
AWS Certificate Manager

Guía del usuario

Version 1.0



AWS Certificate Manager: Guía del usuario

Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

¿Qué es AWS Certificate Manager?	1
Conceptos	1
Características de los certificados de ACM	3
Regiones admitidas	4
Servicios integrados	4
Precintos del sitio y logotipos de confianza	6
Límites	6
Número de certificados de ACM al año (últimos 365 días)	7
Cantidad de nombres de dominio por certificado de ACM	7
Añadir o eliminar nombres de dominio	7
prácticas recomendadas	7
AWS CloudFormation	8
Asignación de certificados	8
Precios	8
Configuración	10
Configurar IAM y AWS	10
Suscribirse en AWS	10
Creación de un usuario de IAM	10
Registrar un nombre de dominio	11
Configurar correo electrónico	11
Base de datos WHOIS	11
Registro MX	11
Configurar su sitio web o aplicación	12
Inicio rápido de Linux	12
Inicio rápido de Windows	13
(Opcional) Configuración de una CAA	13
Introducción	15
Solicitar un certificado	15
Validar propiedad de dominio	16
Administrar certificados de ACM	20
Administrar certificados de ACM (consola)	20
Administrar certificados de ACM (AWS CLI)	22
Instalar Certificados de ACM	23
Renovación administrada	24
Cómo funciona la validación de dominios	24
Cómo funciona la validación automática de dominios	25
Cómo funciona la validación de dominio manual	25
Configurar su dominio de validación automática	26
Comprobar el estado de renovación de un certificado	27
Significado del estado de la renovación de un certificado	27
Solicitar un correo electrónico de validación de dominio para renovación de certificado	28
Importar certificados	29
Requisitos previos	29
Importar un certificado	30
Importar mediante la consola	30
Importe utilizando el AWS CLI	31
Reimportar un certificado	31
Reimportar utilizando la consola	31
Reimportar utilizando el AWS CLI	32
Etiquetar certificados de ACM	33
Restricciones de las etiquetas	33
Gestión de etiquetas	34
Administración de etiquetas (Consola)	34
Administración de etiquetas (AWS Command Line Interface)	35

Administración de etiquetas (API de AWS Certificate Manager)	35
Autenticación y control de acceso	36
Autenticación	36
Control de acceso	37
Información general sobre la administración de acceso	37
Recursos y operaciones de ACM	38
Titularidad de los recursos	38
Administración de acceso a certificados de ACM	38
Políticas administradas por AWS	39
AWSCertificateManagerReadOnly	39
AWSCertificateManagerFullAccess	39
Políticas administradas por el cliente	40
Políticas insertadas	40
Creación de una lista de certificados	41
Recuperación de un certificado	41
Importación de un certificado	41
Borrar un certificado	41
Acceso de solo lectura a ACM	42
Acceso completo a ACM	42
Acceso de administrador a todos los recursos de AWS	43
Referencia de los permisos de la API de ACM	43
Uso de AWS CloudTrail	45
Registro de llamadas a la API ACM	45
Adición de etiquetas	46
Borrar un certificado	47
Descripción de un certificado	47
Recuperación de un certificado	48
Importar un certificado	49
Creación de una lista de certificados	50
Visualización de etiquetas	51
Eliminar etiquetas	51
Solicitud de un certificado	52
Reenviando correo electrónico de validación	53
Registro de llamadas a la API relacionadas con ACM	53
Creación de un balanceador de carga	54
Registrar Amazon EC2	54
Cifrando una clave privada	55
Descifrando una clave privada	56
Uso de la API de ACM	58
AddTagsToCertificate	58
DeleteCertificate	60
DescribeCertificate	61
GetCertificate	63
ImportCertificate	65
ListCertificates	67
ListTagsForCertificate	68
RemoveTagsFromCertificate	70
RequestCertificate	71
ResendValidationEmail	73
Seguridad de la clave privada de ACM	75
Solución de problemas	76
Registros de CAA	76
Email	76
No he recibido el correo electrónico de validación	77
Correo electrónico enviado al subdominio	78
Información de contacto oculta	78
Renovación de certificados	79

Limitