"AAAAAAA0000000BBBBBBB",
      "Arn":"arn:aws:iam::{account_no}:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager",
```

```
      "CreateDate":"2020-08-01T23:10:41Z",
      "AssumeRolePolicyDocument":{
         "Version":"2012-10-17",
         "Statement":[
            {
               "Effect":"Allow",
               "Principal":{
                  "Service":"acm.amazonaws.com"
               },
               "Action":"sts:AssumeRole"
            }
         ]
      },
      "Description":"SLR for ACM Service for accessing cross-account Private CA",
      "MaxSessionDuration":3600,
      "RoleLastUsed":{
         "LastUsedDate":"2020-08-01T23:11:04Z",
         "Region":"ap-southeast-1"
      }
   }
}
```

Si falta el SLR, consulte Utilización de un rol vinculado a servicios con ACM.

Validación de la propiedad del dominio

A fin de que la entidad de certificación (CA) de Amazon pueda emitir un certificado para el sitio, AWS Certificate Manager (ACM) debe verificar que usted es el propietario de todos los nombres de dominio que ha especificado en la solicitud, o bien que es quien los controla. Puede optar por demostrar que es propietario con la validación del Sistema de nombres de dominio (DNS) o con la validación por correo electrónico en el momento en que solicita un certificado.

> **Note**
>
> La validación solo se aplica a los certificados de confianza pública emitidos por ACM. ACM no valida la propiedad del dominio para certificados importados o para certificados firmados por una CA privada. ACM no puede validar los recursos de una zona alojada privada de Amazon VPC o cualquier otro dominio privado. Para obtener más información, consulte Solución de problemas de validación de certificados.

En general, se recomienda utilizar la validación por DNS sobre la validación por correo electrónico debido a las siguientes razones:

- Si utiliza Amazon Route 53 para administrar sus registros de DNS públicos, puede actualizar los registros directamente a través de ACM.
- ACM renueva automáticamente los certificados validados por DNS, siempre y cuando el certificado esté en uso y el registro de DNS siga existiendo.
- Para renovar los certificados validados por correo electrónico, el propietario del dominio debe realizar una acción. ACM comienza a enviar avisos de renovación 45 días antes de su vencimiento. Estos avisos van a las direcciones del buzón de correo WHOIS del dominio y hasta cinco direcciones de administrador comunes. Las notificaciones contienen un enlace que el propietario del dominio puede presionar para facilitar la renovación. Una vez validados todos los dominios enumerados, ACM emite un certificado renovado con el mismo ARN.

Si no tiene autorización para editar la base de datos de DNS del dominio, debe utilizar la validación por correo electrónico en su lugar.

> **Note**
>
> Después de crear un certificado con validación por correo electrónico, no puede cambiar a la validación mediante DNS.

Temas

- Validación por DNS
- Validación por correo electrónico

Validación por DNS

El sistema de nombres de dominio (DNS) es un servicio de directorio para los recursos conectados a una red. Su proveedor de DNS mantiene una base de datos que contiene registros que definen el dominio. Cuando elige la validación por DNS, ACM proporciona uno o varios registros CNAME que deben agregarse a esta base de datos. Estos registros contienen un par de valor de clave único que sirve como prueba de que usted controla el dominio.

> **Note**
>
> Después de crear un certificado con validación por correo electrónico, no puede cambiar a la validación mediante DNS.

Por ejemplo, si solicita un certificado para el dominio `example.com` con `www.example.com` como nombre adicional, ACM crea dos registros CNAME. Cada registro, creado específicamente para el dominio y la cuenta, contiene un nombre y un valor. El valor es un alias que apunta a un AWS dominio que ACM utiliza para renovar automáticamente el certificado. Los registros CNAME se deben agregar a la base de datos de DNS una sola vez. ACM renueva automáticamente el certificado, siempre y cuando esté en uso y el registro CNAME siga existiendo.

> **Important**
>
> Si no utiliza Amazon Route 53 para administrar los registros de DNS públicos, contacte a su proveedor de DNS para saber cómo agregar registros. Si no tiene autoridad para editar la base de datos de DNS del dominio, debe utilizar la validación por correo electrónico.

Sin necesidad de repetir la validación, puede solicitar certificados de ACM adicionales para el nombre de dominio completo (FQDN) mientras el registro CNAME siga existiendo. Es decir, puede crear certificados de reemplazo que tengan el mismo nombre de dominio o certificados que cubran diferentes subdominios. Como el token de validación CNAME funciona en cualquier AWS región, puedes volver a crear el mismo certificado en varias regiones. También puede reemplazar un certificado eliminado.

Para detener la renovación automática, puede eliminar el certificado del servicio de AWS con el que está asociado o eliminar el registro CNAME. Si Route 53 no es su proveedor de DNS, contacte a su proveedor para saber cómo eliminar un registro. Si Route 53 es su proveedor, consulte Eliminación de conjuntos de registro de recursos en la Guía del desarrollador de Route 53. Para obtener más información sobre la renovación de certificados administrados, consulte Renovación administrada para certificados de ACM.

> **Note**
>
> La resolución CNAME fallará si hay más de cinco CNAME encadenados en la configuración de DNS. Si necesita un encadenamiento más largo, recomendamos utilizar la validación por correo electrónico.

Cómo funcionan los registros CNAME de ACM

> **Note**
>
> Esta sección es para los clientes que no utilizan Route 53 como su proveedor de DNS.

Si no utiliza Route 53 como proveedor de DNS, debe introducir de forma manual los registros CNAME proporcionados por ACM en la base de datos del proveedor, normalmente a través de un sitio web. Los registros CNAME se utilizan para una serie de propósitos, incluidos los mecanismos de redirección y contenedores para metadatos específicos del proveedor. En el caso de ACM, estos registros permiten la validación inicial de la propiedad del dominio y la renovación automática de certificados en curso.

En la siguiente tabla, se muestran ejemplos de registros CNAME para seis nombres de dominio. Cada par de Nombre-Valor del registro sirve para autenticar la propiedad del nombre de dominio.

En la tabla, tenga en cuenta que los dos primeros pares de Nombre-Valor del registro son iguales. Esto ilustra que, para un dominio comodín, como `*.example.com`, las cadenas creadas por ACM son las mismas que las creadas para su dominio base, `example.com`. De lo contrario, el par de Nombre y Valor difiere para cada nombre de dominio.

Registros CNAME de ejemplo

Nombre del dominio	Nombre del registro	Valor del registro	Comentario
*.example.com	*_x1*.example.com.	*_x2*.acm-validations.aws.	Idéntico
example.com	*_x1*.example.com.	*_x2*.acm-validations.aws.	

Nombre del dominio	Nombre del registro	Valor del registro	Comentario
www.example.com	*_x3*.www.example.com.	*_x4*.acm-validations.aws.	Único
host.example.com	*_x5*.host.example.com.	*_x6*.acm-validations.aws.	Único
subdomain.example.com	*_x7*.subdomain.example.com.	*_x8*.acm-validations.aws.	Único
host.subdomain.example.com	*_x9*.host.subdomain.example.com.	*_x10*.acm-validations.aws.	Único

Los valores *xN* después del carácter guion bajo (_) son cadenas largas generadas por ACM. Por ejemplo,

```
_3639ac514e785e898d2646601fa951d5.example.com.
```

es representativo de un Nombre de registro generado. El Valor de registro asociado podría ser

```
_98d2646601fa951d53639ac514e785e8.acm-validation.aws.
```

para el mismo registro.

> **Note**
>
> Si su proveedor de DNS no admite valores de CNAME con caracteres de guion bajo iniciales, consulte Solución de problemas de validación con DNS.

Cuando solicita un certificado y especifica la validación por DNS, ACM proporciona información CNAME en el siguiente formato:

Nombre del dominio	Nombre del registro	Tipo del registro	Valor del registro
example.com	_a79865eb4cd1a6ab990a45779b4e0b96.example.com.	CNAME	_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.

El Nombre del dominio es el FQDN asociado al certificado. El Nombre del registro identifica el registro de forma única y sirve como la clave del par de valor de clave. El Valor del registro sirve como el valor del par de valor de clave.

Estos tres valores (Nombre de dominio, Nombre de registro y Valor de registro) deben ingresarse en los campos apropiados de la interfaz web del proveedor de DNS para agregar registros de DNS. Los proveedores no manejan del mismo modo el campo de nombre de registro (o simplemente "nombre"). En algunos casos, se espera que proporcione toda la cadena como se muestra arriba. Otros proveedores agregan automáticamente el nombre de dominio a cualquier cadena que ingrese, lo que significa (en este ejemplo) que solo debe ingresar

```
_a79865eb4cd1a6ab990a45779b4e0b96
```

en el campo de nombre. Si la entrada es incorrecta e ingresa un nombre de registro que contiene un nombre de dominio (como *.example.com*), es posible que el resultado sea el siguiente:

```
_a79865eb4cd1a6ab990a45779b4e0b96.example.com.example.com.
```

La validación fallará en este caso. Por eso, debe intentar determinar de antemano qué tipo de entrada espera su proveedor.

Configuración de la validación por DNS

En esta sección se describe cómo configurar un certificado público para usar la validación de DNS.

Para configurar la validación por DNS en la consola

> **Note**
>
> Este procedimiento supone que ya has creado al menos un certificado y que estás trabajando en la AWS región en la que lo creaste. Si intenta abrir la consola y aparece en su lugar la pantalla de primer uso, o consigue abrir la consola y no ve su certificado en la lista, confirme que ha especificado la región correcta.

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/.
2. En la lista de certificados, elija la ID de certificado de un certificado con estado Pending validation (Pendiente de validación) que desea configurar. Se abre una página de detalles del certificado.
3. En la sección Domains (Dominios), realice uno de los dos procedimientos siguientes:

   a. (Opcional) Validar con Route 53.

   Aparece el botón Create records in Route 53 (Crear registros en Route 53) si se cumplen las siguientes condiciones:

   - Utiliza Route 53 como el proveedor de DNS.
   - Tiene permiso para escribir en la zona alojada por Route 53.
   - Su FQDN aún no se ha validado.

   > **Note**
   >
   > Si utiliza Route 53, pero no se encuentra el ícono Crear registro en Route 53 o está desactivado, consulte La consola de ACM no muestra el botón “Crear registro en Route 53”.

   Elija el icono Create records in Route 53 (Crear registros en Route 53) y, a continuación, elija Create records (Crear registros). La página Certificate status (Estado del certificado) debería abrirse con un informe de banner de estado Successfully created DNS records (Registros DNS creados correctamente).

El nuevo certificado podría continuar mostrando un estado de Pending validation (Validación pendiente) durante un máximo de 30 minutos.

> **Tip**
>
> No puede solicitar mediante programación que ACM cree automáticamente su registro en Route 53. Sin embargo, puede realizar una llamada a la API de Route 53 AWS CLI o a la API para crear el registro en la base de datos DNS de Route 53. Para obtener más información sobre los conjuntos de registros de Route 53, consulte Trabajar con conjuntos de registros de recursos.

b. (Opcional) Si no utiliza Route 53 como proveedor de DNS, debe recuperar la información CNAME y agregarla a la base de datos de DNS. En la página de detalles del nuevo certificado, puede hacer esto de una de estas dos formas:

- Copie los componentes CNAME que se muestran en la sección Domains (Dominios). Esta información aún debe agregarse manualmente a la base de datos de DNS.
- También puede elegir Export to CSV (Exportar a CSV. La información del archivo resultante se debe agregar manualmente a la base de datos de DNS.

> **Important**
>
> Para evitar problemas de validación, revise Cómo funcionan los registros CNAME de ACM antes de agregar información a la base de datos de su proveedor de DNS. Si surgen problemas, consulte Solución de problemas en la validación por DNS.

Si ACM no puede validar el nombre de dominio en un plazo de 72 horas desde el momento en que genera un valor de CNAME por usted, ACM cambia el estado del certificado a Validation timed out (Tiempo de espera de validación agotado). La razón más probable de este resultado es que no actualizó con éxito la configuración de DNS con el valor que ACM generó. Para solucionar este problema, debe solicitar un certificado nuevo después de revisar las instrucciones CNAME.

Validación por correo electrónico

Antes de que la autoridad de certificación (CA) de Amazon pueda emitir un certificado para tu sitio, AWS Certificate Manager (ACM) debe comprobar que eres el propietario o el control de todos

los dominios que especificaste en tu solicitud. Puede realizar la verificación mediante el correo electrónico o DNS. En este tema, se explica la validación por correo electrónico. Para obtener información sobre la validación por DNS, consulte Validación por DNS.

Tenga en cuenta lo siguiente acerca de la validación por correo electrónico.

- Para poder utilizar la validación por correo electrónico, necesita una dirección de correo electrónico que funcione registrada en su dominio. Los procedimientos para configurar una dirección de correo electrónico quedan fuera del alcance de esta guía.
- La validación solo se aplica a los certificados de confianza pública emitidos por ACM. ACM no valida la propiedad del dominio para certificados importados o para certificados firmados por una CA privada. ACM no puede validar los recursos de una zona alojada privada de Amazon VPC o cualquier otro dominio privado. Para obtener más información, consulte Solución de problemas de validación de certificados.
- Después de crear un certificado con validación por correo electrónico, no puede cambiar a la validación mediante DNS.

Los certificados de ACM son válidos durante 13 meses (395 días). Para renovar los certificados validados por correo electrónico, el propietario del dominio debe realizar una acción. ACM comienza a enviar avisos de renovación 45 días antes del vencimiento y utiliza las direcciones de buzón WHOIS del dominio y cinco direcciones comunes de administrador. Las notificaciones contienen un enlace que el propietario del dominio puede presionar para facilitar la renovación. Una vez validados todos los dominios enumerados, ACM emite un certificado renovado con el mismo ARN.

Si tiene problemas al utilizar la validación por correo electrónico, consulte Solución de problemas de validación por correo electrónico.

ACM envía mensajes de correo electrónico al superdominio que elijas. Cualquier subdominio que no supere la dirección mínima de sitio web es válido y se utilizará como dominio de la dirección de correo electrónico como sufijo después de «@» (por ejemplo, puede recibir un correo electrónico a admin@example.com si especifica example.com como dominio de validación para el subdominio.example.com).

Se envían mensajes de correo electrónico a las siguientes tres direcciones de contacto registradas en WHOIS:

- Titularidad del dominio

- Contacto técnico
- Contacto administrativo

> **Note**
>
> Le recomendamos encarecidamente que configure y supervise las cinco direcciones comunes del sistema para el certificado. La recuperación de la información de contacto de WHOIS no es fiable. La tasa de éxito de las búsquedas en WHOIS es baja (menos del 5 %), en parte debido al cumplimiento de la legislación internacional en materia de privacidad.

> **Important**
>
> A partir de junio de 2024, ACM dejará de admitir la validación de nuevos correos electrónicos mediante direcciones de contacto de WHOIS. En el caso de los certificados existentes, a partir de octubre de 2024, ACM no enviará avisos de renovación a las direcciones de contacto de WHOIS del dominio. ACM seguirá enviando correos electrónicos de validación a las cinco direcciones comunes del sistema para el dominio solicitado. Para obtener más información, consulte AWS Certificate Manager Suspenderá la búsqueda en WHOIS de certificados validados por correo electrónico

Cuando solicitas un certificado, ACM envía un correo electrónico al nombre de dominio que especifiques en el `DomainName` parámetro o en el parámetro opcional. `ValidationDomain` Para obtener más información, consulte ???.

- administrator@*su_nombre_de_dominio*
- hostmaster@*su_nombre_de_dominio*
- postmaster@*su_nombre_de_dominio*
- webmaster@*su_nombre_de_dominio*
- admin@*su_nombre_de_dominio*

Para obtener más información sobre cómo ACM determina las direcciones de correo electrónico para sus dominios, consulte (Opcional) Configuración del correo electrónico para el dominio.

Excepción a este proceso

Si solicita un certificado de ACM para un nombre de dominio que empiece con **www** o un asterisco de comodín (*****), ACM elimina **www** o el asterisco inicial y envía un correo electrónico a las direcciones administrativas. Estas direcciones se forman anteponiendo admin@, administrator@, hostmaster@, postmaster@ y webmaster@ a la parte restante del nombre de dominio. Por ejemplo, si solicita un certificado de ACM para www.example.com, se envía un correo electrónico a admin@example.com en vez de a admin@www.example.com. Del mismo modo, si solicita un certificado de ACM para *.test.example.com, se envía un correo electrónico a admin@test.example.com. El resto de las direcciones administrativas comunes se forman de manera similar.

> **Note**
>
> Asegúrese de que se envía el correo electrónico a las direcciones administrativas de un dominio ápex, como `example.com`, en lugar de hacerlo a las direcciones administrativas de un subdominio como `test.example.com`. Para ello, especifique la opción en la API o en el comando request-certificate. `ValidationDomain` AWS CLI `RequestCertificate` Esta característica no se admite actualmente cuando utiliza la consola para solicitar un certificado. Incluso cuando todos los mensajes se envían a una sola dirección de correo electrónico, debe responder a un mensaje para cada dominio o subdominio para validarlo y generar el certificado.

Vencimiento y renovación de certificados

Los certificados de ACM son válidos durante 13 meses (395 días). Para renovar los certificados validados por correo electrónico, el propietario del dominio debe realizar una acción. ACM comienza a enviar avisos de renovación 45 días antes del vencimiento y utiliza las direcciones de buzón WHOIS del dominio y cinco direcciones comunes de administrador. Las notificaciones contienen un enlace que el propietario del dominio puede presionar para facilitar la renovación. Una vez validados todos los dominios enumerados, ACM emite un certificado renovado con el mismo ARN.

Consulte Validación por correo electrónico, arriba, para obtener más información.

(Opcional) Volver a enviar el correo de validación

Cada correo electrónico de validación contiene un token que puede utilizar para aprobar una solicitud de certificado. No obstante, puesto que el correo electrónico de validación necesario para el proceso de aprobación puede bloquearse por filtros de spam o perderse en el camino, el token vence automáticamente después de 72 horas. Si no recibe el correo electrónico original o si el token ha vencido, puede solicitar que se vuelva a enviar el correo electrónico.

Para problemas persistentes con la validación por correo electrónico, consulte la sección Solución de problemas de validación por correo electrónico de Solución de problemas.

> **Note**
>
> La siguiente información se aplica únicamente a los certificados proporcionados por ACM y a los certificados que utilizan la validación por correo electrónico. El correo electrónico de validación no es necesario para los certificados PKI privados o para los certificados que importó a ACM. Para obtener más información sobre la validación de dominios de DNS, consulte Validación por DNS.

Para volver a enviar el correo electrónico de validación mediante la consola

1. Inicie sesión en la consola AWS de administración y abra la consola ACM en https://console.aws.amazon.com/acm/home.
2. En la lista de certificados, elija la ID de certificado del certificado que desea configurar. Con esta acción, se abre una página de detalles.

   > **Note**
   >
   > Según cómo haya ordenado la lista, es posible que un certificado que esté buscando no esté visible de inmediato. Puede hacer clic en el triángulo negro de la derecha para cambiar el orden. También puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha.

3. En la sección Domains (Dominios), elija Resend validation email (Reenviar correo electrónico de validación), seleccione cada uno de los dominios que requieren validación y, a continuación, elija Resend (Reenviar). Debe aparecer el banner Successfully resent validation emails (Correos electrónicos de validación reenviados correctamente).

Para volver a enviar el correo electrónico de validación mediante el AWS CLI

Puede usar el resend-validation-emailcomando para reenviar el correo electrónico.

```
$ aws acm resend-validation-email --certificate-arn
 arn:aws:acm:Region:444455556666:certificate/certificate_ID --domain www.example.com --
validation-domain example.com
```

> **Note**
>
> El resend-validation-emailcomando se aplica únicamente a los certificados ACM para los que se utiliza la validación por correo electrónico. La validación no es necesaria para los certificados que ha importado a ACM o para los certificados privados que administra mediante ACM.

Enumeración de certificados administrados por ACM

Puede utilizar la consola de ACM o AWS CLI para enumerar los certificados gestionados por ACM. La consola puede incluir hasta 500 certificados en una página y la CLI hasta 1000.

Para enumerar los certificados mediante la consola

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/.
2. Revise la información de la lista de certificados. Puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha. Cada certificado ocupa una fila con las siguientes columnas mostradas de forma predeterminada para cada certificado:

- Domain name (Nombre de dominio): el nombre del dominio completo (FQDN) para el certificado.
- Tipo: el tipo de certificado. Los valores posibles son: Amazon issued (Emitido por Amazon) | Private (Privado) | Imported (Importado)
- Status (Estado): estado del certificado. Los valores posibles son: Pending validation (Pendiente de validación) | Issued (Emitido) | Inactive (Inactivo) | Expired (Vencido) | Revoked (Revocado) | Failed (Fallido) | Validation timed out (Validación del tiempo de espera agotado)
- ¿En uso? — Si el certificado ACM está asociado activamente a un AWS servicio como Elastic Load Balancing o CloudFront. El valor puede ser No o Sí.
- Renewal eligibility (Posibilidad de renovación): si ACM puede o no renovar automáticamente el certificado cuando esté a punto de caducar. Los valores pueden ser Eligible (Posible) | Ineligible (No posible). Para conocer las reglas de elegibilidad, consulte Renovación administrada para certificados de ACM.

Al elegir el icono de configuración situado en la esquina superior derecha de la consola, puede personalizar el número de certificados que se muestran en una página, especificar el

comportamiento de ajuste de líneas del contenido de las celdas y mostrar campos de información adicionales. Están disponibles los siguientes campos opcionales:

- Additional domain names (Nombres de dominio adicionales): uno o varios nombres de dominio (nombres alternativos del firmante) incluidos en el certificado.
- Requested at (Solicitado a las): hora a la que ACM solicitó el certificado.
- Issued at (Emitido a las): hora a la que se emitió el certificado. Esta información solo está disponible para los certificados emitidos por Amazon, no para las importaciones.
- Not before (No antes de): hora antes de la cual el certificado no es válido.
- Not after (No después de): hora después de la cual el certificado no es válido.
- Revoked at (Revocado a las): en el caso de los certificados revocados, hora de la revocación.
- Name tag (Etiqueta Nombre): valor de una etiqueta de este certificado denominada Nombre, si tal etiqueta existe.
- Renewal status (Estado de renovación): estado de la renovación solicitada de un certificado. Este campo se muestra y tiene un valor solo cuando se ha solicitado la renovación. Los valores posibles son: Pending automatic renewal (Pendiente de renovación automática) | Pending validation (Validación pendiente) | Success (Correcto) | Failure (Fallo).

> **Note**
>
> Es posible que pasen varias horas hasta que los cambios de estado del certificado estén disponibles. Si se produce un problema, se agota el tiempo de espera de la solicitud de certificado transcurridas 72 horas y se debe repetir el proceso de emisión o renovación desde el principio.

La preferencia de tamaño de página especifica el número de certificados devueltos en cada página de la consola.

Para obtener más información acerca de los detalles de certificados disponibles, consulte Descripción de certificados de ACM.

Para enumerar sus certificados, utilice la AWS CLI

Utilice el comando list-certificates para enumerar los certificados administrados por ACM tal y como se muestra en el siguiente ejemplo:

```
$ aws acm list-certificates --max-items 10
```

El comando devuelve información similar a la siguiente:

```
{
    "CertificateSummaryList": [
        {
            "CertificateArn":
 "arn:aws:acm:Region:444455556666:certificate/certificate_ID",
            "DomainName": "example.com"
  "SubjectAlternativeNameSummaries": [
                "example.com",
                "other.example.com"
            ],
            "HasAdditionalSubjectAlternativeNames": false,
            "Status": "ISSUED",
            "Type": "IMPORTED",
            "KeyAlgorithm": "RSA-2048",
            "KeyUsages": [
                "DIGITAL_SIGNATURE",
                "KEY_ENCIPHERMENT"
            ],
            "ExtendedKeyUsages": [
                "NONE"
            ],
            "InUse": false,
            "RenewalEligibility": "INELIGIBLE",
            "NotBefore": "2022-06-14T23:42:49+00:00",
            "NotAfter": "2032-06-11T23:42:49+00:00",
            "CreatedAt": "2022-08-25T19:28:05.531000+00:00",
            "ImportedAt": "2022-08-25T19:28:05.544000+00:00"
        },...
    ]
}
```

De forma predeterminada, solo se devuelven certificados con keyTypes, `RSA_1024` o `RSA_2048` y con al menos un dominio especificado. Para ver otros certificados que controla, como certificados sin dominio o certificados que utilizan un algoritmo o tamaño de bits diferente, proporcione el parámetro `--includes` como se muestra en el siguiente ejemplo. El parámetro permite especificar un miembro de la estructura Filters (Filtros).

```
$ aws acm list-certificates --max-items 10 --includes keyTypes=RSA_4096
```

Descripción de certificados de ACM

Puede usar la consola ACM o la AWS CLI para enumerar los metadatos detallados sobre sus certificados.

Para ver los detalles del certificado en la consola

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/ para mostrar los certificados. Puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha.
2. Para mostrar metadatos detallados de un certificado de la lista, elija la ID de certificado. Se abre una página en la que se muestra la siguiente información:

   - Certificate status (Estado del certificado)
     - Identifier (Identificador): identificador único hexadecimal de 32 bytes del certificado
     - ARN: un Nombre de recurso de Amazon (ARN) en el formulario `arn:aws:acm:Region:444455556666:certificate/certificate_ID`.
     - Type (Tipo): identifica la categoría de administración de un certificado de ACM. Los valores posibles son: Amazon Issued (Emitido por Amazon) | Private (Privado) | Imported (Importado). Para obtener más información, consulte Solicitar un certificado público, Solicitud de un certificado PKI privado, o Importación de certificados a AWS Certificate Manager.
     - Status (Estado): estado del certificado. Los valores posibles son: Pending validation (Pendiente de validación) | Issued (Emitido) | Inactive (Inactivo) | Expired (Vencido) | Revoked (Revocado) | Failed (Fallido) | Validation timed out (Validación del tiempo de espera agotado)
     - Detailed status (Estado detallado): fecha y hora en la que se emitió o importó el certificado
   - Dominios
     - Domain (Dominio): el nombre del dominio completo (FQDN) para el certificado.
     - Status (Estado): el estado de validación del dominio. Los valores posibles son: Pending validation (Pendiente de validación) | Revoked (Revocado) | Failed (Fallido) | Validation timed out (Validación del tiempo de espera agotado) | Success (Éxito)
   - Detalles

- ¿En uso? Si el certificado está asociado a un servicio integrado de AWSLos valores posibles son: Sí | No
- Domain name (Nombre de dominio): el nombre del dominio completo (FQDN) para el certificado.
- Number of additional names (Número de nombres adicionales): número de nombres de dominio para los que el certificado es válido
- Serial number (Número de serie): número de serie hexadecimal de 16 bytes del certificado
- Public key info (Información de clave pública): el algoritmo criptográfico que generó el par de claves
- Signature algorithm (Algoritmo de firma): el algoritmo criptográfico que se utiliza para firmar el certificado.
- Can be used with (Se puede utilizar con): una lista de servicios integrados de ACM que admiten un certificado con estos parámetros
- Requested at (Solicitado en): fecha y hora de la solicitud de emisión
- Issued at (Expedido en): si procede, la fecha y hora de emisión
- Imported at (Importado a): si procede, la fecha y hora de la importación
- Not before (No antes): el inicio del período de validez del certificado
- Not after (No después de): la fecha y hora de vencimiento del certificado
- Renewal eligibility (Posibilidad de renovación): los valores posibles son: Eligible (Posible) | Inelegible (No posible). Para conocer las reglas de elegibilidad, consulte Renovación administrada para certificados de ACM.
- Renewal status (Estado de renovación): estado de la renovación solicitada de un certificado. Este campo se muestra y tiene un valor solo cuando se ha solicitado la renovación. Los valores posibles son: Pending automatic renewal (Pendiente de renovación automática) | Pending validation (Validación pendiente) | Success (Correcto) | Failure (Fallo).

> **Note**
>
> Es posible que pasen varias horas hasta que los cambios de estado del certificado estén disponibles. Si se produce un problema, se agota el tiempo de espera de la solicitud de certificado transcurridas 72 horas y se debe repetir el proceso de emisión o renovación desde el principio.

- CA: el ARN de la CA emisora de certificados

- Etiquetas
  - Clave
  - Valor
- Validation state (Estado de validación): si procede, los valores posibles son los siguientes:
  - Pendig (Pendiente): la validación se ha solicitado y no se ha completado.
  - Validation timed out (Tiempo de espera de validación agotado): se ha agotado el tiempo de espera de una validación solicitada, pero puede repetir la solicitud.
  - None (Ninguno): el certificado es para una PKI privada o está autofirmado y no necesita validación.

Para ver los detalles del certificado mediante el AWS CLI

Utilice el describe-certificate en el AWS CLI para mostrar los detalles del certificado, como se muestra en el siguiente comando:

```
$ aws acm describe-certificate --certificate-arn
 arn:aws:acm:Region:444455556666:certificate/certificate_ID
```

El comando devuelve información similar a la siguiente:

```
{
    "Certificate": {
        "CertificateArn": "arn:aws:acm:Region:444455556666:certificate/certificate_ID",
        "Status": "EXPIRED",
        "Options": {
            "CertificateTransparencyLoggingPreference": "ENABLED"
        },
        "SubjectAlternativeNames": [
            "example.com",
            "www.example.com"
        ],
        "DomainName": "gregpe.com",
        "NotBefore": 1450137600.0,
        "RenewalEligibility": "INELIGIBLE",
        "NotAfter": 1484481600.0,
        "KeyAlgorithm": "RSA-2048",
        "InUseBy": [
            "arn:aws:cloudfront::account:distribution/E12KXPQHVLSYVC"
        ],
```

```
        "SignatureAlgorithm": "SHA256WITHRSA",
        "CreatedAt": 1450212224.0,
        "IssuedAt": 1450212292.0,
        "KeyUsages": [
            {
                "Name": "DIGITAL_SIGNATURE"
            },
            {
                "Name": "KEY_ENCIPHERMENT"
            }
        ],
        "Serial": "07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b",
        "Issuer": "Amazon",
        "Type": "AMAZON_ISSUED",
        "ExtendedKeyUsages": [
            {
                "OID": "1.3.6.1.5.5.7.3.1",
                "Name": "TLS_WEB_SERVER_AUTHENTICATION"
            },
            {
                "OID": "1.3.6.1.5.5.7.3.2",
                "Name": "TLS_WEB_CLIENT_AUTHENTICATION"
            }
        ],
        "DomainValidationOptions": [
            {
                "ValidationEmails": [
                    "hostmaster@example.com",
                    "admin@example.com",
                    "postmaster@example.com",
                    "webmaster@example.com",
                    "administrator@example.com"
                ],
                "ValidationDomain": "example.com",
                "DomainName": "example.com"
            },
            {
                "ValidationEmails": [
                    "hostmaster@example.com",
                    "admin@example.com",
                    "postmaster@example.com",
                    "webmaster@example.com",
                    "administrator@example.com"
                ],
```

```
                "ValidationDomain": "www.example.com",
                "DomainName": "www.example.com"
            }
        ],
        "Subject": "CN=example.com"
    }
}
```

Eliminar certificados administrados por ACM

Puede utilizar la consola ACM o la AWS CLI para eliminar un certificado.

> **Important**
>
> - No puede eliminar un certificado de ACM que se utilice en otro servicio de AWS . Para eliminar un certificado que esté en uso, primero debe eliminar la asociación del certificado. Esto se hace mediante la consola o la CLI para el servicio asociado.
> - La eliminación de un certificado emitido por una entidad de certificación (CA) privada no afecta a la CA. Se le seguirá cobrando la CA hasta que se elimine. Para obtener más información, consulte Eliminación de una CA privada en la Guía del Usuario de AWS Private Certificate Authority .

Para eliminar un certificado mediante la consola

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/.
2. En la lista de certificados, seleccione la casilla de verificación del certificado de ACM y, a continuación, elija Delete (Eliminar).

> **Note**
>
> Según cómo haya ordenado la lista, es posible que un certificado que esté buscando no esté visible de inmediato. Puede hacer clic en el triángulo negro de la derecha para cambiar el orden. También puede explorar diferentes páginas de certificados utilizando los números de página de la parte superior derecha.

Para eliminar un certificado mediante el AWS CLI

Utilice el comando delete-certificate para eliminar un certificado, tal y como se muestra en el siguiente comando:

```
$ aws acm delete-certificate --certificate-arn
 arn:aws:acm:Region:444455556666:certificate/certificate_ID
```

Instalar certificados de ACM

No puede usar ACM para instalar un certificado público directamente en su sitio web o aplicación AWS basados. Debe utilizar uno de los servicios integrados con ACM. Para obtener más información, consulte Servicios integrados con AWS Certificate Manager.

Los certificados ACM firmados por una entidad emisora de certificados Autoridad de certificación privada de AWS y destinados a su PKI privada se pueden exportar e instalar manualmente en cualquier sistema al que tenga acceso administrativo. Estos certificados no son de confianza en la Internet pública.

Renovación administrada para certificados de ACM

ACM proporciona renovación administrada para los certificados SSL/TLS emitidos por Amazon. Esto significa que ACM renovará sus certificados de forma automática (si utiliza la validación por DNS) o le enviará avisos por correo electrónico cuando se acerque la fecha de vencimiento. Estos servicios se prestan tanto para certificados de ACM públicos como privados.

Un certificado se puede renovar automáticamente en los siguientes supuestos:

- ELEGIBLE si está asociado a otro AWS servicio, como Elastic Load Balancing o CloudFront.
- SE PUEDE RENOVAR si se exporta desde que se emitió o se renovó por última vez.
- ELEGIBLE si se trata de un certificado privado emitido mediante una llamada a la RequestCertificateAPI de ACM y luego exportado o asociado a otro AWS servicio.
- SE PUEDE RENOVAR si se trata de un certificado privado emitido mediante la consola de administración y luego se exporta o asocia con otro servicio de AWS .
- NO ES ELEGIBLE si se trata de un certificado privado emitido mediante una llamada a la Autoridad de certificación privada de AWS IssueCertificateAPI.
- NO SE PUEDE RENOVAR si se importa.
- NO SE PUEDE RENOVAR si ya ha vencido.

Además, se deben cumplir los siguientes requisitos de Punycode relativos a los Nombres de dominio internacionalizados:

1. Los nombres de dominio que empiecen con el patrón “<character><character>--” deben coincidir con “xn--”.
2. Los nombres de dominio que empiecen con “xn--” también deben ser nombres de dominio internacionalizados válidos.

Ejemplos de Punycode

Nombre del dominio	Cumple el n.° 1	Cumple el n.° 2	Permit	Nota
example.com	n/a	n/a	✓	No empieza con “<character><character>--”
a--ejemplo.com	n/a	n/a	✓	No empieza con “<character><character>--”
abc--ejemplo.com	n/a	n/a	✓	No empieza con “<character><character>--”
xn--xyz.com	Sí	Sí	✓	Nombre de dominio internacionalizado válido (se resuelve en 简.com)
xn--ejemplo.com	Sí	No	✗	No es un nombre de dominio internacionalizado válido
ab--ejemplo.com	No	No	✗	Debe empezar con “xn--”

Cuando ACM renueva un certificado, el nombre de recurso de Amazon (ARN) del certificado seguirá siendo el mismo. Además, los certificados de ACM son recursos regionales. Si tiene certificados para el mismo nombre de dominio en varias AWS regiones, cada uno de estos certificados debe renovarse de forma independiente.

Temas

- Renovación de certificados de confianza pública
- Renovación de certificados en una PKI privada
- Verificar el estado de renovación de un certificado

Renovación de certificados de confianza pública

Al emitir un certificado gestionado y de confianza pública, es AWS Certificate Manager necesario que demuestres que eres el propietario del dominio. Esto ocurre mediante la validación por DNS o la validación por correo electrónico. Cuando aparece un certificado para su renovación, ACM utiliza el mismo método que se eligió anteriormente para volver a validar su propiedad. En los temas siguientes se describe cómo se desarrolla el proceso de renovación en cada caso.

Temas

- Renovación de dominios validados por DNS
- Renovación de dominios validados por correo electrónico

Renovación de dominios validados por DNS

La renovación administrada se encuentra totalmente automatizada para los certificados de ACM emitidos originalmente mediante la validación por DNS.

60 días antes del vencimiento, ACM verifica los siguientes criterios de renovación:

- Un AWS servicio utiliza actualmente el certificado.
- Todos los registros CNAME DNS proporcionados por ACM obligatorios (uno para cada nombre alternativo de sujeto exclusivo) están presentes y accesibles a través de DNS público.

Si se cumplen estos criterios, ACM considera válidos los nombres de dominio y renueva el certificado.

ACM envía AWS Health eventos y eventos de Amazon EventBridge cuando no puede validar automáticamente un dominio durante la renovación (por ejemplo, debido a la presencia de un registro CAA). Estos eventos se envían 45 días, 30 días, 15 días, 7 días, 3 días y 1 día antes de la fecha de vencimiento. Para obtener más información, consulte EventBridge Soporte de Amazon para ACM.

Renovación de dominios validados por correo electrónico

Los certificados de ACM son válidos durante 13 meses (395 días). Para renovar los certificados validados por correo electrónico, el propietario del dominio debe realizar una acción. ACM comienza a enviar avisos de renovación 45 días antes del vencimiento y utiliza las direcciones de buzón

WHOIS del dominio y cinco direcciones comunes de administrador. Las notificaciones contienen un enlace que el propietario del dominio puede presionar para facilitar la renovación. Una vez validados todos los dominios enumerados, ACM emite un certificado renovado con el mismo ARN.

Para obtener más información sobre los mensajes de validación por correo electrónico, consulte Validación por correo electrónico.

Para obtener información sobre cómo responder mediante programación al correo electrónico de validación, consulte Automatización de la validación por correo electrónico .

Solicitar un mensaje de correo electrónico de validación de dominio

Una vez configuradas las direcciones de correo electrónico de contacto de su dominio (consulte (Opcional) Configuración del correo electrónico para el dominio), puede utilizar la consola de AWS Certificate Manager o la API de ACM para solicitar que ACM envíe un correo electrónico de validación de dominio para la renovación del certificado. Debe hacerlo en las siguientes circunstancias:

- Utilizó la validación por correo electrónico cuando solicitó inicialmente su certificado de ACM.
- El estado de renovación del certificado es pending validation. Para obtener más información sobre cómo determinar el estado de renovación del certificado, consulte Verificar el estado de renovación de un certificado.
- No ha recibido o no puede encontrar el mensaje de correo electrónico de validación de dominio original que ACM envió para la renovación del certificado.

Para solicitar que ACM reenvíe el mensaje de correo electrónico de validación de dominio (consola)

1. Abra la AWS Certificate Manager consola en https://console.aws.amazon.com/acm/home.
2. Elija el ID de certificado del certificado que requiere validación.
3. Elija Resend validation email (Volver a enviar el correo electrónico de validación).

Para solicitar que ACM reenvíe el correo electrónico de validación de dominio (API de ACM)

Utilice la ResendValidationEmailoperación en la API de ACM. Al hacerlo, se aprueba el ARN del certificado, el dominio que requiere validación manual y el dominio donde desea recibir los correos electrónicos de validación de dominio. El siguiente ejemplo muestra cómo hacerlo con la AWS CLI. Este ejemplo contiene saltos de línea para facilitar la lectura.

```
$ aws acm resend-validation-email \
 --certificate-arn arn:aws:acm:region:account:certificate/certificate_ID \
 --domain subdomain.example.com \
 --validation-domain example.com
```

Renovación de certificados en una PKI privada

Los certificados ACM firmados por una entidad emisora de certificados privada Autoridad de certificación privada de AWS son aptos para la renovación gestionada. A diferencia de los certificados de ACM de confianza pública, un certificado para una PKI privada no requiere validación. La confianza se establece cuando un administrador instala el certificado de entidad de certificación raíz apropiado en los almacenes de confianza del cliente.

> **Note**
>
> Solo los certificados obtenidos mediante la consola de ACM o mediante la RequestCertificateacción de la API de ACM son aptos para la renovación gestionada. ACM no administra los certificados emitidos directamente Autoridad de certificación privada de AWS mediante la IssueCertificateacción de la Autoridad de certificación privada de AWS API.

Cuando quedan 60 días para que venza un certificado administrado, ACM intenta renovarlo de forma automática. Esto incluye los certificados que se exportaron e instalaron de forma manual (por ejemplo, en un centro de datos en las instalaciones). Los clientes también pueden forzar la renovación en cualquier momento mediante la RenewCertificateacción de la API ACM. Para obtener un ejemplo de una implementación de renovación forzada de Java, consulte Renovación de un certificado.

Después de la renovación, la implementación de un certificado para un servicio se realiza de una de las siguientes maneras:

- Si se asocia el certificado a un servicio integrado de ACM, el certificado nuevo reemplaza al anterior sin que el cliente tenga que realizar acciones adicionales.
- Si no se asocia el certificado a un servicio integrado de ACM, es necesario que el cliente exporte e instale el certificado renovado. Puede realizar estas acciones manualmente o con la ayuda de AWS HealthAmazon EventBridge y de la AWS Lambdasiguiente manera. Para obtener más información, consulte Automatización de la exportación de certificados renovados

Automatización de la exportación de certificados renovados

En el siguiente procedimiento se proporciona un ejemplo de solución para automatizar la exportación de sus certificados PKI privados cuando ACM los renueva. En este ejemplo solo se exporta un certificado y su clave privada de ACM. Una vez hecha la exportación, el certificado debe estar instalado en su dispositivo de destino.

Cómo automatizar la exportación de un certificado mediante la consola

1. Siguiendo los procedimientos de la Guía para desarrolladores de AWS Lambda, cree y configure una función de Lambda que llame a la API de exportación de ACM.

   a. Creación de una función de Lambda

   b. Cree un rol de ejecución de Lambda para su función y agréguele la siguiente política de confianza. La política concede permiso al código de su función para recuperar el certificado y la clave privada renovados mediante una llamada a la ExportCertificateacción de la API de ACM.

   ```
   {
      "Version":"2012-10-17",
      "Statement":[
         {
            "Effect":"Allow",
            "Action":"acm:ExportCertificate",
            "Resource":"*"
         }
      ]
   }
   ```

2. Cree una regla en Amazon EventBridge para detectar eventos de estado de ACM y llame a su función Lambda cuando detecte alguno. ACM escribe en un AWS Health evento cada vez que intenta renovar un certificado. Para obtener más información sobre estos avisos, consulte Verificar el estado mediante Personal Health Dashboard (PHD).

   Configure la regla al agregar el siguiente patrón de eventos.

   ```
   {
      "source":[
         "aws.health"
      ],
   ```

```
   "detail-type":[
      "AWS Health Event"
   ],
   "detail":{
      "service":[
         "ACM"
      ],
      "eventTypeCategory":[
         "scheduledChange"
      ],
      "eventTypeCode":[
         "AWS_ACM_RENEWAL_STATE_CHANGE"
      ]
   },
   "resources":[
      "arn:aws:acm:region:account:certificate/certificate_ID"
   ]
}
```

3. Complete el proceso de renovación al instalar de forma manual el certificado en el sistema de destino.

Prueba de la renovación administrada de los certificados de PKI privada

Puede usar la API de ACM o AWS CLI probar manualmente la configuración de su flujo de trabajo de renovación gestionada por ACM. Al hacerlo, puede confirmar que ACM renovará sus certificados de forma automática antes de que venzan.

> **Note**
>
> Solo puede probar la renovación de los certificados emitidos y exportados por. Autoridad de certificación privada de AWS

Cuando utiliza las acciones de la API o los comandos de la CLI descritos a continuación, ACM intenta renovar el certificado. Si la renovación se realiza correctamente, ACM actualiza los metadatos del certificado que se muestran en la consola de administración o en la salida de la API. Si el certificado está asociado a un servicio integrado de ACM, se implementa el nuevo certificado y se genera un evento de renovación en Amazon CloudWatch Events. Si la renovación falla, ACM devuelve un error y sugiere una acción correctiva. (Puede ver esta información mediante el comando

describe-certificate). Si el certificado no se implementa a través de un servicio integrado, tendrá que exportarlo e instalarlo de forma manual en el recurso.

> **Important**
>
> Para renovar sus Autoridad de certificación privada de AWS certificados con ACM, primero debe conceder al servicio de ACM los permisos principales para hacerlo. Para obtener más información, consulte Asignación de permisos de renovación de certificados a ACM.

Para probar manualmente la renovación de certificados (AWS CLI)

1. Use el comando renew-certificate para renovar un certificado privado exportado.

```
aws acm renew-certificate \
 --certificate-arn arn:aws:acm:region:account:certificate/certificate_ID
```

2. A continuación, utilice el comando describe-certificate para confirmar que se han actualizado los detalles de renovación del certificado.

```
aws acm describe-certificate \
 --certificate-arn arn:aws:acm:region:account:certificate/certificate_ID
```

Para probar de forma manual la renovación de certificados (API de ACM)

- Envíe una RenewCertificatesolicitud especificando el ARN del certificado privado que se va a renovar. A continuación, utilice la DescribeCertificateoperación para confirmar que se han actualizado los detalles de renovación del certificado.

Verificar el estado de renovación de un certificado

Cuando intenta renovar un certificado, ACM proporciona un campo de información sobre el estado de la renovación en los detalles del certificado. Puede utilizar la AWS Certificate Manager consola, la API de ACM o la AWS Health Dashboard para comprobar el AWS CLI estado de renovación de un certificado de ACM. Si utiliza la consola o la API ACM AWS CLI, el estado de renovación puede tener uno de los cuatro valores de estado posibles que se indican a continuación. Se muestran valores similares si utiliza el AWS Health Dashboard.

Pending automatic renewal

ACM está intentando validar los nombres de dominio en el certificado de forma automática. Para obtener más información, consulte Renovación de dominios validados por DNS. No hay que hacer nada más.

Validación pendiente

ACM no pudo validar uno o varios de los nombres de dominio del certificado de forma automática. Debe tomar medidas para validar estos nombres de dominio. De lo contrario, el certificado no se renovará. Si utilizó originalmente la validación por correo electrónico para el certificado, busque un mensaje de correo electrónico de ACM y siga el enlace de ese mensaje a fin de realizar la validación. Si utilizó la validación por DNS, compruebe que su registro de DNS existe y que su certificado sigue estando en uso.

Success

Todos los nombres de dominio del certificado se encuentran validados y ACM ha renovado el certificado. No hay que hacer nada más.

Con error

Uno o varios de los nombres de dominio no se validaron antes de que el certificado venciera y ACM no renovó el certificado. Puede solicitar un certificado nuevo.

Un certificado puede renovarse si está asociado a otro AWS servicio, como Elastic Load Balancing CloudFront, o si se ha exportado desde que se emitió o se renovó por última vez.

> **Note**
>
> Es posible que pasen varias horas hasta que los cambios del estado de renovación estén disponibles. Si se produce un problema, se agota el tiempo de espera de la solicitud de renovación transcurridas 72 horas y se debe repetir el proceso de renovación desde el principio. Para obtener ayuda sobre la resolución de problemas, consulte Solución de problemas de solicitudes de certificados.

Temas

- Comprobar el estado (CLI)
- Verificar el estado mediante Personal Health Dashboard (PHD)

Comprobar el estado (consola)

En el siguiente procedimiento se explica cómo utilizar la consola de ACM para verificar el estado de renovación de un certificado de ACM.

1. Abra la AWS Certificate Manager consola en https://console.aws.amazon.com/acm/home.
2. Expanda un certificado para ver sus detalles.
3. Busque Renewal Status (Estado de renovación) en la sección Details (Detalles). Si no ve el estado, ACM no ha comenzado el proceso de renovación administrado de este certificado.

Comprobar el estado (API)

Para ver un ejemplo de Java que muestra cómo utilizar la DescribeCertificateacción para comprobar el estado, consulteDescripción de un certificado.

Comprobar el estado (CLI)

El siguiente ejemplo muestra cómo verificar el estado de renovación del certificado de ACM con la AWS Command Line Interface (AWS CLI).

```
$ aws acm describe-certificate \
 --certificate-arn arn:aws:acm:region:account:certificate/certificate_ID
```

En la respuesta, observe el valor del campo `RenewalStatus`. Si no ve el campo `RenewalStatus`, ACM no ha comenzado el proceso de renovación administrado del certificado.

Verificar el estado mediante Personal Health Dashboard (PHD)

ACM intenta renovar de forma automática su certificado de ACM 60 días antes del vencimiento. Si ACM no puede renovar su certificado automáticamente, le enviará avisos sobre los eventos de renovación del certificado a intervalos de 45, 30, 15 días, 7, 3 días y 1 día antes del vencimiento para informarle de que debe tomar medidas. AWS Health Dashboard Esto AWS Health Dashboard forma parte del AWS Health servicio. No precisa configuración y cualquier usuario autenticado en su cuenta puede consultarlo. Si quiere obtener más información, consulte la Guía del usuario de AWS Health.

> **Note**
>
> ACM escribe avisos sucesivos de eventos de renovación en un solo evento en su línea de tiempo de PHD. Cada aviso sobrescribe el anterior hasta que la renovación se realiza correctamente.

Para usar el AWS Health Dashboard:

1. Inicie sesión AWS Health Dashboard en https://phd.aws.amazon.com/phd/home#/.
2. Elija Event log.
3. En Filter by tags or attributes, elija Service.
4. Elija Certificate Manager.
5. Seleccione Apply.
6. En Event category elija Scheduled Change.
7. Seleccione Apply.

Automatización de la validación por correo electrónico

Por lo general, los certificados de ACM validados por correo electrónico requieren la acción manual del propietario del dominio. Las organizaciones que se ocupan de un gran número de certificados validados por correo electrónico pueden preferir crear un analizador que pueda automatizar las respuestas necesarias. A fin de ayudar a los clientes a utilizar la validación por correo electrónico, la información en esta sección describe las plantillas utilizadas para los mensajes de correo electrónico de validación de dominio y el flujo de trabajo utilizado para completar el proceso de validación.

Plantillas de correo electrónico de validación

Los mensajes de correo electrónico de validación tienen uno de los dos formatos siguientes, en función de si se solicita un certificado nuevo o se renueva un certificado existente. El contenido de las cadenas resaltadas debe reemplazarse por valores específicos del dominio que se valida.

Validación de un nuevo certificado

Texto de la plantilla de correo electrónico:

```
Greetings from Amazon Web Services,

We received a request to issue an SSL/TLS certificate for requested_domain.

Verify that the following domain, AWS account ID, and certificate identifier
 correspond
to a request from you or someone in your organization.

Domain: fqdn
AWS account ID: account_id
AWS Region name: region_name
Certificate Identifier: certificate_identifier

To approve this request, go to Amazon Certificate Approvals
(https://region_name.acm-certificates.amazon.com/approvals?
code=validation_code&context=validation_context)
and follow the instructions on the page.

This email is intended solely for authorized individuals for fqdn. To express any
 concerns
```

```
about this email or if this email has reached you in error, forward it along with a
 brief
explanation of your concern to validation-questions@amazon.com.

Sincerely,
Amazon Web Services
```

Validación de un certificado para su renovación

Texto de la plantilla de correo electrónico:

```
Greetings from Amazon Web Services,

We received a request to issue an SSL/TLS certificate for requested_domain.
This email is a request to validate ownership of the domain in order to renew
the existing, currently in use, certificate. Certificates have defined
validity periods and email validated certificates, like this one, require you
to re-validate for the certificate to renew.

Verify that the following domain, AWS account ID, and certificate identifier
correspond to a request from you or someone in your organization.

Domain: fqdn
AWS account ID: account_id
AWS Region name: region_name
Certificate Identifier: certificate_identifier

To approve this request, go to Amazon Certificate Approvals at
https://region_name.acm-certificates.amazon.com/approvals?code=
$validation_code&context=$validation_context
and follow the instructions on the page.

This email is intended solely for authorized individuals for fqdn. You can see
more about how AWS Certificate Manager validation works here -
https://docs.aws.amazon.com/acm/latest/userguide/email-validation.html.
To express any concerns about this email or if this email has reached you in
error, forward it along with a brief explanation of your concern to
validation-questions@amazon.com.

Sincerely,
Amazon Web Services

--
```

```
Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a
registered trademark of Amazon.com, Inc.

This message produced and distributed by Amazon Web Services, Inc.,
410 Terry Ave. North, Seattle, WA 98109-5210.

(c)2015-2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Our privacy policy is posted at https://aws.amazon.com/privacy
```

Una vez que reciba un nuevo mensaje de validación AWS, le recomendamos que lo utilice como la plantilla más up-to-date autorizada para su analizador. Los clientes con analizadores de mensajes diseñados antes de noviembre de 2020 deben tener en cuenta los siguientes cambios que pueden haberse realizado en la plantilla:

- La línea de asunto del correo electrónico ahora dice "`Certificate request for` *`domain name`*" en lugar de decir "`"Certificate approval for` *`domain name`*".
- El `AWS account ID` ahora se presenta sin rayas ni guiones.
- El `Certificate Identifier` ahora presenta todo el ARN del certificado en lugar de una forma abreviada, por ejemplo, *`arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369`* en lugar de *`3b4d78e1-0882-4f51-954a-298ee44ff369`*.
- La URL de aprobación del certificado contiene ahora `acm-certificates.amazon.com` en lugar de `certificates.amazon.com`.
- El formulario de aprobación que se abre al hacer clic en la dirección URL de aprobación del certificado ahora contiene el botón de aprobación. El nombre del botón de aprobación div es ahora `approve-button` en lugar de `approval_button`.
- Los mensajes de validación para los certificados recién solicitados y los certificados de renovación tienen el mismo formato de correo electrónico.

Flujo de trabajo de validación

En esta sección se proporciona información sobre el flujo de trabajo de renovación de certificados validados por correo electrónico.

- Cuando la consola ACM procesa una solicitud de certificado multidominio, envía mensajes de correo electrónico de validación a la TAREA TODO. El propietario del dominio debe validar un mensaje de correo electrónico para cada dominio antes de que ACM pueda emitir el certificado. A

fin de obtener más información, consulte Uso del correo electrónico para validar la propiedad del dominio.

- La validación por correo electrónico para solicitudes de certificados de varios dominios mediante la API o CLI de ACM genera el envío de un mensaje de correo electrónico de forma predeterminada al dominio ápex y a cada subdominio. El propietario del dominio debe validar un mensaje de correo electrónico para cada uno de estos dominios antes de que ACM pueda emitir el certificado.

  > **Note**
  >
  > Antes de noviembre de 2020, los clientes solo debían validar el dominio ápex y ACM emitía un certificado que también cubría cualquier subdominio. Los clientes con analizadores de mensajes diseñados antes de esa fecha deben tener en cuenta el cambio en el flujo de trabajo de validación por correo electrónico.

- Con la API o CLI de ACM, puede forzar que todos los mensajes de correo electrónico de validación para una solicitud de certificado de varios dominios se envíen al dominio ápex. En la API, utilice el `DomainValidationOptions` parámetro de la RequestCertificateacción para `ValidationDomain` especificar un valor que pertenezca al DomainValidationOptiontipo. En la CLI, utilice el parámetro --domain-validation-options del comando request-certificate para especificar un valor de `ValidationDomain`.

Importación de certificados a AWS Certificate Manager

Además de solicitar los certificados SSL/TLS proporcionados por AWS Certificate Manager (ACM), puede importar los certificados que haya obtenido de forma externa. AWS Posiblemente quiera hacerlo porque ya tiene un certificado de una entidad de certificación (CA) de terceros o porque tiene requisitos específicos de la aplicación que los certificados emitidos por ACM no cumplen.

Puede utilizar un certificado importado con cualquier servicio de AWS integrado con ACM. Los certificados importados funcionan de la misma manera que los proporcionados por ACM, aunque con una excepción importante: ACM no ofrece renovación administrada para los certificados importados.

Para renovar un certificado importado, puede obtener un nuevo certificado del emisor y, a continuación, volver a importarlo manualmente a ACM. Esta acción conserva la asociación del certificado y su nombre de recurso de Amazon (ARN). También puede importar un certificado completamente nuevo. Se pueden importar varios certificados con el mismo nombre de dominio, pero se deben importar de uno en uno.

> **Important**
>
> El cliente es responsable de vigilar la fecha de vencimiento de los certificados importados y de renovarlos antes de que se venzan. Puede simplificar esta tarea utilizando Amazon CloudWatch Events para enviar avisos cuando sus certificados importados estén próximos a caducar. Para obtener más información, consulte Uso de Amazon EventBridge.

En ACM, todos los certificados son recursos regionales, incluso los importados. Para usar el mismo certificado con los balanceadores de carga de Elastic Load Balancing en distintas AWS regiones, debe importar el certificado a cada región en la que desee usarlo. Para utilizar un certificado con Amazon CloudFront, debes importarlo a la región EE.UU. Este (Virginia del Norte). Para obtener más información, consulte Regiones admitidas.

Para más información sobre cómo importar certificados a ACM, consulte los siguientes temas. Si tiene problemas al importar un certificado, consulte Problemas de importación de certificados.

Temas

- Requisitos previos para la importación de certificados
- Formato del certificado y de la clave para la importación

- Importación de un certificado
- Volver a importar un certificado

Requisitos previos para la importación de certificados

Para importar un certificado SSL/TLS autofirmado a ACM, debe proporcionar tanto el certificado como su clave privada. Para importar un certificado firmado por una entidad de certificación (CA) que no sea de AWS , también deberá incluir las claves públicas y privadas de certificación. El certificado debe cumplir con todos los criterios descritos en este tema.

Para todos los certificados importados, debe especificar un algoritmo criptográfico y un tamaño de clave. ACM admite los siguientes algoritmos (nombre de API entre paréntesis):

- RSA de 1024 bits (`RSA_1024`)
- RSA de 2048 bits (`RSA_2048`)
- RSA de 3072 bits (`RSA_3072`)
- RSA de 4096 bits (`RSA_4096`)
- ECDSA de 256 bits (`EC_prime256v1`)
- ECDSA de 384 bits (`EC_secp384r1`)
- ECDSA de 521 bits (`EC_secp521r1`)

Además, tenga en cuenta los siguientes requisitos adicionales:

- Los servicios integrados de ACM solo permiten asociar a sus recursos los algoritmos y tamaños de clave que admiten. Por ejemplo, CloudFront solo admite claves RSA de 1024 bits, RSA de 2048 bits, RSA de 3072 bits y Elliptic Prime Curve de 256 bits, mientras que Application Load Balancer admite todos los algoritmos disponibles en ACM. Para obtener más información, consulte la documentación de los servicios que utiliza.
- El certificado debe ser un certificado SSL/TLS X.509 versión 3. Debe contener una clave pública, el nombre de dominio completo (FQDN) o dirección IP del sitio web e información sobre el emisor.
- Un certificado puede ser autofirmado por una clave privada de su propiedad o firmado por la clave privada de una CA emisora. Debe proporcionar la clave privada, la cual no debe superar los 5 KB (5120 bytes) y debe estar sin cifrar.
- Si el certificado está firmado por una CA, y elige indicar la cadena de certificados, la cadena debe estar codificada en PEM.

- Un certificado debe ser válido en el momento de la importación. No puede importar un certificado antes de que comience su periodo de validez o después de que venza. El campo de certificado `NotBefore` contiene la fecha de comienzo de validez y el campo `NotAfter` contiene la fecha de finalización.
- Todos los materiales de certificado necesarios (certificado, clave privada y cadena de certificados) deben tener codificación PEM. La carga de materiales con codificación DER produce un error. Para obtener más información y ejemplos, consulte Formato del certificado y de la clave para la importación.
- Cuando renueva (vuelve a importar) un certificado, no puede agregar un certificado con extensión `KeyUsage` o `ExtendedKeyUsage`, si la extensión no estaba presente en el certificado importado anteriormente.
- AWS CloudFormation no admite la importación de certificados a ACM.

Formato del certificado y de la clave para la importación

ACM requiere importar por separado el certificado, la cadena de certificados y la clave privada (si la hay) y codificar cada componente en formato PEM. PEM son las siglas de correo de privacidad mejorada. El formato PEM se utiliza a menudo para representar certificados, solicitudes de certificados, cadenas de certificados y claves. La extensión típica de un archivo con formato PEM es `.pem`, pero no es obligatoria.

> **Note**
>
> AWS no proporciona utilidades para manipular archivos PEM u otros formatos de certificado. Los siguientes ejemplos se basan en un editor de texto genérico para operaciones simples. Si necesita realizar tareas más complejas (como convertir formatos de archivo o extraer claves), están disponibles herramientas gratuitas y de código abierto como OpenSSL.

Los siguientes ejemplos ilustran el formato de los archivos que se van a importar. Si los componentes se le entregan en un solo archivo, use un editor de texto (con cuidado) para separarlos en tres archivos. Tenga en cuenta que si edita incorrectamente cualquiera de los caracteres de un archivo PEM o si añade uno o varios espacios al final de cualquier línea, el certificado, la cadena de certificados o la clave privada dejarán de ser válidos.

Example 1. Certificado codificado en PEM

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Example 2. Cadena de certificados codificada en PEM

Una cadena de certificados contiene uno o más certificados. Puede utilizar un editor de texto, el comando `copy` de Windows o el comando `cat` de Linux para concatenar archivos de certificado en una cadena. Los certificados deben concatenarse por orden, de modo que cada uno certifique directamente al anterior. Si importa un certificado privado, copie el certificado raíz al final. El siguiente ejemplo contiene tres certificados, pero una cadena de certificados podría contener más o menos.

> **Important**
>
> No copie su certificado en la cadena de certificados.

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Example 3. Claves privadas codificadas en PEM

Los certificados X.509 versión 3 utilizan algoritmos de clave pública. Cuando se crea una solicitud de certificado o un certificado X.509, se debe especificar el algoritmo y el tamaño de la clave en bits que se deben utilizar para crear el par de claves públicas-privadas. La clave pública se incluye en el certificado o la solicitud. Debe mantener en secreto la clave privada asociada. Especifique la clave privada al importar el certificado. La clave no debe estar cifrada. En el ejemplo siguiente se muestra una clave privada RSA.

```
-----BEGIN RSA PRIVATE KEY-----
Base64-encoded private key
```

```
-----END RSA PRIVATE KEY-----
```

En el ejemplo siguiente se muestra una clave privada de curva elíptica codificada en PEM. En función de cómo se cree la clave, es posible que no se incluya el bloque de parámetros. Si se incluye el bloque de parámetros, ACM lo elimina antes de utilizar la clave durante el proceso de importación.

```
-----BEGIN EC PARAMETERS-----
Base64-encoded parameters
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
Base64-encoded private key
-----END EC PRIVATE KEY-----
```

Importación de un certificado

Puede importar un certificado obtenido externamente (es decir, uno proporcionado por un proveedor de servicios de confianza externo) a ACM mediante la AWS Management Console AWS CLI API de ACM. En los temas siguientes se muestra cómo utilizar el AWS Management Console y el. AWS CLI Los procedimientos para obtener un certificado de una AWS entidad no emisora quedan fuera del ámbito de esta guía.

> **Important**
>
> El algoritmo de firma seleccionado debe cumplir con el Requisitos previos para la importación de certificados.

Temas

- Importar (consola)
- Importación (AWS CLI)

Importar (consola)

El siguiente ejemplo muestra cómo importar un certificado con la AWS Management Console.

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/home. Si es la primera vez que utiliza ACM, busque el encabezado AWS Certificate Manager y seleccione el botón Get started (Empezar) que hay debajo de él.

2. Seleccione Import a certificate.
3. Haga lo siguiente:

   a. En el Certificate body, pegue el certificado codificado en PEM para importar. Debería comenzar con `-----BEGIN CERTIFICATE-----` y terminar con `-----END CERTIFICATE-----`.

   b. En Certificate private key (Clave privada del certificado), pegue la clave privada codificada en PEM y sin cifrar del certificado. Debería comenzar con `-----BEGIN PRIVATE KEY-----` y terminar con `-----END PRIVATE KEY-----`.

   c. (Opcional) En Certificate chain, pegue la cadena de certificados codificada en PEM.
4. (Opcional) Para añadir etiquetas a su certificado importado, elija Etiquetas. Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Puedes usar etiquetas para organizar tus recursos o hacer un seguimiento de tus AWS costos.
5. Seleccione Importar.

Importación (AWS CLI)

El siguiente ejemplo muestra cómo importar un certificado con la AWS Command Line Interface (AWS CLI). El ejemplo supone lo siguiente:

- El certificado codificado en PEM se guarda en un archivo llamado `Certificate.pem`.
- La cadena de certificados codificados en PEM se guarda en un archivo llamado `CertificateChain.pem`.
- La clave privada codificada en PEM sin cifrar se guarda en un archivo llamado `PrivateKey.pem`.

Para utilizar el siguiente ejemplo, sustituya los nombres de archivo con el suyo y escriba el comando en una línea continua. El siguiente ejemplo incluye saltos de línea y espacios adicionales para facilitar su lectura.

```
$ aws acm import-certificate --certificate fileb://Certificate.pem \
      --certificate-chain fileb://CertificateChain.pem \
      --private-key fileb://PrivateKey.pem
```

Si el comando `import-certificate` es correcto, devolverá el nombre de recurso de Amazon (ARN) del certificado importado.

Volver a importar un certificado

Si ha importado un certificado y lo ha asociado a otros AWS servicios, puede volver a importarlo antes de que caduque y, al mismo tiempo, conservar las asociaciones de AWS servicios del certificado original. Para obtener más información sobre AWS los servicios integrados con ACM, consulte. Servicios integrados con AWS Certificate Manager

Las siguientes condiciones se aplican al volver a importar un certificado:

- Puede añadir o eliminar nombres de dominio.
- No puede eliminar todos los nombres de dominio de un certificado.
- Si hay extensiones de uso de claves presentes en el certificado importado originalmente, puede agregar nuevos valores de extensión, pero no puede quitar valores existentes.
- Si hay extensiones de uso extendido de claves presentes en el certificado importado originalmente, puede agregar nuevos valores de extensión, pero no puede quitar valores existentes.
- El tipo y el tamaño de clave no pueden modificarse.
- No puede aplicar etiquetas de recurso al reimportar un certificado.

Temas

Volver a importar (consola)

El siguiente ejemplo muestra cómo volver a importar un certificado con la AWS Management Console.

1. Abra la consola de ACM en https://console.aws.amazon.com/acm/home.
2. Seleccione o amplíe el certificado que vaya a reimportar.
3. Abra el panel de detalles del certificado y haga clic en el botón Reimport certificate. Si ha seleccionado el certificado marcando la casilla junto a su nombre, elija Reimport certificate en el menú Actions.
4. En Certificate body, pegue el certificado de entidad final codificado en PEM.
5. En Certificate private key, pegue la clave privada codificada en PEM y sin cifrar asociada con la clave pública del certificado.

6. (Opcional) En Certificate chain, pegue la cadena de certificados codificada en PEM. La cadena de certificados incluye uno o más certificados para todas las entidades de certificación emisoras intermedias y el certificado raíz. Si el certificado que se va a importar se asigna automáticamente, no es necesaria ninguna cadena de certificados.
7. Seleccione Review and import.
8. Revise la información sobre su certificado. Si no hay errores, elija Reimport.

Volver a importar (AWS CLI)

El siguiente ejemplo muestra cómo volver a importar un certificado con la AWS Command Line Interface (AWS CLI). El ejemplo supone lo siguiente:

- El certificado codificado en PEM se guarda en un archivo llamado `Certificate.pem`.
- La cadena de certificados codificados en PEM se guarda en un archivo llamado `CertificateChain.pem`.
- (Solo certificados privados) La clave privada sin cifrar y codificada en PEM se almacena en un archivo llamado `PrivateKey.pem`.
- Tiene el ARN del certificado que desea importar.

Para utilizar el siguiente ejemplo, sustituya los nombres de archivo y el ARN con el suyo y escriba el comando en una línea continua. El siguiente ejemplo incluye saltos de línea y espacios adicionales para facilitar su lectura.

> **Note**
>
> Para reimportar un certificado, debe especificar el ARN del certificado.

```
$ aws acm import-certificate --certificate fileb://Certificate.pem \
      --certificate-chain fileb://CertificateChain.pem \
      --private-key fileb://PrivateKey.pem \
      --certificate-
arn arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Si el comando `import-certificate` es correcto, devolverá el nombre de recurso de Amazon (ARN) del certificado.

Exportación de un certificado privado

Puede exportar un certificado emitido por Autoridad de certificación privada de AWS para usarlo en cualquier lugar de su entorno de PKI privado. El archivo exportado contiene el certificado, la cadena de certificados y la clave privada cifrada. Este archivo debe almacenarse de forma segura. Para obtener más información al respecto Autoridad de certificación privada de AWS, consulte la Guía AWS Private Certificate Authority del usuario.

> **Note**
>
> No puede exportar un certificado de confianza pública ni su clave privada, independientemente de si lo ha emitido ACM o se ha importado.

Temas

Exportación de un certificado privado (consola)

1. Inicie sesión en la consola AWS de administración y abra la consola de ACM en https://console.aws.amazon.com/acm/home.
2. Elija Certificate Manager
3. Elija el enlace del certificado que desea exportar.
4. Seleccione Exportar.
5. Escriba y confirme una frase de contraseña para la clave privada.

   > **Note**
   >
   > Al crear la frase de contraseña, puede utilizar cualquier carácter ASCII excepto #, $ o%.

6. Elija Generate PEM Encoding (Generar codificación PEM).
7. Puede copiar el certificado, la cadena de certificados y la clave cifrada en la memoria o elegir Export to a file (Exportar a un archivo) para cada uno de ellos.
8. Seleccione Listo.

Exportación de un certificado privado (CLI)

Utilice el comando export-certificate para exportar un certificado privado y la clave privada. Debe asignar una frase de contraseña cuando ejecuta el comando. Para una mayor seguridad, utilice un editor de archivos para almacenar su frase de contraseña en un archivo y, a continuación, proporcione la frase de contraseña suministrando el archivo. Esto impide que la frase de contraseña se almacene en el historial de comandos y que otras personas la vean mientras la escribe.

> **Note**
>
> El archivo que contiene la frase de contraseña no debe concluir con un terminador de línea. Puede verificar su archivo de contraseña de esta manera:
>
> ```
> $ file -k passphrase.txt
> passphrase.txt: ASCII text, with no line terminators
> ```

Los siguientes ejemplos canalizan la salida del comando en `jq` para aplicar el formato PEM.

```
[Linux]
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:Region:444455556666:certificate/certificate_ID \
     --passphrase fileb://path-to-passphrase-file  \
     | jq -r '"\(.Certificate)\(.CertificateChain)\(.PrivateKey)"'

[Windows]
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:Region:444455556666:certificate/certificate_ID \
     --passphrase fileb://path-to-passphrase-file  \
     | jq -r '\"(.Certificate)(.CertificateChain)(.PrivateKey)\"'
```

Genera un certificado en formato PEM codificado en Base64 que también contiene una cadena de certificados y una clave privada cifrada, como se muestra en el siguiente ejemplo abreviado.

```
-----BEGIN CERTIFICATE-----
MIIDTDCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwWOdLOkxpwkkKWtcEkQuHE1v5Vn6HpbfFmxkdPEasoDhthH
```

```
FFWIf4/+VOlbDLgjU4HgtmV4IJDtqM9rGOZ42eFYmmc3eQO0GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmannS8j6YxmtpPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQQKDAh0cm9sb2xvbDCCASIwDQYJKoZIhvcNAQEBBQADggEP
...
j2PAOviqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPdl+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCAggAMB0GCWCGSAFlAwQBKgQQDViroIHStQgNOjR6nTUnuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTPskNCdCAHqdhOSqBwt65qUTZe3gBt
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrrxuHTWjFl
wEuqyd8X/ApkQsYFX/nhepOEIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxfOC1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs9OV/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----
```

Para generar todo en un archivo, añada el redirector > al ejemplo anterior para producir lo siguiente.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:Region:444455556666:certificate/certificate_ID \
     --passphrase fileb://path-to-passphrase-file \
     | jq -r '"\(.Certificate)\(.CertificateChain)\(.PrivateKey)"' \
     > /tmp/export.txt
```

Etiquetar certificados de AWS Certificate Manager

Una etiqueta es un rótulo que se puede asignar a un certificado de ACM. Cada etiqueta consta de una key (clave) y un value (valor). Puede usar la consola de AWS Certificate Manager, AWS Command Line Interface (AWS CLI) o la API de ACM para agregar, ver o eliminar etiquetas de certificados de ACM. Puede elegir qué etiquetas mostrar en la consola de ACM.

También puede crear etiquetas personalizadas que se adapten mejor a sus necesidades. Por ejemplo, puede etiquetar varios certificados de ACM con una etiqueta `Environment = Prod` o `Environment = Beta` a fin de identificar para qué entorno está previsto cada certificado de ACM. La siguiente lista incluye algunos ejemplos adicionales de etiquetas personalizadas:

- `Admin = Alice`
- `Purpose = Website`
- `Protocol = TLS`
- `Registrar = Route53`

Otros recursos de AWS también admiten etiquetado. Por lo tanto, puede asignar la misma etiqueta a diferentes recursos para indicar si están relacionados. Por ejemplo, puede asignar una etiqueta como `Website = example.com` al certificado de ACM, al balanceador de carga y a otros recursos utilizados para su sitio web example.com.

Temas

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas del certificado de ACM:

- El número máximo de etiquetas por certificado de ACM es 50.
- La longitud máxima de una etiqueta de clave es 127 caracteres.
- La longitud máxima de un valor de etiqueta es 255 caracteres.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.

- El prefijo `aws:` se reserva para uso de AWS; no puede añadir, editar o eliminar etiquetas cuya clave empiece por `aws:`. Las etiquetas que comienzan por `aws:` no cuentan para la cuota de etiquetas por recurso.
- Si pretende utilizar su esquema de etiquetado en múltiples servicios y recursos, recuerde que otros servicios pueden tener otras restricciones de caracteres permitidos. Consulte la documentación correspondiente a dicho servicio.
- Las etiquetas del certificado de ACM no están disponibles para utilizar en los Resource Groups y el editor de etiquetas de la AWS Management Console.

Para obtener información general sobre las convenciones de etiquetado de AWS, consulte Etiquetado de recursos de AWS.

Administración de etiquetas

Puede añadir, editar y eliminar etiquetas utilizando la consola de administración de AWS, la AWS Command Line Interface o la API de AWS Certificate Manager.

Administrar etiquetas (consola)

Puede utilizar la AWS Management Console para añadir, eliminar o editar etiquetas. También puede mostrar etiquetas en columnas.

Agregar una etiqueta

Utilice el siguiente procedimiento para agregar etiquetas mediante la consola de ACM.

Para añadir una etiqueta a un certificado (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Certificate Manager en https://console.aws.amazon.com/acm/home.
2. Elija la flecha situada al lado del certificado que desea etiquetar.
3. En el panel de detalles, desplácese hasta Tags.
4. Seleccione Edit y Add Tag.
5. Escriba una clave y un valor para la etiqueta.
6. Seleccione Save.

Eliminar una etiqueta

Utilice el siguiente procedimiento para eliminar etiquetas mediante la consola de ACM.

Para eliminar una etiqueta (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Certificate Manager en https://console.aws.amazon.com/acm/home.
2. Elija la flecha junto al certificado que tiene la etiqueta que desea eliminar.
3. En el panel de detalles, desplácese hasta Tags.
4. Elija Edit (Editar).
5. Elija la X situada al lado de la etiqueta que desea eliminar.
6. Seleccione Save.

Editar una etiqueta

Utilice el siguiente procedimiento para editar etiquetas mediante la consola de ACM.

Para editar una etiqueta (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Certificate Manager en https://console.aws.amazon.com/acm/home.
2. Elija la flecha situada al lado del certificado que desea editar.
3. En el panel de detalles, desplácese hasta Tags.
4. Elija Edit (Editar).
5. Modifique la clave o el valor de la etiqueta que desea cambiar.
6. Seleccione Save.

Mostrar etiquetas en columnas

Utilice el siguiente procedimiento para mostrar etiquetas en columnas en la consola de ACM.

Para mostrar las etiquetas en columnas (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Certificate Manager en https://console.aws.amazon.com/acm/home.

2. Elija las etiquetas que desee mostrar eligiendo el icono de engranaje

   situado en la esquina superior derecha de la consola.
3. Seleccione la casilla de verificación situada al lado de la etiqueta que desea mostrar en una columna.

Administrar etiquetas (CLI)

Consulte los siguientes temas para aprender a añadir, mostrar y eliminar etiquetas utilizando la AWS CLI.

- add-tags-to-certificate
- list-tags-for-certificate
- remove-tags-from-certificate

Administrar etiquetas (API de ACM)

Consulte los siguientes temas para aprender a añadir, listar y eliminar etiquetas utilizando la API.

- AddTagsToCertificate
- ListTagsForCertificate
- RemoveTagsFromCertificate

Supervisión y registro AWS Certificate Manager

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Certificate Manager sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca alguna.

En los siguientes temas se describen las herramientas de AWS supervisión de la nube disponibles para su uso con ACM.

Temas

Uso de Amazon EventBridge

Puede usar Amazon EventBridge (anteriormente CloudWatch Events) para automatizar sus AWS servicios y responder automáticamente a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios en los recursos. Los eventos de AWS los servicios, incluido ACM, se envían a Amazon casi EventBridge en tiempo real. Puede utilizar eventos para activar objetivos como AWS Lambda funciones, AWS Batch trabajos, temas de Amazon SNS y muchos otros. Para obtener más información, consulta ¿Qué es Amazon EventBridge?

Temas

EventBridge Soporte de Amazon para ACM

En este tema se enumeran y describen los eventos relacionados con la ACM compatibles con Amazon EventBridge.

Evento próximo a la caducidad del certificado ACM

ACM envía eventos con vencimientos diarios para todos los certificados activos (públicos, privados e importados) a partir de 45 días antes de su fecha de vencimiento. Este tiempo se puede cambiar mediante la PutAccountConfigurationacción de la API ACM.

ACM inicia automáticamente la renovación de los certificados aptos que ha emitido, pero los certificados importados deben volver a emitirse y volver a importarse antes de que caduquen para evitar interrupciones. Para obtener más información, consulte Reimportar un certificado. Puede utilizar eventos de vencimiento para configurar la automatización a fin de volver a importar certificados a ACM. Para ver un ejemplo del uso de la automatización, consulte. AWS LambdaActivación de acciones con Amazon EventBridge en ACM

Los eventos de vencimiento próximo del certificado de ACM tienen la siguiente estructura.

```
{
  "version": "0",
  "id": "id",
  "detail-type": "ACM Certificate Approaching Expiration",
  "source": "aws.acm",
  "account": "account",
  "time": "2020-09-30T06:51:08Z",
  "region": "region",
  "resources": [
    "arn:aws:acm:region:account:certificate/certificate_ID"
  ],
  "detail": {
    "DaysToExpiry": 31,
    "CommonName": "example.com"
  }
}
```

Evento de vencimiento del certificado de ACM

> **Note**
>
> Los eventos de certificado caducado no están disponibles para los certificados importados.

Los clientes pueden escuchar este evento para que les avise si caduca un certificado público o privado emitido por ACM en su cuenta.

Los eventos de vencimiento del certificado de ACM tienen la siguiente estructura.

```
{
    "version": "0",
    "id": "id",
    "detail-type": "ACM Certificate Expired",
    "source": "aws.acm",
    "account": "account",
    "time": "2019-12-22T18:43:48Z",
    "region": "region",
    "resources": [
        "arn:aws:acm:region:account:certificate/certificate_ID"
     ],
     "detail": {
        "CertificateType" : "AMAZON_ISSUED" | "PRIVATE",
        "CommonName": "example.com",
        "DomainValidationMethod" : "EMAIL" | "DNS",
        "CertificateCreatedDate" : "2018-12-22T18:43:48Z",
        "CertificateExpirationDate" : "2019-12-22T18:43:48Z",
        "InUse" : TRUE | FALSE,
        "Exported" : TRUE | FALSE
    }
 }
```

Evento de certificado de ACM disponible

Los clientes pueden escuchar este evento para recibir una notificación cuando un certificado público o privado administrado esté listo para su uso. El evento se publica en fecha de emisión, renovación e importación. En el caso de un certificado privado, una vez que esté disponible, seguirá siendo necesaria la acción del cliente para implementarlo en los hosts.

Los eventos de certificado de ACM disponible tienen la siguiente estructura.

```
{
    "version": "0",
    "id": "id",
    "detail-type": "ACM Certificate Available",
    "source": "aws.acm",
    "account": "account",
    "time": "2019-12-22T18:43:48Z",
    "region": "region",
    "resources": [
        "arn:aws:acm:region:account:certificate/certificate_ID"
```

```
    ],
    "detail": {
       “Action” : "ISSUANCE" | "RENEWAL" | "IMPORT" | "REIMPORT",
       "CertificateType" : "AMAZON_ISSUED" | "PRIVATE" | "IMPORTED",
       "CommonName": "example.com",
       "DomainValidationMethod" : "EMAIL" | "DNS",
       "CertificateCreatedDate" : "2019-12-22T18:43:48Z",
       "CertificateExpirationDate" : "2019-12-22T18:43:48Z",
       "DaysToExpiry" : 395,
       "InUse" : TRUE | FALSE,
       "Exported" : TRUE | FALSE
     }
}
```

Evento de acción obligatoria para la renovación del certificado de ACM

> **Note**
>
> Acción de renovación del certificado Los eventos obligatorios no están disponibles para los certificados importados.

Los clientes pueden escuchar este evento para recibir una alerta cuando se deba realizar una acción por parte del cliente antes de poder renovar un certificado. Por ejemplo, si un cliente agrega registros de CAA que impiden que ACM renueve un certificado, ACM publica este evento cuando la renovación automática falla 45 días antes del vencimiento. Si el cliente no toma ninguna medida, ACM realizará nuevos intentos de renovación a los 30, 15 días, 3 días y 1 día, o hasta que el cliente tome medidas, el certificado expire o ya no sea apto para la renovación. Se publica un evento para cada uno de estos intentos de renovación.

Los eventos de acción obligatoria para la renovación del certificado de ACM tienen la siguiente estructura.

```
{
   "version": "0",
   "id": "id",
   "detail-type": "ACM Certificate Renewal Action Required",
   "source": "aws.acm",
   "account": "account",
   "time": "2019-12-22T18:43:48Z",
   "region": "region",
```

```
   "resources": [
       "arn:aws:acm:region:account:certificate/certificate_ID"
    ],
    "detail": {
       "CertificateType" : "AMAZON_ISSUED" | "PRIVATE",
       "CommonName": "example.com",
       "DomainValidationMethod" : "EMAIL" | "DNS",
       "RenewalStatusReason" : "CAA_ERROR" | "PENDING_DOMAIN_VALIDATION" |
 "NO_AVAILABLE_CONTACTS" | "ADDITIONAL_VERIFICATION_REQUIRED" | "DOMAIN_NOT_ALLOWED"
 | "INVALID_PUBLIC_DOMAIN" | "DOMAIN_VALIDATION_DENIED" | "PCA_LIMIT_EXCEEDED"
 | "PCA_INVALID_ARN" | "PCA_INVALID_STATE" | "PCA_REQUEST_FAILED" |
 "PCA_NAME_CONSTRAINTS_VALIDATION" | "PCA_RESOURCE_NOT_FOUND" | "PCA_INVALID_ARGS" |
 "PCA_INVALID_DURATION" | "PCA_ACCESS_DENIED" | "SLR_NOT_FOUND" | "OTHER",
       "DaysToExpiry": 30,
       "CertificateExpirationDate" : "2019-12-22T18:43:48Z",
       "InUse" : TRUE | FALSE,
       "Exported" : TRUE | FALSE
   }
}
```

AWS eventos de salud

AWS los eventos de salud se generan para los certificados de la ACM que pueden renovarse. Para obtener información acerca de la elegibilidad para la renovación, consulte Renovación administrada para certificados de ACM.

Los eventos de estado se generan en dos situaciones:

- Cuando ocurre la renovación satisfactoria de un certificado público o privado.
- Cuando un cliente debe tomar medidas para que haya una renovación. Esto puede ser hacer clic en un enlace de un mensaje de correo electrónico (para certificados validados por correo electrónico) o la resolución de un error. Con cada evento se incluye uno de los siguientes códigos de evento. Los códigos se exponen como variables que se pueden utilizar para filtrar.
  - `AWS_ACM_RENEWAL_STATE_CHANGE` (el certificado ha sido renovado, ha vencido o está por vencer)
  - `CAA_CHECK_FAILURE` (la comprobación de CAA ha fallado)
  - `AWS_ACM_RENEWAL_FAILURE` (para certificados firmados por una CA privada)

Los eventos de estado tienen la siguiente estructura. En este ejemplo, se ha generado un evento de `AWS_ACM_RENEWAL_STATE_CHANGE`.

```
{
   "source":[
      "aws.health"
   ],
   "detail-type":[
      "AWS Health Event"
   ],
   "detail":{
      "service":[
         "ACM"
      ],
      "eventTypeCategory":[
         "scheduledChange"
      ],
      "eventTypeCode":[
         "AWS_ACM_RENEWAL_STATE_CHANGE"
      ]
   }
}
```

Activación de acciones con Amazon EventBridge en ACM

Puede crear EventBridge reglas de Amazon basadas en estos eventos y usar la EventBridge consola de Amazon para configurar las acciones que se llevan a cabo cuando se detectan los eventos. En esta sección se proporcionan ejemplos de procedimientos para configurar EventBridge las reglas de Amazon y las acciones resultantes.

Temas

- Respuesta a un evento con Amazon SNS
- Respuesta a un evento con una función Lambda

Respuesta a un evento con Amazon SNS

En esta sección se muestra cómo configurar Amazon SNS para que envíe una notificación de texto siempre que ACM genere un evento de estado.

Complete el siguiente procedimiento para configurar una respuesta.

Para crear una EventBridge regla de Amazon y activar una acción

1. Crea una EventBridge regla de Amazon. Para obtener más información, consulta Cómo crear EventBridge reglas de Amazon que reaccionen a los eventos.

   a. En la EventBridge consola de Amazon, en https://console.aws.amazon.com/events/, dirígete a la página Eventos > Reglas y selecciona Crear regla.

   b. En la página Create rule (Crear regla), seleccione Event Pattern (Patrón de eventos).

   c. En Service Name (Nombre del servicio), elija Health (Estado) en el menú.

   d. En Event Type (Tipo de evento), elija Specific Health events (Eventos de estado específicos).

   e. Seleccione Specific service(s) (Servicios específicos) y elija ACM en el menú.

   f. Seleccione Specific event type category(s) (Categoría[s] específica[s] de tipo de evento) y elija accountNotification.

   g. Elija Any event type code (Cualquier código de tipo de evento).

   h. Elija Add resource (Agregar recurso).

   i. En el editor Event pattern preview (Vista previa de patrón de eventos), pegue el patrón JSON que emitió el evento. En este ejemplo se utiliza el patrón de la sección AWS eventos de salud.

```
{
   "source":[
      "aws.health"
   ],
   "detail-type":[
      "AWS Health Event"
   ],
   "detail":{
      "service":[
         "ACM"
      ],
      "eventTypeCategory":[
         "scheduledChange"
      ],
      "eventTypeCode":[
         "AWS_ACM_RENEWAL_STATE_CHANGE"
      ]
   }
```

```
}
```

2. Configure una acción.

   En la sección Targets (Destinos), puede elegir entre muchos servicios que pueden consumir su evento de forma inmediata, como Amazon Simple Notification Service (SNS), o puede elegir Lambda function (Función Lambda) para pasar el evento a código personalizado ejecutable. Para consultar un ejemplo de una implementación de AWS Lambda , consulte Respuesta a un evento con una función Lambda.

Respuesta a un evento con una función Lambda

Este procedimiento muestra cómo AWS Lambda escuchar en Amazon EventBridge, crear notificaciones con Amazon Simple Notification Service (SNS) y publicar los resultados en Amazon, lo que proporciona visibilidad a AWS Security Hub los administradores y equipos de seguridad.

Para configurar una función Lambda y un rol de IAM

1. En primer lugar, configure un rol AWS Identity and Access Management (de IAM) y defina los permisos que necesita la función Lambda. Esta práctica recomendada de seguridad brinda flexibilidad a la hora de designar quién tiene autorización para llamar a la función y de limitar los permisos concedidos a esa persona. No se recomienda ejecutar la mayoría de AWS las operaciones directamente con una cuenta de usuario y, especialmente, con una cuenta de administrador.

   Abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. Utilice el editor de políticas de JSON para crear la política definida en la siguiente plantilla. Proporcione su propia región y los detalles AWS de su cuenta. Para obtener más información, consulte Creación de políticas en la pestaña de JSON.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"LambdaCertificateExpiryPolicy1",
         "Effect":"Allow",
         "Action":"logs:CreateLogGroup",
         "Resource":"arn:aws:logs:<region>:<AWS-ACCT-NUMBER>:*"
      },
      {
```

```
         "Sid":"LambdaCertificateExpiryPolicy2",
         "Effect":"Allow",
         "Action":[
            "logs:CreateLogStream",
            "logs:PutLogEvents"
         ],
         "Resource":[
            "arn:aws:logs:<region>:<AWS-ACCT-NUMBER>:log-group:/aws/lambda/handle-
expiring-certificates:*"
         ]
      },
      {
         "Sid":"LambdaCertificateExpiryPolicy3",
         "Effect":"Allow",
         "Action":[
            "acm:DescribeCertificate",
            "acm:GetCertificate",
            "acm:ListCertificates",
            "acm:ListTagsForCertificate"
         ],
         "Resource":"*"
      },
      {
         "Sid":"LambdaCertificateExpiryPolicy4",
         "Effect":"Allow",
         "Action":"SNS:Publish",
         "Resource":"*"
      },
      {
         "Sid":"LambdaCertificateExpiryPolicy5",
         "Effect":"Allow",
         "Action":[
            "SecurityHub:BatchImportFindings",
            "SecurityHub:BatchUpdateFindings",
            "SecurityHub:DescribeHub"
         ],
         "Resource":"*"
      },
      {
         "Sid":"LambdaCertificateExpiryPolicy6",
         "Effect":"Allow",
         "Action":"cloudwatch:ListMetrics",
         "Resource":"*"
      }
```

```
    ]
}
```

3. Cree un rol de IAM y adjúntele la política nueva. Para obtener información sobre cómo crear un rol de IAM y adjuntar una política, consulte Crear un rol para un AWS servicio (consola).
4. Abra la AWS Lambda consola en https://console.aws.amazon.com/lambda/.
5. Cree la función Lambda. Para obtener más información, consulte Crear una función Lambda con la consola. Realice los siguientes pasos:

   a. En la página Create function (Crear función), elija la opción Author from scratch (Crear desde cero) para crear la función.

   b. Especifique un nombre como «handle-expiring-certificates» en el campo Nombre de la función.

   c. En la lista Runtime (Tiempo de ejecución), elija Python 3.8.

   d. Expanda Change default execution role (Cambiar rol de ejecución predeterminado) y elija Use an existing role (Utilizar un rol existente).

   e. En la lista Existing role (Rol existente), elija el rol que creó antes.

   f. Elija Crear función.

   g. En Function code (Código de la función), inserte el siguiente código:

```
# Copyright 2021 Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: MIT-0
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
 of this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy,
 modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software,
 and to
# permit persons to whom the Software is furnished to do so.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
 COPYRIGHT
```

```
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
 ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH
 THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

import json
import boto3
import os
from datetime import datetime, timedelta, timezone
# ----------------------------------------
# setup global data
# ----------------------------------------
utc = timezone.utc
# make today timezone aware
today = datetime.now().replace(tzinfo=utc)
# set up time window for alert - default to 45 if its missing
if os.environ.get('EXPIRY_DAYS') is None:
    expiry_days = 45
else:
    expiry_days = int(os.environ['EXPIRY_DAYS'])
expiry_window = today + timedelta(days = expiry_days)
def lambda_handler(event, context):
    # if this is coming from the ACM event, its for a single certificate
    if (event['detail-type'] == "ACM Certificate Approaching Expiration"):
        response = handle_single_cert(event, context.invoked_function_arn)
    return {
        'statusCode': 200,
        'body': response
    }
def handle_single_cert(event, context_arn):
    cert_client = boto3.client('acm')
    cert_details =
 cert_client.describe_certificate(CertificateArn=event['resources'][0])
    result = 'The following certificate is expiring within ' + str(expiry_days)
 + ' days: ' + cert_details['Certificate']['DomainName']
    # check the expiry window before logging to Security Hub and sending an SNS
    if cert_details['Certificate']['NotAfter'] < expiry_window:
        # This call is the text going into the SNS notification
        result = result + ' (' + cert_details['Certificate']['CertificateArn']
 + ') '
        # this call is publishing to SH
        result = result + ' - ' + log_finding_to_sh(event, cert_details,
 context_arn)
```

```
        # if there's an SNS topic, publish a notification to it
        if os.environ.get('SNS_TOPIC_ARN') is None:
            response = result
        else:
            sns_client = boto3.client('sns')
            response = sns_client.publish(TopicArn=os.environ['SNS_TOPIC_ARN'],
 Message=result, Subject='Certificate Expiration Notification')
    return result
def log_finding_to_sh(event, cert_details, context_arn):
    # setup for security hub
    sh_region = get_sh_region(event['region'])
    sh_hub_arn = "arn:aws:securityhub:{0}:{1}:hub/default".format(sh_region,
 event['account'])
    sh_product_arn = "arn:aws:securityhub:{0}:{1}:product/{1}/
default".format(sh_region, event['account'])
    # check if security hub is enabled, and if the hub arn exists
    sh_client = boto3.client('securityhub', region_name = sh_region)
    try:
        sh_enabled = sh_client.describe_hub(HubArn = sh_hub_arn)
    # the previous command throws an error indicating the hub doesn't exist or
 lambda doesn't have rights to it so we'll stop attempting to use it
    except Exception as error:
        sh_enabled = None
        print ('Default Security Hub product doesn\'t exist')
        response = 'Security Hub disabled'
    # This is used to generate the URL to the cert in the Security Hub Findings
 to link directly to it
    cert_id = right(cert_details['Certificate']['CertificateArn'], 36)
    if sh_enabled:
        # set up a new findings list
        new_findings = []
            # add expiring certificate to the new findings list
        new_findings.append({
            "SchemaVersion": "2018-10-08",
            "Id": cert_id,
            "ProductArn": sh_product_arn,
            "GeneratorId": context_arn,
            "AwsAccountId": event['account'],
            "Types": [
                "Software and Configuration Checks/AWS Config Analysis"
            ],
            "CreatedAt": event['time'],
            "UpdatedAt": event['time'],
            "Severity": {
```

```
                "Original": '89.0',
                "Label": 'HIGH'
            },
            "Title": 'Certificate expiration',
            "Description": 'cert expiry',
            'Remediation': {
                'Recommendation': {
                    'Text': 'A new certificate for ' +
 cert_details['Certificate']['DomainName'] + ' should be imported to replace
 the existing imported certificate before expiration',
                    'Url': "https://console.aws.amazon.com/acm/home?region=" +
 event['region'] + "#/?id=" + cert_id
                }
            },
            'Resources': [
                {
                    'Id': event['id'],
                    'Type': 'ACM Certificate',
                    'Partition': 'aws',
                    'Region': event['region']
                }
            ],
            'Compliance': {'Status': 'WARNING'}
        })
        # push any new findings to security hub
        if new_findings:
            try:
                response =
 sh_client.batch_import_findings(Findings=new_findings)
                if response['FailedCount'] > 0:
                    print("Failed to import {}
 findings".format(response['FailedCount']))
            except Exception as error:
                print("Error: ", error)
                raise
    return json.dumps(response)
# function to setup the sh region
def get_sh_region(event_region):
    # security hub findings may need to go to a different region so set that
 here
    if os.environ.get('SECURITY_HUB_REGION') is None:
        sh_region_local = event_region
    else:
        sh_region_local = os.environ['SECURITY_HUB_REGION']
```

```
    return sh_region_local
# quick function to trim off right side of a string
def right(value, count):
    # To get right part of string, use negative first index in slice.
    return value[-count:]
```

h. En Environment variables (Variables de entorno), elija Edit (Editar) y, opcionalmente, agregue las siguientes variables.

- (Opcional) EXPIRY_DAYS

  Especifica el tiempo de espera, en días, antes de que se envíe el aviso de vencimiento del certificado. La función tiene un valor predeterminado de 45 días, pero puede especificar valores personalizados.

- (Opcional) SNS_TOPIC_ARN

  Especifica un ARN para un Amazon SNS. Proporcione el ARN completo en el formato arn:aws:sns:*<region>*:*<account-number>*:*<topic-name>*.

- (Opcional) SECURITY_HUB_REGION

  Especifica AWS Security Hub uno en una región diferente. Si no se especifica, se utiliza la región de la función Lambda en ejecución. Si la función se ejecuta en varias regiones, puede ser conveniente que todos los mensajes de certificado vayan a Security Hub en una sola región.

i. En Basic settings (Configuración básica), establezca el valor Timeout (Tiempo de espera) en 30 segundos.

j. En la parte superior de la página, elija Deploy (Implementar).

Complete las tareas del siguiente procedimiento para comenzar a utilizar esta solución.

Automatizar un aviso de vencimiento por correo electrónico

En este ejemplo, proporcionamos un solo correo electrónico para cada certificado que caduca en el momento en que Amazon EventBridge genera el evento. De forma predeterminada, cada día ACM genera un evento para un certificado al que le quedan 45 días o menos para vencer. (Este período se puede personalizar mediante el PutAccountConfigurationfuncionamiento de la API ACM). Cada uno de estos eventos activa la siguiente cadena de acciones automatizadas:

```
ACM raises Amazon EventBridge event #
```

```
>>>>>>> events

          Event matches Amazon EventBridge rule #

                    Rule calls Lambda function #

                              Function sends SNS email and logs a Finding in Security
 Hub
```

1. Cree la función Lambda y configure los permisos. (Ya se ha completado, consulte Para configurar una función Lambda y un rol de IAM).
2. Cree un tema de SNS estándar para la función Lambda que se utilizará a fin de enviar notificaciones. Para obtener más información, consulte Creación de un tema de Amazon SNS.
3. Suscriba las partes interesadas al tema de SNS nuevo. Para obtener más información, consulte Suscripción a un tema de Amazon SNS.
4. Cree una EventBridge regla de Amazon para activar la función Lambda. Para obtener más información, consulta Cómo crear EventBridge reglas de Amazon que reaccionen a los eventos.

   En la EventBridge consola de Amazon, en https://console.aws.amazon.com/events/, dirígete a la página Eventos > Reglas y selecciona Crear regla. Especifique el Service Name (Nombre del servicio), Event Type (Tipo de evento) y Lambda function (Función Lambda). En el editor Event Pattern preview (Vista previa de patrón de eventos), pegue el siguiente código:

   ```
   {
     "source": [
       "aws.acm"
     ],
     "detail-type": [
       "ACM Certificate Approaching Expiration"
     ]
   }
   ```

   Un evento como el que recibe Lambda se muestra en Show sample event(s) (Mostrar eventos de muestra):

   ```
   {
     "version": "0",
     "id": "9c95e8e4-96a4-ef3f-b739-b6aa5b193afb",
     "detail-type": "ACM Certificate Approaching Expiration",
   ```

```
  "source": "aws.acm",
  "account": "123456789012",
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:acm:us-east-1:123456789012:certificate/61f50cd4-45b9-4259-b049-
d0a53682fa4b"
  ],
  "detail": {
    "DaysToExpiry": 31,
    "CommonName": "My Awesome Service"
  }
}
```

Eliminación

Una vez que ya no necesite la configuración de ejemplo, o cualquier configuración, es una práctica recomendada eliminar todos los rastros de esta para evitar problemas de seguridad y cargos futuros inesperados:

- Política y rol de IAM
- Función de Lambda
- CloudWatch Regla de eventos
- CloudWatch Registros asociados a Lambda
- Tema de SNS

Utilizándolo con CloudTrail AWS Certificate Manager

AWS Certificate Manager está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en ACM. CloudTrail está activado de forma predeterminada en su AWS cuenta. CloudTrail captura las llamadas a la API de ACM como eventos, incluidas las llamadas desde la consola de ACM y las llamadas en código a las operaciones de la API de ACM. Si configura una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de ACM. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por usted CloudTrail, puede determinar la solicitud que se realizó a ACM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles

adicionales. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos. Cuando se produce una actividad de eventos admitida en ACM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS .

Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos.

Para obtener más información al respecto CloudTrail, consulte la siguiente documentación:

- AWS CloudTrail Guía del usuario.
- Introducción a la creación de registros de seguimiento
- CloudTrail Servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Temas

- Se admiten acciones de la API ACM en el registro CloudTrail
- Registro de llamadas a la API para servicios integrados

Se admiten acciones de la API ACM en el registro CloudTrail

ACM admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario Usuario raíz de la cuenta de AWS o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio AWS

Para obtener más información, consulte el elemento CloudTrailUserIdentity.

Las siguientes secciones proporcionan registros de ejemplo para las operaciones de la API admitidas.

- Adición de etiquetas a un certificado (AddTagsToCertificate)
- Eliminación de un certificado (DeleteCertificate)
- Descripción de un certificado (DescribeCertificate)
- Exportación de un certificado (ExportCertificate)
- Importación de un certificado (ImportCertificate)
- Enumeración de certificados (ListCertificates)
- Enumeración de etiquetas de un certificado (ListTagsForCertificate)
- Eliminación de etiquetas de un certificado (RemoveTagsFromCertificate)
- Solicitud de un certificado (RequestCertificate)
- Reenvío del correo electrónico de validación (ResendValidationEmail)
- Recuperación de un certificado (GetCertificate)

Adición de etiquetas a un certificado (AddTagsToCertificate)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la API. AddTagsToCertificate


```
{

   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-04-06T13:53:53Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"AddTagsToCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
```

```
         "userAgent":"aws-cli/1.10.16",
         "requestParameters":{
            "tags":[
               {
                  "value":"Alice",
                  "key":"Admin"
               }
            ],
            "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
         },
         "responseElements":null,
         "requestID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Eliminación de un certificado (DeleteCertificate)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la DeleteCertificateAPI.

```
{

   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:26Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"DeleteCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
```

```
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
         },
         "responseElements":null,
         "requestID":"01234567-89ab-cdef-0123-456789abcdef",
         "eventID":"01234567-89ab-cdef-0123-456789abcdef",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Descripción de un certificado (DescribeCertificate)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la DescribeCertificateAPI.

> **Note**
>
> El CloudTrail registro de la `DescribeCertificate` operación no muestra información sobre el certificado ACM que especifique. Puede ver la información sobre el certificado mediante la consola AWS Command Line Interface, la o la DescribeCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:42Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"DescribeCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
```

```
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
         },
         "responseElements":null,
         "requestID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Exportación de un certificado (ExportCertificate)

En el siguiente CloudTrail ejemplo, se muestran los resultados de una llamada a la ExportCertificateAPI.

```
{
   "Records":[
      {
         "version":"0",
         "id":"01234567-89ab-cdef-0123-456789abcdef",
         "detail-type":"AWS API Call via CloudTrail",
         "source":"aws.acm",
         "account":"123456789012",
         "time":"2018-05-24T15:28:11Z",
         "region":"us-east-1",
         "resources":[

         ],
         "detail":{
            "eventVersion":"1.04",
            "userIdentity":{
               "type":"Root",
               "principalId":"123456789012",
               "arn":"arn:aws:iam::123456789012:user/Alice",
               "accountId":"123456789012",
               "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
               "userName":"Alice"
            },
            "eventTime":"2018-05-24T15:28:11Z",
            "eventSource":"acm.amazonaws.com",
```

```
            "eventName":"ExportCertificate",
            "awsRegion":"us-east-1",
            "sourceIPAddress":"192.0.2.0",
            "userAgent":"aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4",
            "requestParameters":{
               "passphrase":{
                  "hb":[
                     42,
                     42,
                     42,
                     42,
                     42,
                     42,
                     42,
                     42,
                     42,
                     42
                  ],
                  "offset":0,
                  "isReadOnly":false,
                  "bigEndian":true,
                  "nativeByteOrder":false,
                  "mark":-1,
                  "position":0,
                  "limit":10,
                  "capacity":10,
                  "address":0
               },
               "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
            },
            "responseElements":{
                "certificateChain":
                "-----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----
                -----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----",
                "privateKey":"**********",
                "certificate":
                "-----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----"
```

```
            },
            "requestID":"01234567-89ab-cdef-0123-456789abcdef",
            "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
            "eventType":"AwsApiCall"
         }
      }
   ]
}
```

Importación de un certificado (ImportCertificate)

El siguiente ejemplo muestra la entrada de CloudTrail registro que registra una llamada a la operación de la ImportCertificateAPI de ACM.

```
{
   "eventVersion":"1.04",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::111122223333:user/Alice",
      "accountId":"111122223333",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"Alice"
   },
   "eventTime":"2016-10-04T16:01:30Z",
   "eventSource":"acm.amazonaws.com",
   "eventName":"ImportCertificate",
   "awsRegion":"ap-southeast-2",
   "sourceIPAddress":"54.240.193.129",
   "userAgent":"Coral/Netty",
   "requestParameters":{
      "privateKey":{
         "hb":[
            "byte",
            "byte",
            "byte",
            "..."
         ],
         "offset":0,
         "isReadOnly":false,
         "bigEndian":true,
         "nativeByteOrder":false,
         "mark":-1,
```

```
         "position":0,
         "limit":1674,
         "capacity":1674,
         "address":0
      },
      "certificateChain":{
         "hb":[
            "byte",
            "byte",
            "byte",
            "..."
         ],
         "offset":0,
         "isReadOnly":false,
         "bigEndian":true,
         "nativeByteOrder":false,
         "mark":-1,
         "position":0,
         "limit":2105,
         "capacity":2105,
         "address":0
      },
      "certificate":{
         "hb":[
            "byte",
            "byte",
            "byte",
            "..."
         ],
         "offset":0,
         "isReadOnly":false,
         "bigEndian":true,
         "nativeByteOrder":false,
         "mark":-1,
         "position":0,
         "limit":2503,
         "capacity":2503,
         "address":0
      }
   },
   "responseElements":{
      "certificateArn":"arn:aws:acm:ap-
southeast-2:111122223333:certificate/01234567-89ab-cdef-0123-456789abcdef"
   },
```

```
   "requestID":"01234567-89ab-cdef-0123-456789abcdef",
   "eventID":"01234567-89ab-cdef-0123-456789abcdef",
   "eventType":"AwsApiCall",
   "recipientAccountId":"111122223333"
}
```

Enumeración de certificados (ListCertificates)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la ListCertificatesAPI.

> **Note**
>
> El CloudTrail registro de la `ListCertificates` operación no muestra los certificados de ACM. Puede ver la lista de certificados mediante la consola AWS Command Line Interface, la o la ListCertificatesAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:43Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ListCertificates",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "maxItems":1000,
            "certificateStatuses":[
               "ISSUED"
            ]
         },
         "responseElements":null,
```

```
         "requestID":"74c99844-ec9c-11e5-ac34-d1e4dfe1a11b",
         "eventID":"cdfe1051-88aa-4aa3-8c33-a325270bff21",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Enumeración de etiquetas de un certificado (ListTagsForCertificate)

En el siguiente CloudTrail ejemplo, se muestran los resultados de una llamada a la ListTagsForCertificateAPI.

> **Note**
>
> El CloudTrail registro de la `ListTagsForCertificate` operación no muestra tus etiquetas. Puede ver la lista de etiquetas mediante la consola AWS Command Line Interface, la o la ListTagsForCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-04-06T13:30:11Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ListTagsForCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.10.16",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
         },
```

```
         "responseElements":null,
         "requestID":"b010767f-fbfb-11e5-b596-79e9a97a2544",
         "eventID":"32181be6-a4a0-48d3-8014-c0d972b5163b",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Eliminación de etiquetas de un certificado (RemoveTagsFromCertificate)

En el siguiente CloudTrail ejemplo, se muestran los resultados de una llamada a la RemoveTagsFromCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-04-06T14:10:01Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"RemoveTagsFromCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.10.16",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
            "tags":[
               {
                  "value":"Bob",
                  "key":"Admin"
               }
            ]
         },
         "responseElements":null,
```

```
         "requestID":"40ded461-fc01-11e5-a747-85804766d6c9",
         "eventID":"0cfa142e-ef74-4b21-9515-47197780c424",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Solicitud de un certificado (RequestCertificate)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la RequestCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:49Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"RequestCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "subjectAlternativeNames":[
               "example.net"
            ],
            "domainName":"example.com",
            "domainValidationOptions":[
               {
                  "domainName":"example.com",
                  "validationDomain":"example.com"
               },
               {
                  "domainName":"example.net",
                  "validationDomain":"example.net"
```

```
               }
            ],
            "idempotencyToken":"8186023d89681c3ad5"
         },
         "responseElements":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
         },
         "requestID":"77dacef3-ec9c-11e5-ac34-d1e4dfe1a11b",
         "eventID":"a4954cdb-8f38-44c7-8927-a38ad4be3ac8",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Reenvío del correo electrónico de validación (ResendValidationEmail)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la ResendValidationEmailAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-17T23:58:25Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ResendValidationEmail",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "domain":"example.com",
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
```

```
            "validationDomain":"example.com"
         },
         "responseElements":null,
         "requestID":"23760b88-ec9c-11e5-b6f4-cb861a6f0a28",
         "eventID":"41c11b06-ca91-4c1c-8c61-af349ea8bab8",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Recuperación de un certificado (GetCertificate)

El siguiente CloudTrail ejemplo muestra los resultados de una llamada a la GetCertificateAPI.

```
{

   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:41Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"GetCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
         },
         "responseElements":{
            "certificateChain":

            "-----BEGIN CERTIFICATE-----
            Base64-encoded certificate chain
```

```
            -----END CERTIFICATE-----",
            "certificate":
            "-----BEGIN CERTIFICATE-----
            Base64-encoded certificate
            -----END CERTIFICATE-----"

         },
         "requestID":"744dd891-ec9c-11e5-ac34-d1e4dfe1a11b",
         "eventID":"7aa4f909-00dd-478a-9a00-b2709bcad2bb",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Registro de llamadas a la API para servicios integrados

Puede utilizarlos CloudTrail para auditar las llamadas a la API realizadas por los servicios que están integrados con ACM. Para obtener más información sobre su uso CloudTrail, consulte la Guía del AWS CloudTrail usuario. Los siguientes ejemplos muestran los tipos de registros que se pueden generar en función de los recursos de AWS en los que aprovisiona el certificado de ACM.

Temas

- Creación de un balanceador de carga

Creación de un balanceador de carga

Se puede utilizar CloudTrail para auditar las llamadas a la API realizadas por los servicios que están integrados con ACM. Para obtener más información sobre su uso CloudTrail, consulte la Guía del AWS CloudTrail usuario. Los siguientes ejemplos muestran los tipos de registros que se pueden generar en función de AWS los recursos con los que se aprovisione el certificado ACM.

Temas

- Creación de un balanceador de carga
- Registro de una instancia de Amazon EC2 con un balanceador de carga
- Cifrando una clave privada
- Descifrando una clave privada

Creación de un balanceador de carga

El siguiente ejemplo muestra una llamada a la función `CreateLoadBalancer` por parte de una usuaria de IAM llamada Alice. El nombre del balanceador de carga es `TestLinuxDefault` y el agente de escucha se crea con un certificado de ACM.


```
{

   "eventVersion":"1.03",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::111122223333:user/Alice",
      "accountId":"111122223333",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"Alice"
   },
   "eventTime":"2016-01-01T21:10:36Z",
   "eventSource":"elasticloadbalancing.amazonaws.com",
   "eventName":"CreateLoadBalancer",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"192.0.2.0/24",
   "userAgent":"aws-cli/1.9.15",
   "requestParameters":{
      "availabilityZones":[
         "us-east-1b"
      ],
      "loadBalancerName":"LinuxTest",
      "listeners":[
         {
            "sSLCertificateId":"arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
            "protocol":"HTTPS",
            "loadBalancerPort":443,
            "instanceProtocol":"HTTP",
            "instancePort":80
         }
      ]
   },
   "responseElements":{
      "dNSName":"LinuxTest-1234567890.us-east-1.elb.amazonaws.com"
   },
   "requestID":"19669c3b-b0cc-11e5-85b2-57397210a2e5",
```

```
   "eventID":"5d6c00c9-a9b8-46ef-9f3b-4589f5be63f7",
   "eventType":"AwsApiCall",
   "recipientAccountId":"111122223333"
}
```

Registro de una instancia de Amazon EC2 con un balanceador de carga

Cuando aprovisiona su sitio web o aplicación en una instancia de Amazon Elastic Compute Cloud (Amazon EC2), el balanceador de carga debe reconocer dicha instancia. Esto se puede realizar mediante la consola de Elastic Load Balancing o la AWS Command Line Interface. En el siguiente ejemplo, se muestra una llamada a un balanceador `RegisterInstancesWithLoadBalancer` de cargas con el nombre de la AWS cuenta LinuxTest 123456789012.

```
{
   "eventVersion":"1.03",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/ALice",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"Alice",
      "sessionContext":{
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2016-01-01T19:35:52Z"
         }
      },
      "invokedBy":"signin.amazonaws.com"
   },
   "eventTime":"2016-01-01T21:11:45Z",
   "eventSource":"elasticloadbalancing.amazonaws.com",
   "eventName":"RegisterInstancesWithLoadBalancer",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"192.0.2.0/24",
   "userAgent":"signin.amazonaws.com",
   "requestParameters":{
      "loadBalancerName":"LinuxTest",
      "instances":[
         {
            "instanceId":"i-c67f4e78"
         }
      ]
```

```
   },
   "responseElements":{
      "instances":[
         {
            "instanceId":"i-c67f4e78"
         }
      ]
   },
   "requestID":"438b07dc-b0cc-11e5-8afb-cda7ba020551",
   "eventID":"9f284ca6-cbe5-42a1-8251-4f0e6b5739d6",
   "eventType":"AwsApiCall",
   "recipientAccountId":"123456789012"
}
```

Cifrando una clave privada

El siguiente ejemplo muestra una llamada `Encrypt` que cifra la clave privada asociada a un certificado de ACM. El cifrado se realiza en AWS.

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::111122223333:user/acm",
            "accountId":"111122223333",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"acm"
         },
         "eventTime":"2016-01-05T18:36:29Z",
         "eventSource":"kms.amazonaws.com",
         "eventName":"Encrypt",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"AWS Internal",
         "userAgent":"aws-internal",
         "requestParameters":{
            "keyId":"arn:aws:kms:us-east-1:123456789012:alias/aws/acm",
            "encryptionContext":{
               "aws:acm:arn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
            }
```

```
         },
         "responseElements":null,
         "requestID":"3c417351-b3db-11e5-9a24-7d9457362fcc",
         "eventID":"1794fe70-796a-45f5-811b-6584948f24ac",
         "readOnly":true,
         "resources":[
            {
               "ARN":"arn:aws:kms:us-
east-1:123456789012:key/87654321-4321-4321-4321-210987654321",
               "accountId":"123456789012"
            }
         ],
         "eventType":"AwsServiceEvent",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Descifrando una clave privada

El siguiente ejemplo muestra una llamada `Decrypt` que descifra la clave privada asociada a un certificado de ACM. El descifrado se realiza desde dentro y la clave AWS descifrada nunca sale. AWS

```
{
   "eventVersion":"1.03",
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE:1aba0dc8b3a728d6998c234a99178eff",
      "arn":"arn:aws:sts::111122223333:assumed-role/
DecryptACMCertificate/1aba0dc8b3a728d6998c234a99178eff",
      "accountId":"111122223333",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "sessionContext":{
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2016-01-01T21:13:28Z"
         },
         "sessionIssuer":{
            "type":"Role",
            "principalId":"APKAEIBAERJR2EXAMPLE",
            "arn":"arn:aws:iam::111122223333:role/DecryptACMCertificate",
            "accountId":"111122223333",
```

```
            "userName":"DecryptACMCertificate"
         }
      }
   },
   "eventTime":"2016-01-01T21:13:28Z",
   "eventSource":"kms.amazonaws.com",
   "eventName":"Decrypt",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-internal/3",
   "requestParameters":{
      "encryptionContext":{
         "aws:elasticloadbalancing:arn":"arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/LinuxTest",
         "aws:acm:arn":"arn:aws:acm:us-
east-1:123456789012:certificate/87654321-4321-4321-4321-210987654321"
      }
   },
   "responseElements":null,
   "requestID":"809a70ff-b0cc-11e5-8f42-c7fdf1cb6e6a",
   "eventID":"7f89f7a7-baff-4802-8a88-851488607fb9",
   "readOnly":true,
   "resources":[
      {
         "ARN":"arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012",
         "accountId":"123456789012"
      }
   ],
   "eventType":"AwsServiceEvent",
   "recipientAccountId":"123456789012"
}
```


Métricas compatibles CloudWatch

Amazon CloudWatch es un servicio de monitorización de AWS recursos. Puede usarlo CloudWatch para recopilar métricas y realizar un seguimiento, configurar alarmas y reaccionar automáticamente ante los cambios en sus AWS recursos. ACM publica las métricas una vez al día para cada certificado de una cuenta hasta su vencimiento.

El espacio de nombres de `AWS/CertificateManager` incluye la siguiente métrica.

Métrica	Descripción	Unidad	Dimensiones
`DaysToExpiry`	Número de días hasta que caduque un certificado. ACM deja de publicar esta métrica después de que vence un certifica do.	Entero	CertificateArn • Valor: ARN del certificado

Para obtener más información sobre CloudWatch las métricas, consulta los siguientes temas:

- Uso de Amazon CloudWatch Metrics
- Creación de Amazon CloudWatch Alarms

Uso de la API (ejemplos de Java)

Puede utilizar la API de AWS Certificate Manager para interactuar con el servicio mediante programación enviando solicitudes HTTP. Para obtener más información, consulte la referencia de la API de AWS Certificate Manager.

Además de la API web (o API HTTP), puede utilizar los SDK y las herramientas de línea de comandos de AWS para interactuar con ACM y otros servicios. Para obtener más información, consulte Herramientas para Amazon Web Services.

En los temas siguientes se muestra cómo utilizar uno de los SDK de AWS, AWS SDK for Java, para realizar algunas de las operaciones disponibles en la API de AWS Certificate Manager.

Temas

Adición de etiquetas a un certificado

El siguiente ejemplo muestra cómo utilizar la función AddTagsToCertificate.

```
package com.amazonaws.samples;

import java.io.IOException;
import java.nio.ByteBuffer;
```

```
import java.nio.charset.StandardCharsets;
import java.nio.file.Files;
import java.nio.file.Paths;

import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 Certificate Manager
 * service.
 *
 * Input parameters:
 *   Accesskey - AWS access key
 *   SecretKey - AWS secret key
 *   CertificateArn - Use to reimport a certificate (not included in this example).
 *   region - AWS region
 *   Certificate - PEM file that contains the certificate to import. Ex: /data/certs/
servercert.pem
 *   CertificateChain - The certificate chain, not including the end-entity
 certificate.
 *   PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 *   CertificcateArn - The ARN of the imported certificate.
 *
 */
public class AWSCertificateManagerSample {

    public static void main(String[] args) throws IOException {
     String accessKey = "";
     String secretKey = "";
     String certificateArn = null;
     Regions region = Regions.DEFAULT_REGION;
     String serverCertFilePath = "";
     String privateKeyFilePath = "";
     String caCertFilePath = "";

     ImportCertificateRequest req = new ImportCertificateRequest()
       .withCertificate(getCertContent(serverCertFilePath))
```

```
        .withPrivateKey(getCertContent(privateKeyFilePath))

  .withCertificateChain(getCertContent(caCertFilePath)).withCertificateArn(certificateArn);

      AWSCertificateManager client =
  AWSCertificateManagerClientBuilder.standard().withRegion(region)
        .withCredentials(new AWSStaticCredentialsProvider(new
  BasicAWSCredentials(accessKey, secretKey)))
        .build();
      ImportCertificateResult result = client.importCertificate(req);

      System.out.println(result.getCertificateArn());

      List<Tag> expectedTags =
  ImmutableList.of(Tag.builder().withKey("key").withValue("value").build());

      AddTagsToCertificateRequest addTagsToCertificateRequest =
  AddTagsToCertificateRequest.builder()
              .withCertificateArn(result.getCertificateArn())
              .withTags(tags)
              .build();

      client.addTagsToCertificate(addTagsToCertificateRequest);
     }

     private static ByteBuffer getCertContent(String filePath) throws IOException {
      String fileContent = new String(Files.readAllBytes(Paths.get(filePath)));
      return StandardCharsets.UTF_8.encode(fileContent);
     }
}
```

Eliminación de un certificado

El siguiente ejemplo muestra cómo utilizar la función DeleteCertificate. Si lo realiza correctamente, la función devuelve un conjunto vacío {}.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.DeleteCertificateRequest;
import com.amazonaws.services.certificatemanager.model.DeleteCertificateResult;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceInUseException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the DeleteCertificate function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameter:
 *   CertificateArn - The ARN of the certificate to delete.
 *
 */

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception{

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load the credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and specify the ARN of the certificate to delete.
```

```
      DeleteCertificateRequest req = new DeleteCertificateRequest();

 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");

      // Delete the specified certificate.
      DeleteCertificateResult result = null;
      try {
         result = client.deleteCertificate(req);
      }
      catch (InvalidArnException ex)
      {
         throw ex;
      }
      catch (ResourceInUseException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
      }

      // Display the result.
      System.out.println(result);

   }
}
```

Descripción de un certificado

En el siguiente ejemplo se muestra cómo utilizar la función DescribeCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.DescribeCertificateRequest;
import com.amazonaws.services.certificatemanager.model.DescribeCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
```

```
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the DescribeCertificate function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameter:
 *   CertificateArn - The ARN of the certificate to be described.
 *
 * Output parameter:
 *   Certificate information
 *
 */

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception{

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load the credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and set the ARN of the certificate to be described.
      DescribeCertificateRequest req = new DescribeCertificateRequest();
```

```
 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");

      DescribeCertificateResult result = null;
      try{
         result = client.describeCertificate(req);
      }
      catch (InvalidArnException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
      }

      // Display the certificate information.
      System.out.println(result);

   }
}
```

Si se ejecuta correctamente, el ejemplo anterior mostrará información similar a la siguiente.

```
{
    Certificate: {
        CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012,
        DomainName: www.example.com,
        SubjectAlternativeNames: [www.example.com],
        DomainValidationOptions: [{
            DomainName: www.example.com,
        }],
        Serial: 10: 0a,
        Subject: C=US,
        ST=WA,
        L=Seattle,
        O=ExampleCompany,
        OU=sales,
        CN=www.example.com,
        Issuer: ExampleCompany,
        ImportedAt: FriOct0608: 17: 39PDT2017,
```

```
        Status: ISSUED,
        NotBefore: ThuOct0510: 14: 32PDT2017,
        NotAfter: SunOct0310: 14: 32PDT2027,
        KeyAlgorithm: RSA-2048,
        SignatureAlgorithm: SHA256WITHRSA,
        InUseBy: [],
        Type: IMPORTED,
    }
}
```

Exportación de un certificado

El siguiente ejemplo muestra cómo utilizar la función ExportCertificate. La función exporta un certificado privado emitido por una entidad de certificación (CA) privada en el formato PKCS #8. (No es posible exportar certificados públicos, tanto si los ha expedido ACM como si son importados). También exporta la cadena de certificados y la clave privada. En el ejemplo, la frase de contraseña de la clave se almacena en un archivo local.

```
package com.amazonaws.samples;

import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;


import com.amazonaws.services.certificatemanager.model.ExportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ExportCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.InvalidTagException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;

import java.io.FileNotFoundException;
import java.io.IOException;
import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
```

```
import java.nio.channels.FileChannel;

public class ExportCertificate {

   public static void main(String[] args) throws Exception {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.your_region)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Initialize a file descriptor for the passphrase file.
      RandomAccessFile file_passphrase = null;

      // Initialize a buffer for the passphrase.
      ByteBuffer buf_passphrase = null;

      // Create a file stream for reading the private key passphrase.
      try {
         file_passphrase = new RandomAccessFile("C:\\Temp\\password.txt", "r");
      }
      catch (IllegalArgumentException ex) {
         throw ex;
      }
      catch (SecurityException ex) {
         throw ex;
      }
      catch (FileNotFoundException ex) {
         throw ex;
      }
```

```
      // Create a channel to map the file.
      FileChannel channel_passphrase = file_passphrase.getChannel();

      // Map the file to the buffer.
      try {
         buf_passphrase = channel_passphrase.map(FileChannel.MapMode.READ_ONLY, 0,
channel_passphrase.size());

         // Clean up after the file is mapped.
         channel_passphrase.close();
         file_passphrase.close();
      }
      catch (IOException ex)
      {
         throw ex;
      }

      // Create a request object.
      ExportCertificateRequest req = new ExportCertificateRequest();

      // Set the certificate ARN.
      req.withCertificateArn("arn:aws:acm:region:account:"
            +"certificate/M12345678-1234-1234-1234-123456789012");

      // Set the passphrase.
      req.withPassphrase(buf_passphrase);

      // Export the certificate.
      ExportCertificateResult result = null;

      try {
         result = client.exportCertificate(req);
      }
      catch(InvalidArnException ex)
      {
         throw ex;
      }
      catch (InvalidTagException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
```

```
        }

        // Clear the buffer.
        buf_passphrase.clear();

        // Display the certificate and certificate chain.
        String certificate = result.getCertificate();
        System.out.println(certificate);

        String certificate_chain = result.getCertificateChain();
        System.out.println(certificate_chain);

        // This example retrieves but does not display the private key.
        String private_key = result.getPrivateKey();
    }
}
```

Recuperación de un certificado y una cadena de certificados

El siguiente ejemplo muestra cómo utilizar la función GetCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.GetCertificateRequest;
import com.amazonaws.services.certificatemanager.model.GetCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.RequestInProgressException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the GetCertificate function in the AWS
 Certificate
 * Manager service.
 *
```

```
 * Input parameter:
 *   CertificateArn - The ARN of the certificate to retrieve.
 *
 * Output parameters:
 *   Certificate - A base64-encoded certificate in PEM format.
 *   CertificateChain - The base64-encoded certificate chain in PEM format.
 *
 */

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception{

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load the credentials from the
 credential profiles file.", ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and set the ARN of the certificate to be described.
      GetCertificateRequest req = new GetCertificateRequest();

 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");

      // Retrieve the certificate and certificate chain.
      // If you recently requested the certificate, loop until it has been created.
      GetCertificateResult result = null;
      long totalTimeout = 120000l;
      long timeSlept = 0l;
      long sleepInterval = 10000l;
      while (result == null && timeSlept < totalTimeout) {
```

```
         try {
            result = client.getCertificate(req);
         }
         catch (RequestInProgressException ex) {
            Thread.sleep(sleepInterval);
         }
         catch (ResourceNotFoundException ex)
         {
            throw ex;
         }
         catch (InvalidArnException ex)
         {
            throw ex;
         }

         timeSlept += sleepInterval;
      }

      // Display the certificate information.
      System.out.println(result);
   }
}
```

El ejemplo anterior obtiene un resultado similar al siguiente.

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

Importación de un certificado

El siguiente ejemplo muestra cómo utilizar la función ImportCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 Certificate Manager
 * service.
 *
 * Input parameters:
 *   Certificate - PEM file that contains the certificate to import.
 *   CertificateArn - Use to reimport a certificate (not included in this example).
 *   CertificateChain - The certificate chain, not including the end-entity
 certificate.
 *   PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 *   CertificcateArn - The ARN of the imported certificate.
 *
 */
public class AWSCertificateManagerSample {

   public static void main(String[] args) throws Exception {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
```

```
        catch (Exception ex) {
            throw new AmazonClientException(
                "Cannot load the credentials from file.", ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
                .withRegion(Regions.US_EAST_1)
                .withCredentials(new AWSStaticCredentialsProvider(credentials))
                .build();

        // Initialize the file descriptors.
        RandomAccessFile file_certificate = null;
        RandomAccessFile file_chain = null;
        RandomAccessFile file_key = null;

        // Initialize the buffers.
        ByteBuffer buf_certificate = null;
        ByteBuffer buf_chain = null;
        ByteBuffer buf_key = null;

        // Create the file streams for reading.
        try {
           file_certificate = new RandomAccessFile("C:\\Temp\\certificate.pem", "r");
           file_chain = new RandomAccessFile("C:\\Temp\\chain.pem", "r");
           file_key = new RandomAccessFile("C:\\Temp\\private_key.pem", "r");
        }
        catch (IllegalArgumentException ex) {
           throw ex;
        }
        catch (SecurityException ex) {
           throw ex;
        }
        catch (FileNotFoundException ex) {
           throw ex;
        }

        // Create channels for mapping the files.
        FileChannel channel_certificate = file_certificate.getChannel();
        FileChannel channel_chain = file_chain.getChannel();
        FileChannel channel_key = file_key.getChannel();

        // Map the files to buffers.
        try {
```

```
        buf_certificate = channel_certificate.map(FileChannel.MapMode.READ_ONLY, 0,
channel_certificate.size());
        buf_chain = channel_chain.map(FileChannel.MapMode.READ_ONLY, 0,
channel_chain.size());
        buf_key = channel_key.map(FileChannel.MapMode.READ_ONLY, 0,
channel_key.size());

        // The files have been mapped, so clean up.
        channel_certificate.close();
        channel_chain.close();
        channel_key.close();
        file_certificate.close();
        file_chain.close();
        file_key.close();
     }
     catch (IOException ex)
     {
        throw ex;
     }

     // Create a request object and set the parameters.
     ImportCertificateRequest req = new ImportCertificateRequest();
     req.setCertificate(buf_certificate);
     req.setCertificateChain(buf_chain);
     req.setPrivateKey(buf_key);

     // Import the certificate.
     ImportCertificateResult result = null;
     try {
        result = client.importCertificate(req);
     }
     catch(LimitExceededException ex)
     {
        throw ex;
     }
     catch (ResourceNotFoundException ex)
     {
        throw ex;
     }

     // Clear the buffers.
     buf_certificate.clear();
     buf_chain.clear();
     buf_key.clear();
```

```
      // Retrieve and display the certificate ARN.
      String arn = result.getCertificateArn();
      System.out.println(arn);
    }
}
```

Creación de una lista de certificados

El siguiente ejemplo muestra cómo utilizar la función ListCertificates.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListCertificatesRequest;
import com.amazonaws.services.certificatemanager.model.ListCertificatesResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.AmazonClientException;

import java.util.Arrays;
import java.util.List;

/**
 * This sample demonstrates how to use the ListCertificates function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameters:
 *   CertificateStatuses - An array of strings that contains the statuses to use for
 filtering.
 *   MaxItems - The maximum number of certificates to return in the response.
 *   NextToken - Use when paginating results.
 *
 * Output parameters:
 *   CertificateSummaryList - A list of certificates.
 *   NextToken - Use to show additional results when paginating a truncated list.
 *
```

```
 */

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception{

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load the credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and set the parameters.
      ListCertificatesRequest req = new ListCertificatesRequest();
      List<String> Statuses = Arrays.asList("ISSUED", "EXPIRED", "PENDING_VALIDATION",
 "FAILED");
      req.setCertificateStatuses(Statuses);
      req.setMaxItems(10);

      // Retrieve the list of certificates.
      ListCertificatesResult result = null;
      try {
         result = client.listCertificates(req);
      }
      catch (Exception ex)
      {
         throw ex;
      }

      // Display the certificate list.
      System.out.println(result);
   }
```

```
}
```

La muestra de código anterior obtiene un resultado similar al siguiente.

```
{
    CertificateSummaryList: [{
        CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012,
        DomainName: www.example1.com
    },
    {
        CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012,
        DomainName: www.example2.com
    },
    {
        CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012,
        DomainName: www.example3.com
    }]
}
```

Renovación de un certificado

El siguiente ejemplo muestra cómo utilizar la función RenewCertificate. La función renueva un certificado privado emitido por una entidad de certificación (CA) privada y exportado con la función ExportCertificate. En este momento, solo los certificados exportados privados pueden renovarse con esta función. Para renovar sus certificados de Autoridad de certificación privada de AWS con ACM, primero debe conceder los permisos de principal de servicio de ACM para hacerlo. Para obtener más información, consulte Asignación de permisos de renovación de certificados a ACM.

```
package com.amazonaws.samples;

import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
```

```
import com.amazonaws.services.certificatemanager.AWSCertificateManager;

import com.amazonaws.services.certificatemanager.model.RenewCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RenewCertificateResult;


import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.ValidationException;

import java.io.FileNotFoundException;
import java.io.IOException;
import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

public class RenewCertificate {

   public static void main(String[] args) throws Exception {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.your_region)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();


      // Create a request object and specify the ARN of the certificate to renew.
      RenewCertificateRequest req = new RenewCertificateRequest();
      req.withCertificateArn("arn:aws:acm:region:account:"
            +"certificate/M12345678-1234-1234-1234-123456789012");
```

```
      // Renew the certificate.
      RenewCertificateResult result = null;
      try {
         result = client.renewCertificate(req);
      }
      catch(InvalidArnException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
      }
      catch (ValidationException ex)
      {
         throw ex;
      }

      // Display the result.
     System.out.println(result);
   }
}
```

Listado de etiquetas de certificados

El siguiente ejemplo muestra cómo utilizar la función ListTagsForCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.regions.Regions;
```

```
/**
 * This sample demonstrates how to use the ListTagsForCertificate function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameter:
 *   CertificateArn - The ARN of the certificate whose tags you want to list.
 *
*/

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception{

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and specify the ARN of the certificate.
      ListTagsForCertificateRequest req = new ListTagsForCertificateRequest();

 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");

      // Create a result object.
      ListTagsForCertificateResult result = null;
      try {
         result = client.listTagsForCertificate(req);
```

```
      }
      catch(InvalidArnException ex) {
         throw ex;
      }
      catch(ResourceNotFoundException ex) {
         throw ex;
      }

      // Display the result.
      System.out.println(result);

   }
}
```

La muestra de código anterior obtiene un resultado similar al siguiente.

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

Eliminación de etiquetas de un certificado

El siguiente ejemplo muestra cómo utilizar la función RemoveTagsFromCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import
 com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateResult;
import com.amazonaws.services.certificatemanager.model.Tag;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.InvalidTagException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import java.util.ArrayList;
```

```
/**
 * This sample demonstrates how to use the RemoveTagsFromCertificate function in the
 AWS Certificate
 * Manager service.
 *
 * Input parameters:
 *   CertificateArn - The ARN of the certificate from which you want to remove one or
 more tags.
 *   Tags - A collection of key-value pairs that specify which tags to remove.
 *
*/

public class AWSCertificateManagerExample {

   public static void main(String[] args) throws Exception {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Specify the tags to remove.
      Tag tag1 = new Tag();
      tag1.setKey("Short_Name");
      tag1.setValue("My_Cert");

      Tag tag2 = new Tag()
            .withKey("Purpose")
            .withValue("Test");
```

```
      // Add the tags to a collection.
      ArrayList<Tag> tags = new ArrayList<Tag>();
      tags.add(tag1);
      tags.add(tag2);

      // Create a request object.
      RemoveTagsFromCertificateRequest req = new RemoveTagsFromCertificateRequest();

 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");
      req.setTags(tags);

      // Create a result object.
      RemoveTagsFromCertificateResult result = null;
      try {
         result = client.removeTagsFromCertificate(req);
      }
      catch(InvalidArnException ex)
      {
         throw ex;
      }
      catch(InvalidTagException ex)
      {
         throw ex;
      }
      catch(ResourceNotFoundException ex)
      {
         throw ex;
      }

      // Display the result.
      System.out.println(result);
   }
}
```

Solicitud de un certificado

El siguiente ejemplo muestra cómo utilizar la función RequestCertificate.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.services.certificatemanager.model.RequestCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RequestCertificateResult;

import
 com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import java.util.ArrayList;

/**
 * This sample demonstrates how to use the RequestCertificate function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameters:
 *   DomainName - FQDN of your site.
 *   DomainValidationOptions - Domain name for email validation.
 *   IdempotencyToken - Distinguishes between calls to RequestCertificate.
 *   SubjectAlternativeNames - Additional FQDNs for the subject alternative names
 extension.
 *
 * Output parameter:
 *   Certificate ARN - The Amazon Resource Name (ARN) of the certificate you requested.
 *
*/

public class AWSCertificateManagerExample {

   public static void main(String[] args) {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
```

```
            throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
                .withRegion(Regions.US_EAST_1)
                .withCredentials(new AWSStaticCredentialsProvider(credentials))
                .build();

        // Specify a SAN.
        ArrayList<String> san = new ArrayList<String>();
        san.add("www.example.com");

        // Create a request object and set the input parameters.
        RequestCertificateRequest req = new RequestCertificateRequest();
        req.setDomainName("example.com");
        req.setIdempotencyToken("1Aq25pTy");
        req.setSubjectAlternativeNames(san);

        // Create a result object and display the certificate ARN.
        RequestCertificateResult result = null;
        try {
           result = client.requestCertificate(req);
        }
        catch(InvalidDomainValidationOptionsException ex)
        {
           throw ex;
        }
        catch(LimitExceededException ex)
        {
           throw ex;
        }

        // Display the ARN.
        System.out.println(result);

    }

}
```

La muestra de código anterior obtiene un resultado similar al siguiente.

```
{CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

Reenviar correo electrónico de validación

El siguiente ejemplo muestra cómo utilizar la función ResendValidationEmail.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailRequest;
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailResult;

import
 com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.InvalidStateException;
import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

/**
 * This sample demonstrates how to use the ResendValidationEmail function in the AWS
 Certificate
 * Manager service.
 *
 * Input parameters:
 *   CertificateArn - Amazon Resource Name (ARN) of the certificate request.
 *   Domain - FQDN in the certificate request.
 *   ValidationDomain - The base validation domain that is used to send email.
 *
*/

public class AWSCertificateManagerExample {

   public static void main(String[] args) {
```

```
      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

      // Create a client.
      AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
              .withRegion(Regions.US_EAST_1)
              .withCredentials(new AWSStaticCredentialsProvider(credentials))
              .build();

      // Create a request object and set the input parameters.
      ResendValidationEmailRequest req = new ResendValidationEmailRequest();

 req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");
      req.setDomain("gregpe.io");
      req.setValidationDomain("gregpe.io");

      // Create a result object.
      ResendValidationEmailResult result = null;
      try {
         result = client.resendValidationEmail(req);
      }
      catch(ResourceNotFoundException ex)
      {
         throw ex;
      }
      catch (InvalidStateException ex)
      {
         throw ex;
      }
      catch (InvalidArnException ex)
      {
         throw ex;
      }
      catch (InvalidDomainValidationOptionsException ex)
```

```
      {
         throw ex;
      }

      // Display the result.
      System.out.println(result.toString());

   }
}
```

En la muestra de código anterior se vuelve a enviar su correo electrónico de validación y se muestra un conjunto vacío.

Solución de problemas

Consulte los siguientes temas si tienes problemas al utilizar AWS Certificate Manager.

> **Note**
>
> Si el problema no se trata en esta sección, recomendamos que visite el Centro de conocimientos de AWS.

Temas

Solución de problemas de solicitudes de certificados

Consulte los siguientes temas si tiene problemas al solicitar un certificado de ACM.

Temas

Se ha agotado el tiempo de espera de la solicitud de certificado

Las solicitudes de certificados de ACM vencen si no se validan en un plazo de 72 horas. Para corregir esta condición, abra la consola, busque el registro del certificado, haga clic en la casilla de verificación correspondiente, elija Actions (Acciones) y luego, Delete (Eliminar). A continuación, elija Actions (Acciones) y Request a certificate (Solicitar un certificado) para volver a comenzar. Para obtener más información, consulte Validación por DNS o Validación por correo electrónico. Le recomendamos que utilice la validación de DNS si es posible.

Error en la solicitud de certificado

Si la solicitud produce un error en ACM y recibe uno de los siguientes mensajes de error, siga los pasos sugeridos para solucionar el problema. No puede volver a enviar una solicitud de certificado que produce un error; después de resolver el problema, envíe una nueva solicitud.

Temas

Mensaje de error: No hay contactos disponibles

Ha elegido la validación por correo electrónico al solicitar un certificado, pero ACM no ha podido encontrar una dirección de correo electrónico para validar uno o varios de los nombres de dominio incluidos en la solicitud. Para solucionar este problema, puede elegir una de las siguientes opciones:

- Asegúrese de disponer de una dirección de correo electrónico registrada en WHOIS y que esté visible al realizar una búsqueda WHOIS estándar de nombres de dominio en la solicitud de certificado. Por lo general, esto se hace a través de su registrador de dominio.
- Asegúrese de que su dominio esté configurado para recibir correos electrónicos. El servidor de nombres de dominio debe tener un registro de intercambio de correo electrónico (MX) para que los servidores de correo electrónico de ACM sepan a dónde deben enviar el correo electrónico de validación de dominio.

Realizar una de las tareas anteriores es suficiente para solucionar este problema; no es necesario realizar ambas. Después de solucionar el problema, solicite un certificado nuevo.

Para obtener más información sobre cómo asegurarse de recibir correos electrónicos de validación de dominio de ACM, consulte (Opcional) Configuración del correo electrónico para el dominio o No he recibido el correo electrónico de validación. Si sigue estos pasos y sigue apareciendo el mensaje No Available Contacts (Contactos no disponibles), informe de ello a AWS para que podamos investigar el problema.

Mensaje de error: Se requiere verificación adicional

ACM requiere información adicional para procesar esta solicitud de certificado. Esto ocurre como medida de protección contra el fraude si su dominio se encuentra entre los 1000 mejores sitios web de Alexa. Para proporcionar la información requerida, utilice el Centro de asistencia para contactar con AWS Support. Si no tiene un plan de asistencia técnica, publique un mensaje en el Foro de debate de ACM.

> **Note**
>
> No se puede solicitar un certificado para nombres de dominio propiedad de Amazon como los que terminan en amazonaws.com, cloudfront.net o elasticbeanstalk.com.

Mensaje de error: Dominio público no válido

Uno o varios de los nombres de dominio de la solicitud de certificado no son válidos. Por lo general, esto se debe a que alguno de los nombres de dominio de la solicitud no es un dominio de nivel superior válido. Intente volver a solicitar un certificado, corregir errores de ortografía o tipográficos en la solicitud y asegurarse de que todos los nombres de dominio de la solicitud son dominios de nivel superior válidos. Por ejemplo, no se puede solicitar un certificado de ACM para example.invalidpublicdomain porque “invalidpublicdomain” no es un dominio de primer nivel válido. Si sigue apareciendo este motivo de error, póngase en contacto con el Centro de soporte. Si no tiene un plan de asistencia técnica, publique un mensaje en el Foro de debate de ACM.

Mensaje de error: Otro

Normalmente, este error se debe a una falta ortográfica en uno o varios nombres de dominio de la solicitud de certificado. Intente volver a solicitar el certificado después de corregir cualquier error ortográfico o tipográfico que hubiese en la solicitud. Si continúa recibiendo este mensaje de error, utilice el Centro de soporte técnico para ponerse en contacto con AWS Support. Si no tiene un plan de asistencia técnica, publique un mensaje en el Foro de debate de ACM.

Solución de problemas de validación de certificados

Si el estado de la solicitud del certificado de ACM es Validación pendiente, la solicitud está esperando una acción de su parte. Si eligió la validación por correo electrónico cuando realizó la solicitud, usted o su representante autorizado debe responder a los mensajes de correo electrónico

de validación. Estos mensajes se enviaron a las direcciones de contacto de WHOIS registradas y a otras direcciones de correo electrónico comunes para el dominio solicitado. Para obtener más información, consulte Validación por correo electrónico. Si eligió la validación por DNS, debe escribir el registro CNAME que ACM creó para usted en su base de datos de DNS. Para obtener más información, consulte Validación por DNS.

> **Important**
>
> Debe validar que usted es el propietario o controla cada nombre de dominio incluido en la solicitud de certificado. Si eligió la validación por correo electrónico, recibirá mensajes de correo electrónico de validación para cada dominio. En caso contrario, consulte No he recibido el correo electrónico de validación. Si eligió la validación por DNS, debe crear un registro CNAME para cada dominio.

> **Note**
>
> Los certificados de ACM públicos se pueden instalar en instancias de Amazon EC2 conectadas a un Nitro Enclave, pero no a otras instancias de Amazon EC2. Para obtener información sobre la configuración de un servidor web independiente en una instancia de Amazon EC2 no conectada a un Nitro Enclave, consulte Tutorial: Install a LAMP web server on Amazon Linux 2 o Tutorial: Install a LAMP web server with the Amazon Linux AMI.

Le recomendamos que utilice la validación por DNS en lugar de la validación por correo electrónico.

Consulte los siguientes temas si tiene problemas de validación.

Temas

- Solución de problemas en la validación por DNS
- Solución de problemas de validación por correo electrónico

Solución de problemas en la validación por DNS

Consulte la siguiente guía si tiene algún problema para validar un certificado con DNS.

El primer paso en la solución de problemas DNS es comprobar el estado actual de su dominio con herramientas como las siguientes:

- dig—Linux,Windows
- nslookup—Linux,Windows
- WHOIS—Linux,Windows

Temas

Caracteres de subrayado prohibidos por el proveedor de DNS

Si el proveedor de DNS prohíbe los caracteres de subrayado iniciales en los valores de CNAME, puede eliminar el carácter de subrayado del valor proporcionado por ACM y validar el dominio sin él. Por ejemplo, el valor de CNAME `_x2.acm-validations.aws` se puede cambiar por `x2.acm-validations.aws` para la validación. Sin embargo, el parámetro del nombre de CNAME siempre debe comenzar por un carácter de subrayado inicial.

Puede utilizar cualquiera de los valores de la parte derecha de la tabla que se muestra a continuación para validar un dominio.

Nombre	Tipo	Valor
`_<random value>.example.com.`	CNAME	`_<random value>.acm-validations.aws.`
`_<random value>.example.com.`	CNAME	`<random value>.acm-validations.aws.`

Periodo de seguimiento predeterminado agregado por el proveedor DNS

Algunos proveedores DNS agregan de forma predeterminada un periodo de seguimiento al valor CNAME proporcionado. Como resultado, se genera un error si agrega el periodo usted mismo. Por ejemplo, "`<random_value>.acm-validations.aws.`" se rechaza mientras "`<random_value>.acm-validations.aws`" se acepta.

La validación de DNS GoDaddy no falla

Se puede producir un error en la validación por DNS para dominios registrados con Godaddy y otros registros a menos que se modifiquen los valores CNAME proporcionados por ACM. Si se toma example.com como nombre de dominio, el registro CNAME emitido tiene el siguiente formato:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

Puedes crear un registro CNAME compatible con él GoDaddy truncando el dominio principal (incluido el punto) al final del campo NAME, de la siguiente manera:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

La consola de ACM no muestra el botón "Crear registro en Route 53"

Si selecciona Amazon Route 53 como su proveedor de DNS, AWS Certificate Manager podrá interactuar directamente con él para validar la propiedad de su dominio. En algunas circunstancias, es posible que el botón Crear registros en Route 53 de la consola no esté disponible. Si esto ocurre, compruebe las siguientes causas posibles.

- No utiliza Route 53 como proveedor de DNS.
- Ha iniciado sesión en ACM y Route 53 con cuentas diferentes.
- Carece de permisos de IAM necesarios para crear registros en una zona alojada por Route 53.
- Usted u otra persona ya ha validado el dominio.
- El dominio no es direccionable públicamente.

La validación de Route 53 falla en dominios privados (poco fiables)

Durante la validación DNS, ACM busca un CNAME en una zona alojada públicamente. Cuando no encuentra uno, se agota el tiempo de espera tras 72 horas con el estado de Validation timed out (Tiempo de espera de validación agotado). No se puede utilizar para alojar registros DNS en dominios privados, incluidos recursos en una zona alojada privada de Amazon VPC, dominios poco fiables en su PKI privada y certificados autofirmados.

AWS proporciona soporte para dominios que no son de confianza pública a través del Autoridad de certificación privada de AWSservicio.

La validación se realiza correctamente, pero la emisión o la renovación fallan

Si la emisión del certificado falla y aparece la opción “Validación pendiente” aunque el DNS sea correcto, compruebe que un registro de autorización de la autoridad certificadora (CAA) no esté bloqueando la emisión. Para obtener más información, consulte (Opcional) Configuración de un registro de CAA.

Error de validación para el servidor DNS en una VPN

Si se localiza un servidor DNS en una VPN y ACM no consigue validar un certificado, compruebe que el servidor tenga acceso público. La emisión de certificados públicos mediante la validación por DNS de ACM requiere que los registros de dominio se puedan resolver a través de la Internet pública.

Solución de problemas de validación por correo electrónico

Consulte la siguiente guía si tiene algún problema para validar un dominio de certificado por correo electrónico.

Temas

- No he recibido el correo electrónico de validación
- Correo electrónico enviado al subdominio
- Información de contacto oculta
- Renovaciones de certificados
- Limitación controlada de WHOIS
- Marca de tiempo inicial persistente para la validación por correo electrónico
- Solución de problemas con el dominio de primer nivel .IO
- No puedo cambiar a la validación por DNS

No he recibido el correo electrónico de validación

Cuando solicite un certificado a ACM y elija la validación por correo electrónico, el correo electrónico de validación del dominio se enviará a tres direcciones de contacto especificadas en WHOIS y a cinco direcciones administrativas comunes. Para obtener más información, consulte Validación por correo electrónico. Si tiene problemas para recibir el correo electrónico de validación, revise las sugerencias que aparecen a continuación.

Dónde buscar el correo electrónico

: El correo electrónico de validación se envía a las direcciones de contacto enumeradas en WHOIS y a las direcciones administrativas comunes del dominio. El correo electrónico no se envía al propietario de la AWS cuenta a menos que el propietario también figure como contacto de dominio en WHOIS. Revise la lista de direcciones de correo electrónico que se muestran en la consola de ACM (o que la CLI o la API han devuelto) para determinar dónde debe buscar el correo electrónico de validación. Para consultar la lista, haga clic en el icono junto al nombre de dominio del cuadro Validation not complete.

El correo electrónico está marcado como spam

: Compruebe si el correo de validación se encuentra en la carpeta de spam.

GMail clasifica automáticamente su correo electrónico

: Si utiliza GMail, el correo electrónico de validación puede haberse clasificado automáticamente en las pestañas Updates o Promotions.

El registrador del dominio no muestra la información de contacto o la protección de la privacidad está habilitada.

: En algunos casos, es posible que los contactos técnicos y administrativos del registrante del dominio en WHOIS no estén disponibles públicamente y, AWS por lo tanto, no puedan comunicarse con estos contactos. A su discreción, puede optar por configurar su registrador para publicar su dirección de correo electrónico en WHOIS, aunque no todos los registradores admiten esta opción. Puede que necesite realizar un cambio directamente en el registro de su dominio. En otros casos, la información de contacto del dominio puede estar utilizando una dirección de privacidad, como las que se proporcionan a través WhoisGuard de o. PrivacyGuard

  En el caso de los dominios adquiridos desde Route 53, la protección de privacidad está habilitada de manera predeterminada y la dirección de correo electrónico se asigna a una dirección de correo electrónico de `whoisprivacyservice.org`, `contact.gandi.net` o `identity-protect.org`. Asegúrese de que su dirección de correo electrónico de registrador en el archivo

con su registrador de dominio esté actualizado de forma que el correo electrónico enviado a estas direcciones de correo electrónico oscurecidas puedan reenviarse a una dirección de correo electrónico que usted controle.

> **Note**
>
> La protección de privacidad para algunos dominios que se adquieran con Route 53 se habilitará incluso si decide hacer pública su información de contacto. Por ejemplo, no se puede deshabilitar mediante programación por Route 53 la protección de privacidad para el dominio de primer nivel. Debe ponerse en contacto con el Centro de AWS Support para solicitar que se deshabilite la protección de privacidad.

Si una cuenta de correo electrónico de contacto para su dominio no está disponible a través de correo electrónico WHOIS, o si se envían a la información de contacto no alcanza el propietario del dominio o su representante autorizado, le recomendamos que configure su dominio o subdominio para recibir el correo electrónico enviado a una o más de las direcciones administrativas formadas tras añadir admin @, administrator @, hostmaster @, webmaster@y postmaster@para el nombre de dominio solicitado. Para obtener más información sobre la configuración del correo electrónico para su dominio, consulte la documentación de su proveedor de servicios de correo electrónico y siga las instrucciones de (Opcional) Configuración del correo electrónico para el dominio. Si utilizas Amazon WorkMail, consulta Cómo trabajar con usuarios en la Guía del WorkMail administrador de Amazon.

Después de poner a disposición al menos una de las ocho direcciones de correo electrónico a las que AWS envía el correo electrónico de validación y de confirmar que puede recibir correos electrónicos en esa dirección, está listo para solicitar un certificado a través de ACM. Después de realizar una solicitud de certificado, asegúrese de que la dirección de correo electrónico pretendida aparece en la lista de direcciones de correo electrónico de la AWS Management Console. A pesar de que el certificado está en estado Pending validation, puede ampliar la lista para verlo haciendo clic en el icono junto al nombre de dominio del cuadro Validation not complete. También puede ver la lista en Step 3: Validate (Paso 3: Validar) del asistente Request a Certificate (Solicitar un certificado) de ACM. Las direcciones de correo electrónico listadas son aquellas a las que se ha enviado el correo electrónico.

Faltan registros MX o no están configurados de forma correcta

Un registro MX es un registro de recursos de la base de datos del sistema de nombres de dominio (DNS) que especifica uno o varios servidores de correo que aceptan mensajes para un

dominio. Si el registro MX no existe o no está configurado correctamente, no se puede enviar correo electrónico a ninguna de las cinco direcciones comunes de administración del sistema especificadas en Validación por correo electrónico. Corrija el registro MX que falta o que está mal configurado y vuelva a enviar el correo electrónico o a solicitar el certificado.

> **Note**
>
> En la actualidad, le recomendamos que espere al menos una hora antes de intentar volver a enviar el correo electrónico o solicitar el certificado.

> **Note**
>
> Para evitar la necesidad de un registro MX, puedes usar la `ValidationDomain` opción de la RequestCertificateAPI o el AWS CLI comando request-certificate para especificar el nombre de dominio al que ACM envía los correos electrónicos de validación. Si utiliza la API o la AWS CLI, AWS no realiza ninguna búsqueda de MX.

Póngase en contacto con el Centro de soporte

Si, después de revisar las instrucciones anteriores, sigue sin recibir el correo electrónico de validación del dominio, visite el Centro de AWS Support y cree una incidencia. Si no dispone de un acuerdo de soporte, publique un mensaje en el foro de debate de ACM.

Correo electrónico enviado al subdominio

Si utiliza la consola y solicita un certificado para un nombre de subdominio como `sub.test.example.com`, ACM verifica si existe un registro MX para `sub.test.example.com`. De lo contrario, el dominio principal `test.example.com` está seleccionado, y así sucesivamente, hasta el dominio de la base `example.com`. Si se encuentra un registro MX, la búsqueda se detiene y se envía un correo electrónico de validación a las direcciones comunes de administración del subdominio. Por lo tanto, si un registro MX se encuentra para `test.example.com`, el correo electrónico se envía a admin@test.example.com, administrator@test.example.com y a las demás direcciones administrativas especificadas en Validación por correo electrónico. Si un registro MX no se encuentra en ninguno de los subdominios, se envía un correo electrónico al subdominio para el que solicitó el certificado inicialmente. Si desea saber cómo configurar su correo electrónico y cómo

ACM funciona con DNS y la base de datos de WHOIS, consulte (Opcional) Configuración del correo electrónico para el dominio.

En lugar de usar la consola, puede usar la `ValidationDomain` opción de la RequestCertificateAPI o el AWS CLI comando request-certificate para especificar el nombre de dominio al que ACM envía los correos electrónicos de validación. Si utiliza la API o la AWS CLI, AWS no realiza ninguna búsqueda en MX.

Información de contacto oculta

Hay un problema habitual cuando trata de crear un nuevo certificado. Algunos registradores le permiten ocultar su información de contacto en su listado de WHOIS. Otros le permiten sustituir su dirección de correo electrónico real con una dirección de privacidad (o proxy). Esto le impide recibir el correo electrónico de validación en sus direcciones registradas de contacto.

Para recibir correo, asegúrese de que su información de contacto sea pública en WHOIS o, si su listado de WHOIS muestra una dirección de correo electrónico de privacidad, asegúrese de que el correo electrónico enviado a la dirección de privacidad se reenvía a su dirección de correo electrónico real. Una vez completada la configuración de WHOIS, y siempre que la solicitud de certificado no haya agotado el tiempo de espera, puede elegir reenviar el correo electrónico de validación. ACM realiza una nueva búsqueda en WHOIS/MX y envía un correo electrónico de validación a su dirección de contacto que ahora es pública.

Renovaciones de certificados

Si hizo que su información de WHOIS fuera pública cuando solicitó un certificado nuevo pero luego la ocultó, ACM no podrá recuperar sus direcciones de contacto registradas cuando intente renovar su certificado. ACM envía un correo electrónico de validación a estas direcciones de contacto y a cinco direcciones administrativas formadas mediante su registro MX. Para solucionar este problema, vuelva a hacer pública su información de WHOIS y reenvíe los correos electrónicos de validación. ACM realiza una nueva búsqueda en WHOIS/MX y envía un correo electrónico de validación a sus direcciones de contacto que ahora son públicas.

Limitación controlada de WHOIS

A veces, ACM no puede ponerse en contacto con el servidor de WHOIS incluso después de haber enviado varias solicitudes de correo electrónico de validación. Este problema es externo a AWS. Es decir, AWS no controla los servidores de WHOIS y no puede prevenir la limitación controlada del servidor de WHOIS. Si experimenta este problema, cree un caso en el Centro de AWS Support para que lo ayuden a encontrar la solución.

Marca de tiempo inicial persistente para la validación por correo electrónico

La marca de tiempo de la primera solicitud de validación por correo electrónico de un certificado se conserva en las posteriores solicitudes de renovación de validación. Esto no es una prueba de un error en las operaciones de ACM.

Solución de problemas con el dominio de primer nivel .IO

El dominio .IO está asignado al Territorio Británico del Océano Índico. En la actualidad, el registro de dominio no muestra información pública de la base de datos WHOIS, independientemente de si la protección de privacidad del dominio está activada o no. Los registradores pueden mostrar esta información en sus propios resultados de WHOIS si la protección de la privacidad está desactivada, pero esta práctica varía de un registrador a otro. ACM no puede enviar un correo electrónico de validación a las siguientes tres direcciones de contacto registradas si no están disponibles en WHOIS a través del registrador.

- Titularidad del dominio
- Contacto técnico
- Contacto administrativo

Sin embargo, ACM envía correos electrónicos de validación a las siguientes cinco direcciones comunes del sistema donde *`your_domain`* es el nombre de dominio que introdujo cuando se le solicitó el certificado inicialmente y `.io` es el dominio de nivel superior.

- administrator@*`su_dominio`*.io
- hostmaster@*`su_dominio`*.io
- postmaster@*`su_dominio`*.io
- webmaster@*`su_dominio`*.io
- admin@*`su_dominio`*.io

Asegúrese de que al menos una de esas cinco cuentas de correo electrónico esté habilitada para poder recibir un correo electrónico de validación de un dominio .IO. Si no lo está, no recibirá un correo electrónico de validación y no se podrá emitir su certificado de ACM.

> **Note**
>
> Le recomendamos que utilice la validación por DNS en lugar de la validación por correo electrónico. Para obtener más información, consulte Validación por DNS.

No puedo cambiar a la validación por DNS

Después de crear un certificado con validación por correo electrónico, no puede cambiar a la validación mediante DNS.

Solución de problemas de renovación administrada de certificados

ACM intenta renovar de forma automática sus certificados de ACM antes de que venzan para que no se requiera ninguna acción de su parte. Consulte los siguientes temas si surgen problemas con la Renovación administrada para certificados de ACM.

Preparación para la validación automática de dominios

Para que ACM pueda renovar sus certificados de forma automática, lo siguiente debe ser VERDADERO:

- El certificado debe estar asociado a un AWS servicio que esté integrado con ACM. Para obtener información sobre los recursos que admite ACM, consulte Servicios integrados con AWS Certificate Manager.
- En el caso de los certificados validados por correo electrónico, ACM debe poder comunicarse con usted en una dirección de correo electrónico de administrador para cada dominio que figura en el certificado. Las direcciones de correo electrónico que se probarán son las que aparecen en Validación por correo electrónico.
- Para los certificados validados por DNS, asegúrese de que la configuración de DNS contiene los registros CNAME correctos, tal como se describe en Validación por DNS.

Administración de errores en la renovación administrada de certificados

Al acercarse la fecha de caducidad del certificado (60 días para DNS, 45 para EMAIL y 60 días para Private), ACM intenta renovarlo si cumple con los criterios de elegibilidad. Es posible que tenga que

tomar medidas para que la renovación se realice correctamente. Para obtener más información, consulte Renovación administrada para certificados de ACM.

Renovación administrada de certificados validados por correo electrónico

Los certificados de ACM son válidos durante 13 meses (395 días). Para renovar los certificados validados por correo electrónico, el propietario del dominio debe realizar una acción. ACM comienza a enviar avisos de renovación 45 días antes del vencimiento y utiliza las direcciones de buzón WHOIS del dominio y cinco direcciones comunes de administrador. Las notificaciones contienen un enlace que el propietario del dominio puede presionar para facilitar la renovación. Una vez validados todos los dominios enumerados, ACM emite un certificado renovado con el mismo ARN.

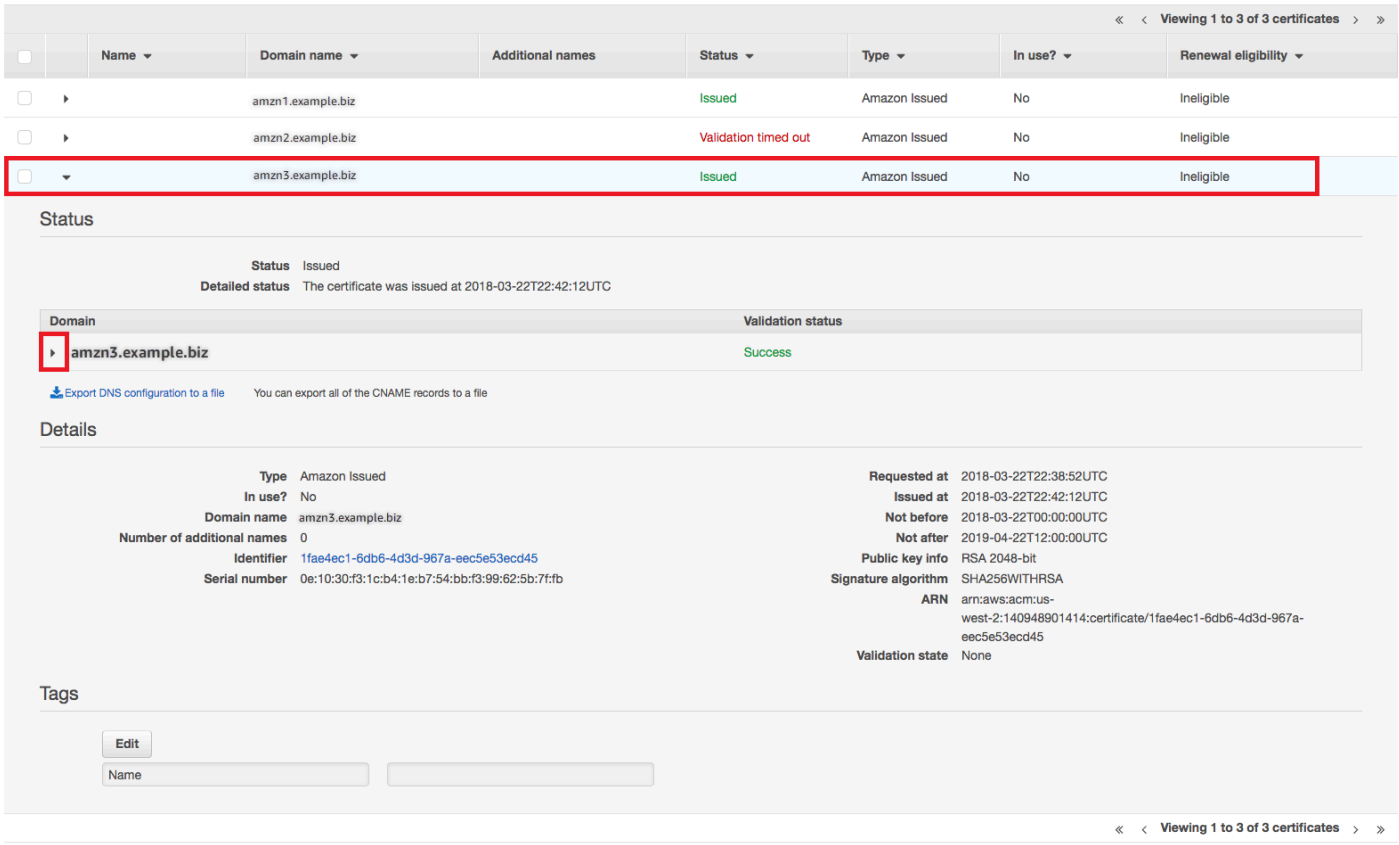
Consulte el artículo sobre la validación con el correo electrónico para obtener instrucciones sobre cómo identificar los dominios que tienen el estado `PENDING_VALIDATION` y repetir el proceso de validación en dichos dominios.

Renovación administrada de certificados validados mediante DNS

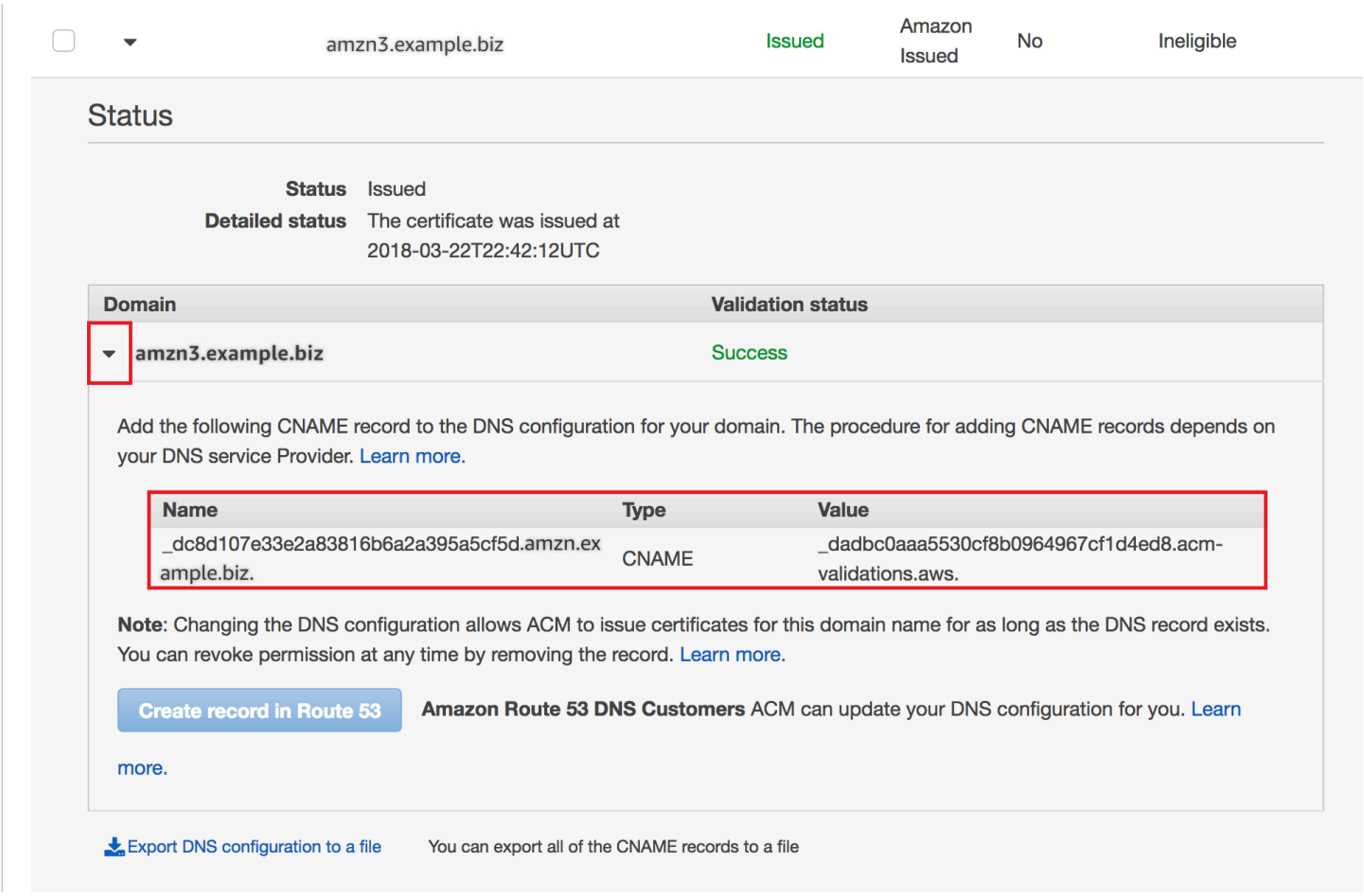
ACM no intenta la validación de TLS en certificados validados por DNS. Si ACM no puede renovar un certificado que se validó mediante DNS, lo más probable es que falten registros CNAME en la configuración de DNS o que estos no sean correctos. Si esto ocurre, ACM avisa que el certificado no se pudo renovar de forma automática.

> **Important**
>
> Debe insertar los registros CNAME correctos en la base de datos de DNS. Consulte a su registrador de dominios sobre cómo hacerlo.

Para encontrar los registros CNAME de los dominios, expanda el certificado y sus entradas de dominio en la consola de ACM. Consulte las ilustraciones siguientes para obtener más información. También puede recuperar registros CNAME mediante la DescribeCertificateoperación de la API de ACM o el comando describe-certificate de la CLI de ACM. Para obtener más información, consulte Validación por DNS.



Seleccione el certificado de destino en la consola.



Expanda la ventana del certificado para buscar información sobre el CNAME del certificado.

Si el problema persiste, póngase en contacto con el centro de Support.

Cronología de la renovación

Renovación administrada para certificados de ACM es un proceso asíncrono. Esto significa que los pasos no suceden uno inmediatamente después del otro. Después de que todos los nombres de dominio de un certificado de ACM se hayan validado, puede haber un retraso antes de que ACM obtenga el nuevo certificado. Puede producirse un retraso adicional entre el momento en que ACM obtiene el certificado renovado y el momento en el que dicho certificado se implementa en los recursos de AWS que lo utilizan. Por lo tanto, es posible que pasen varias horas hasta que los cambios de estado del certificado aparezcan en la consola.

Solución de otros problemas

En esta sección se incluyen instrucciones sobre problemas no relacionados con la emisión o validación de certificados de ACM.

Temas

Solución de problemas con la autorización de la entidad de certificación (CAA)

Puede utilizar registros de DNS de CAA para especificar que la entidad de certificación (CA) de Amazon puede emitir certificados de ACM para su dominio o subdominio. Si recibe un error One or more domain names have failed validation due to a Certification Authority Authentication (CAA) error durante la emisión de certificados, verifique los registros de DNS de CAA. Si recibe este error después de que haya validado correctamente su solicitud de un certificado de ACM, debe actualizar los registros de CAA y volver solicitar un certificado. El campo value (valor) del registro de CAA debe contener uno de los siguientes nombres de dominio:

- amazon.com
- amazontrust.com
- awstrust.com
- amazonaws.com

Para obtener más información sobre cómo crear un registro de CAA, consulte (Opcional) Configuración de un registro de CAA.

> **Note**
>
> Puede elegir no configurar ningún registro de CAA para su dominio si no desea habilitar la comprobación de CAA.

Problemas de importación de certificados

Puede importar certificados de terceros al ACM y asociarlos a los servicios integrados. Si tiene problemas, examine los temas de requisitos previos y formato de los certificados. En concreto, tenga en cuenta lo siguiente:

- Únicamente puede importar certificados SSL/TLS X.509 versión 3.
- El certificado puede ser autofirmado o puede estar firmado por una entidad de certificación (CA).
- Si el certificado está firmado por una CA, debe incluir una cadena de certificados intermedia que proporcione una ruta a la raíz de la entidad de certificación.
- Si el certificado está autofirmado, debe incluir la clave privada en texto sin formato.
- Cada certificado de la cadena debe certificar directamente al que le precede.
- No incluya su certificado de entidad final en la cadena de certificados intermedia.
- El certificado, la cadena de certificados y la clave privada (si la hay) deben estar codificados en PEM. En general, la codificación PEM consiste en bloques de texto ASCII codificado en Base64 que comienzan y terminan con líneas de encabezado y pie de página de texto sin formato. No se deben agregar líneas o espacios ni realizar ningún otro cambio en un archivo PEM al copiarlo o cargarlo. Puede verificar las cadenas de certificados mediante la Utilidad de verificación de OpenSSL.
- La clave privada (si la hubiera) no debe estar cifrada. (Consejo: si tiene una frase de contraseña, está cifrada).
- Los servicios integrados con ACM deben utilizar algoritmos y tamaños de clave admitidos por ACM. Consulte la guía del AWS Certificate Manager usuario y la documentación de cada servicio para asegurarse de que su certificado funcione.
- La compatibilidad con los certificados de los servicios integrados puede variar en función de si el certificado se importa a IAM o ACM.
- El certificado debe ser válido cuando se importa.
- En la consola se muestra información detallada para todos los certificados. Sin embargo, de forma predeterminada, si llamas a la ListCertificatesAPI o al AWS CLI comando list-certificates

sin especificar el `keyTypes` filtro, solo se muestran `RSA_2048` los certificados `RSA_1024` o certificados.

Problemas de asignación de certificados

Para renovar un certificado, ACM genera un nuevo par de claves pública y privada. Si tu aplicación utiliza un certificado ACMAsignación de certificados, lo que también se conoce como anclaje SSL, es posible que la aplicación no pueda conectarse a tu dominio después AWS de renovar el certificado. Por este motivo, recomendamos que no asigne un certificado de ACM. Si su aplicación debe asignar un certificado, puede hacer lo siguiente:

- Importe su propio certificado a ACM y, a continuación, asigne la aplicación al certificado importado. ACM no proporciona una renovación administrada de los certificados importados.
- Si utiliza un certificado público, fije su aplicación a todos los certificados raíz de Amazon disponibles. Si utiliza un certificado privado, fije su aplicación al certificado raíz de la CA.

Problemas con API Gateway

Al implementar un punto final de API optimizado para la periferia, API Gateway configura una CloudFront distribución para usted. La CloudFront distribución es propiedad de API Gateway, no de tu cuenta. Además, la distribución está vinculada al certificado de ACM utilizado al implementar la API. Para eliminar dicho vínculo y permitir que ACM elimine el certificado, deberá eliminar el dominio personalizado de API Gateway asociado al certificado.

Al implementar un punto de enlace de la API regional, API Gateway crea un Application Load Balancer (ALB) en su nombre. El balanceador de carga es propiedad de API Gateway y no está visible. El ALB está vinculado al certificado de ACM utilizado al implementar la API. Para eliminar dicho vínculo y permitir que ACM elimine el certificado, deberá eliminar el dominio personalizado de API Gateway asociado al certificado.

Qué hacer cuando un certificado falla de forma inesperada

Si ha asociado de forma correcta un certificado de ACM a un servicio integrado, pero el certificado deja de funcionar y el servicio integrado comienza a devolver errores, la causa puede ser un cambio en los permisos que el servicio necesita para utilizar un certificado de ACM.

Por ejemplo, Elastic Load Balancing (ELB) requiere permiso para descifrar y, a su vez, descifra la clave privada del certificado. AWS KMS key Este permiso se concede mediante una política basada

en recursos que ACM aplica cuando se asocia un certificado con ELB. Si ELB pierde la concesión de ese permiso, fallará la próxima vez que intente descifrar la clave del certificado.

Para investigar el problema, compruebe el estado de sus subvenciones en la AWS KMS consola de. https://console.aws.amazon.com/kms A continuación, realice una de las siguientes acciones:

- Si cree que los permisos concedidos a un servicio integrado han sido revocados, visite la consola del servicio integrado, desasocie el certificado del servicio y vuelva a asociarlo. De este modo, se volverá a aplicar la política basada en recursos y se pondrá en marcha una nueva concesión de permiso.
- Si cree que se han revocado los permisos concedidos a ACM, póngase AWS Support en contacto con nosotros en https://console.aws.amazon.com/support/home#/.

Problemas con el rol vinculado a servicios (SLR) de ACM

Al emitir un certificado firmado por una entidad de certificación privada que otra cuenta ha compartido con usted, ACM intenta configurar por primera vez un rol vinculado a un servicio (SLR) para interactuar como principal con una política de acceso basada en los recursos. Autoridad de certificación privada de AWS Si emite un certificado privado desde una CA compartida y no hay un SLR, ACM no podrá renovar de forma automática ese certificado por usted.

ACM podría avisarle que no puede determinar si existe un SLR en su cuenta. Si ya se ha concedido el permiso `iam:GetRole` necesario al SLR de ACM para su cuenta, el aviso no se repetirá después de crearse el SLR. Si se repite, es posible que usted o el administrador de su cuenta tengan que conceder el permiso `iam:GetRole` a ACM o asociar la cuenta a la política `AWSCertificateManagerFullAccess` administrada por ACM.

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Tratamiento de excepciones

Un AWS Certificate Manager comando puede fallar por varios motivos. Para obtener información sobre cada excepción, consulte la siguiente tabla.

Tratamiento de excepciones de certificados privados

Se pueden producir las siguientes excepciones al intentar renovar un certificado de PKI privado emitido por Autoridad de certificación privada de AWS.

> **Note**
>
> Autoridad de certificación privada de AWS no se admite en la región de China (Pekín) ni en la región de China (Ningxia).

Código de error de ACM	Comentario
`PCA_ACCESS_DENIED`	La CA privada no ha concedido permisos de ACM. Esto activa un código de Autoridad de certificación privada de AWS `AccessDeniedException` error. Para solucionar el problema, conceda los permisos necesarios al director del servicio de ACM mediante la Autoridad de certificación privada de AWS CreatePermissionoperación.
`PCA_INVALID_DURATION`	El periodo de validez del certificado solicitado supera el periodo de validez de la CA privada emisora. Esto desencadena un código de Autoridad de certificación privada de AWS `ValidationException` error. Para solucionar el problema, instale un nuevo certificado de entidad de certificación con un período de validez adecuado.
`PCA_INVALID_STATE`	La CA privada a la que se llama no tiene el estado correcto para realizar la operación de ACM solicitada. Esto activa un código de Autoridad de certificación privada de AWS `InvalidStateException` fallo. Resuelva el problema de la siguiente manera: • Si la CA tiene el estado `CREATING`, espere a que finalice la creación y, a continuación,

Código de error de ACM	Comentario
	instale el certificado de entidad de certificación. • Si la CA tiene el estado `PENDING_CERTIFICATE`, instale el certificado de entidad de certificación. • Si la CA tiene el estado `DISABLED`, actualíce la al estado `ACTIVE`. • Si la CA tiene el estado `DELETED`, restáurela. • Si la CA tiene el estado `EXPIRED`, instale un nuevo certificado • Si la CA tiene el estado `FAILED` y no puede resolver el problema, póngase en contacto con AWS Support.
`PCA_LIMIT_EXCEEDED`	La CA privada ha alcanzado una cuota de emisión. Esto activa un código de Autoridad de certificación privada de AWS `LimitExceededException` fallo. Intente repetir su solicitud antes de continuar con esta ayuda. Si el error persiste, póngase en contacto con AWS Support para solicitar un aumento de cuota.
`PCA_REQUEST_FAILED`	Se ha producido un error de red o sistema. Esto activa un código de Autoridad de certificación privada de AWS `RequestFailedException` fallo. Intente repetir su solicitud antes de continuar con esta ayuda. Si el error persiste, póngase en contacto con AWS Support.

Código de error de ACM	Comentario
`PCA_RESOURCE_NOT_FOUND`	La CA privada se ha eliminado de forma permanente. Esto activa un código de Autoridad de certificación privada de AWS `ResourceNotFoundException` fallo. Compruebe que ha utilizado el ARN correcto. Si se vuelve a generar el error, no podrá usar esta CA. Para solucionar el problema, cree una nueva CA.
`SLR_NOT_FOUND`	Para renovar un certificado firmado por una CA privada que reside en otra cuenta, ACM requiere un rol vinculado al servicio (SLR) en la cuenta donde reside el certificado. Si necesita volver a crear un SLR eliminado, consulte Creación del SLR para ACM.

Conceptos

En esta sección se proporcionan las definiciones de los conceptos que utiliza AWS Certificate Manager.

Temas

Certificado del ACM

ACM genera certificados X.509 versión 3. Cada uno tiene una validez de 13 meses (395 días) y contiene las siguientes extensiones.

- Basic Constraints (Restricciones básicas): especifica si el sujeto del certificado es una entidad de certificación (CA)

- Authority Key Identifier (Identificador de la clave de entidad): permite la identificación de la clave pública correspondiente a la clave privada utilizada para firmar el certificado.
- Subject Key Identifier (Identificador de la clave de sujeto): permite la identificación de certificados que contienen una clave pública determinada.
- Key Usage (Uso de clave): define el propósito de la clave pública incorporada en el certificado.
- Extended Key Usage (Uso ampliado de claves): especifica uno o varios fines para los que la clave pública se puede utilizar además de los fines especificados por la extensión Key Usage.
- CRL Distribution Points (Puntos de distribución de CRL): especifica dónde se puede obtener información de la CRL.

El texto sin formato de un certificado emitido por ACM se parece al siguiente ejemplo:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:16:ad:85:d8:42:d1:8a:3f:33:fa:cc:c8:50:a8:9e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Example CA
        Validity
            Not Before: Jan 30 18:46:53 2018 GMT
            Not After : Jan 31 19:46:53 2018 GMT
        Subject: C=US, ST=VA, L=Herndon, O=Amazon, OU=AWS, CN=example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:a6:8a:aa:91:0b:63:e8:08:de:ca:e7:59:a4:
                    69:4c:e9:ea:26:04:d5:31:54:f5:ec:cb:4e:af:27:
                    e3:94:0f:a6:85:41:6b:8e:a3:c1:c8:c0:3f:1c:ac:
                    a2:ca:0a:b2:dd:7f:c0:57:53:0b:9f:b4:70:78:d5:
                    43:20:ef:2c:07:5a:e4:1f:d1:25:24:4a:81:ab:d5:
                    08:26:73:f8:a6:d7:22:c2:4f:4f:86:72:0e:11:95:
                    03:96:6d:d5:3f:ff:18:a6:0b:36:c5:4f:78:bc:51:
                    b5:b6:36:86:7c:36:65:6f:2e:82:73:1f:c7:95:85:
                    a4:77:96:3f:c0:96:e2:02:94:64:f0:3a:df:e0:76:
                    05:c4:56:a2:44:72:6f:8a:8a:a1:f3:ee:34:47:14:
                    bc:32:f7:50:6a:e9:42:f5:f4:1c:9a:7a:74:1d:e5:
                    68:09:75:19:4b:ac:c6:33:90:97:8c:0d:d1:eb:8a:
                    02:f3:3e:01:83:8d:16:f6:40:39:21:be:1a:72:d8:
```

```
                5a:15:68:75:42:3e:f0:0d:54:16:ed:9a:8f:94:ec:
                59:25:e0:37:8e:af:6a:6d:99:0a:8d:7d:78:0f:ea:
                40:6d:3a:55:36:8e:60:5b:d6:0d:b4:06:a3:ac:ab:
                e2:bf:c9:b7:fe:22:9e:2a:f6:f3:42:bb:94:3e:b7:
                08:73
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:84:8C:AC:03:A2:38:D9:B6:81:7C:DF:F1:95:C3:28:31:D5:F7:88:42
            X509v3 Subject Key Identifier:
                97:06:15:F1:EA:EC:07:83:4C:19:A9:2F:AF:BA:BB:FC:B2:3B:55:D8
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://example.com/crl

    Signature Algorithm: sha256WithRSAEncryption
         69:03:15:0c:fb:a9:39:a3:30:63:b2:d4:fb:cc:8f:48:a3:46:
         69:60:a7:33:4a:f4:74:88:c6:b6:b6:b8:ab:32:c2:a0:98:c6:
         8d:f0:8f:b5:df:78:a1:5b:02:18:72:65:bb:53:af:2f:3a:43:
         76:3c:9d:d4:35:a2:e2:1f:29:11:67:80:29:b9:fe:c9:42:52:
         cb:6d:cd:d0:e2:2f:16:26:19:cd:f7:26:c5:dc:81:40:3b:e3:
         d1:b0:7e:ba:80:99:9a:5f:dd:92:b0:bb:0c:32:dd:68:69:08:
         e9:3c:41:2f:15:a7:53:78:4d:33:45:17:3e:f2:f1:45:6b:e7:
         17:d4:80:41:15:75:ed:c3:d4:b5:e3:48:8d:b5:0d:86:d4:7d:
         94:27:62:84:d8:98:6f:90:1e:9c:e0:0b:fa:94:cc:9c:ee:3a:
         8a:6e:6a:9d:ad:b8:76:7b:9a:5f:d1:a5:4f:d0:b7:07:f8:1c:
         03:e5:3a:90:8c:bc:76:c9:96:f0:4a:31:65:60:d8:10:fc:36:
         44:8a:c1:fb:9c:33:75:fe:a6:08:d3:89:81:b0:6f:c3:04:0b:
         a3:04:a1:d1:1c:46:57:41:08:40:b1:38:f9:57:62:97:10:42:
         8e:f3:a7:a8:77:26:71:74:c2:0a:5b:9e:cc:d5:2c:c5:27:c3:
         12:b9:35:d5
```

CA raíz de ACM

Los certificados de entidad final pública emitidos por ACM derivan su confianza de las siguientes CA raíz de Amazon:

Nombre distintivo	Algoritmo de cifrado
CN=Amazon Root CA 1,O=Amazon,C=US	RSA de 2048 bits (`RSA_2048`)
CN=Amazon Root CA 2,O=Amazon,C=US	RSA de 4096 bits (`RSA_4096`)
CN=Amazon Root CA 3,O=Amazon,C=US	Elliptic Prime Curve de 256 bits (`EC_prime256v1`)
CN=Amazon Root CA 4,O=Amazon,C=US	Elliptic Prime Curve de 384 bits (`EC_secp384r1`)

La raíz de confianza predeterminada para los certificados emitidos por ACM es CN=Amazon Root CA 1,O=Amazon,C=US, que ofrece seguridad RSA de 2048 bits. Las otras raíces están reservadas para uso futuro. Todas las raíces tienen firma cruzada del certificado de la autoridad de certificación raíz de Starfield Services.

Para obtener más información, consulte Amazon Trust Services.

Dominio de ápex

Consulte Nombres de dominio.

Criptografía de clave asimétrica

A diferencia de la Criptografía de clave simétrica, la criptografía asimétrica utiliza claves distintas, pero relacionadas matemáticamente para cifrar y descifrar el contenido. Una de las claves es pública y suele estar disponible mediante un certificado X.509 v3. La otra clave es privada y se almacena de forma segura. El certificado X.509 asocia la identidad de un usuario, un equipo o cualquier otro recurso (el sujeto del certificado) a la clave pública.

Los certificados de ACM son certificados SSL/TLS X.509 que asocian la identidad de un sitio web y los detalles de una organización a la clave pública que contiene el certificado. ACM utiliza su AWS

KMS key para cifrar la clave privada. Para obtener más información, consulte Seguridad para las claves privadas del certificado.

Certificate Authority (Entidad de certificación)

Una autoridad de certificación (CA) es una entidad que emite certificados digitales. Desde el punto de vista comercial, el tipo más común de certificado digital se basa en el estándar ISO X.509. La CA emite certificados digitales firmados que reafirman la identidad del sujeto del certificado y vinculan dicha identidad a la clave pública del certificado. Una CA también suele administrar la revocación de certificados.

Registro de transparencia de certificados

Para protegerse contra los certificados SSL/TLS emitidos por error o por una CA comprometida, algunos navegadores requieren que los certificados públicos emitidos para su dominio se registren en un registro de transparencia de certificados. El nombre de dominio se registra. La clave privada no se registra. Los certificados que no se han registrado suelen generar un error en el navegador.

Puede monitorizar los registros para asegurarse de que solo se emitan para su dominio los certificados que usted ha autorizado. Puede utilizar un servicio como Certificate Search para comprobar los registros.

Antes de que Amazon CA emita un certificado SSL/TLS de confianza pública para su dominio, envía el certificado al menos a tres servidores de registro de transparencia de certificados. Estos servidores añaden el certificado a sus bases de datos públicas y devuelven una marca de tiempo de certificado firmada (SCT) a la CA de Amazon. Después, la CA incorpora la SCT al certificado, firma el certificado y lo emite para usted. Las marcas de tiempo se incluyen con otras extensiones X.509.

```
X509v3 extensions:

  CT Precertificate SCTs:
    Signed Certificate Timestamp:
      Version   : v1(0)
        Log ID    : BB:D9:DF:...8E:1E:D1:85
        Timestamp : Apr 24 23:43:15.598 2018 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:45:02:...18:CB:79:2F
```

```
    Signed Certificate Timestamp:
      Version   : v1(0)
        Log ID    : 87:75:BF:...A0:83:0F
        Timestamp : Apr 24 23:43:15.565 2018 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:45:02:...29:8F:6C
```

El registro de transparencia de certificados se lleva a cabo de forma automática al solicitar o renovar un certificado a menos que decida cancelarlo. Para obtener más información sobre la cancelación, consulte Cancelación del registro de transparencia de certificados.

Sistema de nombres de dominio

El sistema de nombres de dominio (DNS) es un sistema de nombres distribuido jerárquicamente para equipos y otros recursos conectados a Internet o a una red privada. El DNS se utiliza fundamentalmente para convertir los nombres de dominio con formato de texto, como `aws.amazon.com`, en direcciones IP (protocolo de Internet) numéricas con el formato `111.122.133.144`. La base de datos de DNS de su dominio, sin embargo, contiene un número de registros que se pueden utilizar para otros fines. Por ejemplo, cuando solicita un certificado, con ACM puede utilizar un registro CNAME para validar que es el propietario de un dominio, o bien que es quien lo controla. Para obtener más información, consulte Validación por DNS.

Nombres de dominio

Un nombre de dominio es una cadena de texto como, por ejemplo, `www.example.com` que el sistema de nombres de dominio (DNS) puede traducir en una dirección IP. Las redes informáticas, incluida Internet, utilizan direcciones IP en lugar de nombres de texto. Un nombre de dominio se compone de varias etiquetas separadas por puntos:

TLD

La última etiqueta se denomina dominio de nivel superior (TLD). Por ejemplo, `.com`, `.net` y `.edu`. Además, el TLD para las entidades registradas en algunos países es la abreviatura del nombre del país y se denomina código de país. Por ejemplo, `.uk` para el Reino Unido, `.ru` para Rusia y `.fr` para Francia. Cuando se utilizan códigos de país, se suele introducir un segundo nivel de jerarquía para el TLD con el fin de identificar el tipo de entidad registrada. Por ejemplo, el TLD `.co.uk` identifica compañías comerciales en el Reino Unido.

Dominio de ápex

El nombre de dominio de ápex incluye el dominio de nivel superior y lo amplía. Para los nombres de dominio que incluyen un código de país, el dominio de ápex incluye el código y, en su caso, las etiquetas que identifican el tipo de entidad registrada. El dominio de ápex no incluye subdominios (consulte el párrafo siguiente). En `www.example.com`, el nombre de dominio de ápex es `example.com`. En `www.example.co.uk`, el nombre de dominio de ápex es `example.co.uk`. A menudo se utilizan otros nombres en lugar de ápex, como base, desnudo, raíz, ápex raíz o ápex de zona.

Subdominio

Los nombres de subdominio se anteponen al nombre de dominio de ápex y se separan de él y entre sí con un punto. El nombre de subdominio más común es `www`, pero es posible utilizar cualquier otro. Los nombres de subdominio también pueden tener varios niveles. Por ejemplo, en `jake.dog.animals.example.com`, los subdominios son `jake`, `dog` y `animals`, por ese orden.

Superdominio

El dominio al que pertenece un subdominio.

FQDN

Un nombre de dominio completo (FQDN) es el nombre de DNS completo de un equipo, un sitio web u otro recurso conectado a una red o a Internet. Por ejemplo: `aws.amazon.com` es el FQDN de Amazon Web Services. Un FQDN incluye todos los dominios hasta el dominio de nivel superior. Por ejemplo, $[subdomain_1].[subdomain_2]...[subdomain_n].[apex\ domain].[top\text{-}level\ domain]$ representa el formato general de un FQDN.

PQDN

Un nombre de dominio que no está completo se denomina nombre de dominio incompleto (PQDN) y es ambiguo. Un nombre como $[subdomain_1.subdomain_2.]$ es un PQDN porque no se puede determinar el dominio raíz.

Registro

El derecho a utilizar un nombre de dominio lo delegan los registradores de nombres de dominio. Los registradores suelen estar acreditados por la ICANN (Internet Corporation for Assigned Names and Numbers). Además, otras organizaciones denominadas registros mantienen las bases de datos de TLD. Cuando se solicita un nombre de dominio, el registrador envía la información del solicitante al registro de TLD correspondiente. El registro asigna un nombre de dominio, actualiza la base de

datos de TLD y publica la información en WHOIS. Normalmente, los nombres de dominio deben comprarse.

Cifrado y descifrado

El cifrado es el proceso de determinación de la confidencialidad de los datos. El descifrado invierte el proceso y recupera los datos originales. Por lo general, los datos no cifrados se denominan habitualmente texto no cifrado, ya sea texto o no. Los datos encriptados se suelen llamar texto cifrado. La encriptación HTTPS de mensajes entre clientes y servidores utiliza algoritmos y claves. Los algoritmos definen el step-by-step procedimiento mediante el cual los datos de texto plano se convierten en texto cifrado (cifrado) y el texto cifrado se convierte de nuevo en texto plano original (descifrado). Las claves se utilizan por algoritmos durante el proceso de cifrado o descifrado. Las claves pueden ser privadas o públicas.

Nombre de dominio completo (FQDN)

Consulte Nombres de dominio.

Infraestructura de claves públicas

Una infraestructura de claves públicas (PKI) se compone de hardware, software, personas, políticas, documentos y procedimientos necesarios para crear, emitir, administrar, distribuir, utilizar, almacenar y revocar los certificados digitales. PKI facilita la transferencia segura de información a través de las redes de equipos.

Certificado raíz

Una entidad de certificación (CA) normalmente existe dentro de una estructura jerárquica que contiene otras muchas CA con relaciones principal-secundario claramente definidas entre ellas. Las CA secundarias o subordinadas están certificadas por su CA principal, lo que crea una cadena de certificados. La CA de la parte superior de la jerarquía se denomina “raíz de la CA” y su certificado se denomina “certificado raíz”. Este certificado suele estar autofirmado.

Capa de conexión segura (SSL)

La capa de conexión segura (SSL) y la Transport Layer Security (TLS) son protocolos criptográficos que proporcionan seguridad de comunicación a través de una red de equipos. TLS es el sucesor de

SSL. Los dos utilizan certificados X.509 para autenticar el servidor. Ambos protocolos negocian una clave simétrica entre el cliente y el servidor que se utiliza para cifrar el flujo de datos entre las dos entidades.

HTTPS seguro

HTTPS significa HTTP sobre SSL/TLS, un método seguro de HTTP que es compatible con la mayoría de los navegadores y servidores principales. Todas las solicitudes y respuestas de HTTP se cifran antes de enviarse a través de una red. HTTPS combina el protocolo HTTP con técnicas criptográficas simétricas, asimétricas y basadas en el certificado X.509. HTTPS funciona insertando una capa de seguridad criptográfica por debajo de la aplicación HTTP y por encima de la capa de transporte TCP del modelo de interconexión de sistemas abiertos (OSI). La capa de seguridad utiliza el protocolo de capa de conexión segura (SSL) o el protocolo Transport Layer Security (TLS).

Certificados de servidor SSL

Las transacciones HTTPS requieren certificados de servidor para autenticar un servidor. Un certificado de servidor es una estructura de datos X.509 v3 que vincula la clave pública del certificado al asunto del certificado. Un certificado SSL/TLS está firmado por una entidad de certificación (CA) y contiene el nombre del servidor, el periodo de validez, la clave pública, el algoritmo de firma y mucho más.

Criptografía de clave simétrica

La criptografía de clave simétrica utiliza la misma clave tanto para cifrar como para descifrar datos digitales. Véase también Criptografía de clave asimétrica.

seguridad de la capa de transporte (TLS)

Consulte Capa de conexión segura (SSL).

Confianza

Para que un navegador web confíe en la identidad de un sitio web, el navegador debe tener la posibilidad de verificar el certificado del sitio web. Los navegadores, sin embargo, solo confían en una pequeña cantidad de certificados conocidos como certificados raíz de la CA. Una tercera parte

de confianza, conocida como entidad de certificación (CA), valida la identidad del sitio web y emite un certificado digital firmado para el operador del sitio web. El navegador puede comprobar la firma digital para validar la identidad del sitio web. Si la validación se realiza correctamente, el navegador muestra un icono de un candado en la barra de direcciones.

Historial de documentos

En la siguiente tabla se describe el historial de publicación de la documentación que AWS Certificate Manager comenzó en 2018.

Cambio	Descripción	Fecha
La validación del correo electrónico de Mail Exchanger (MX) ha quedado obsoleta	ACM ya no admite el intercambiador de correo (MX). En su lugar, utilice la validación de DNS o especifiq ue un superdominio para recibir la validación por correo electrónico.	27 de junio de 2024
Añadir las mejores prácticas en torno a la separación a nivel de cuenta	Utilice la separación a nivel de cuenta en sus políticas siempre que sea posible. Si no es posible, puede restringir los permisos a nivel de cuenta o mediante las claves de condición del contexto de cifrado en sus políticas.	11 de junio de 2024
Próximamente quedará obsoleta la verificación del correo electrónico con WHOIS	Se agregó una nota sobre la obsolescencia de la verificac ión del correo electrónico con WHOIS a partir de junio de 2024.	5 de febrero de 2024
Se agregó soporte para las claves de condición	Se agregó soporte para las claves de condición de IAM al solicitar certificados de ACM. Para ver una lista de las condiciones admitidas , consulte https://docs.aws.	24 de agosto de 2023

	amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported.	
Se ha agregado compatibilidad con ECDSA	Se agregó soporte para el algoritmo de firma digital de curva elíptica (ECDSA) al solicitar un certificado de ACM. Para ver una lista de los algoritmos de clave admitidos, consulte https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms.	8 de noviembre de 2022
Nuevos CloudWatch eventos	Se agregaron los eventos de certificado de ACM caducado, certificado de ACM disponible y acción obligatoria para la renovación del certificado de ACM Para obtener una lista de CloudWatch los eventos compatibles, consultehttps://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	27 de octubre de 2022
Actualización de tipos de algoritmos de clave para la importación	Los certificados importados a ACM ahora pueden tener claves con algoritmos RSA y de curva elíptica adicionales. Para ver una lista de los algoritmos de clave admitidos actualmente, consulte https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html.	14 de julio de 2021

Promoción de “Monitoreo y registro” como un capítulo separado	Se ha movido la documentación de monitoreo y registro a su propio capítulo. Este cambio incluye CloudWatch Metrics, CloudWatch Events/ EventBridge y. CloudTrail Para obtener más información, consulte https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html.	23 de marzo de 2021
Se agregó compatibilidad con CloudWatch métricas y eventos	Se agregaron DaysToExpiry métricas y eventos y API compatibles. Para obtener más información, consulte https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html y https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	3 de marzo de 2021
Se agregó soporte entre cuentas	Se agregó soporte multicuenta para usar CA privadas desde Autoridad de certificación privada de AWS. Para obtener más información, consulte https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html.	17 de agosto de 2020

Se agregó compatibilidad con regiones	Se agregó soporte regional para las regiones de AWS China (Beijing y Ningxia). Para obtener una lista completa de las regiones admitidas , consulte https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region.	4 de marzo de 2020
Se agregaron pruebas de flujo de trabajo de renovación	Los clientes ahora pueden probar manualmente la configuración de su flujo de trabajo de renovación administrado de ACM. Para obtener más información, consulte la sección Prueba de la configuración de renovación administrada de ACM.	14 de marzo de 2019
El registro de transparencia de certificados ahora es predeterminado	Se ha agregado de forma predeterminada la capacidad de publicar certificados públicos de ACM en los registros de transparencia de certificados.	24 de abril de 2018
Lanzamiento Autoridad de certificación privada de AWS	Se lanzó ACM Private Certificate Manager (CM) y su extensión permite a los usuarios establecer una infraestructura administrada segura para emitir y revocar certificados digitales privados. AWS Certificate Manager Para obtener más información, consulte AWS Private Certificate Authority.	4 de abril de 2018

Registro de transparencia de certificados	Se ha añadido el registro de transparencia de certificados a las prácticas recomendadas.	27 de marzo de 2018

En la siguiente tabla se describe el historial de publicación de la documentación AWS Certificate Manager anterior a 2018.

Cambio	Descripción	Fecha de lanzamiento
Nuevo contenido	Se ha añadido la validación por DNS a Validación por DNS.	21 de noviembre de 2017
Nuevo contenido	Se han añadido nuevos ejemplos de código de Java para Uso de la API (ejemplos de Java).	12 de octubre de 2017
Nuevo contenido	Se ha añadido información sobre los registros de CAA a (Opcional) Configuración de un registro de CAA.	21 de septiembre de 2017
Nuevo contenido	Se ha añadido información sobre dominios .IO a Solución de problemas.	07 de julio de 2017
Nuevo contenido	Se ha añadido información sobre reimportación de un certificado a Volver a importar un certificado.	07 de julio de 2017
Nuevo contenido	Se ha añadido información sobre asignación de certificados a Prácticas recomendadas y a Solución de problemas.	07 de julio de 2017

Cambio	Descripción	Fecha de lanzamiento
Nuevo contenido	Agregado AWS CloudFormation aServicios integrados con AWS Certificate Manager.	27 de mayo de 2017
Actualización	Se ha añadido más información a Cuotas.	27 de mayo de 2017
Nuevo contenido	Se ha agregado documentación sobre Identity and Access Management para AWS Certificate Manager.	28 de abril de 2017
Actualización	Se ha añadido un gráfico para mostrar el destino del correo electrónico de validación. Consulte Validación por correo electrónico.	21 de abril de 2017
Actualización	Se ha añadido información sobre la configuración de correo electrónico para su dominio. Consulte (Opcional) Configuración del correo electrónico para el dominio.	6 de abril de 2017
Actualización	Se ha añadido información sobre la comprobación del estado de renovación del certificado en la consola. Consulte Verificar el estado de renovación de un certificado.	28 de marzo de 2017
Actualización	Se ha actualizado la documentación para utilizar Elastic Load Balancing.	21 de marzo de 2017

Cambio	Descripción	Fecha de lanzamiento
Nuevo contenido	Se agregó compatibilidad AWS Elastic Beanstalk con Amazon API Gateway. Consulte Servicios integrados con AWS Certificate Manager.	21 de marzo de 2017
Actualización	Se ha actualizado la documentación sobre Renovación administrada.	20 de febrero de 2017
Nuevo contenido	Se ha agregado documentación sobre Importar certificados.	13 de octubre de 2016
Nuevo contenido	Se agregó AWS CloudTrail soporte para las acciones de ACM. Consulte Utilizándolo con CloudTrail AWS Certificate Manager.	25 de marzo de 2016
Nueva guía	Esta versión introduce AWS Certificate Manager.	21 de enero de 2016

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.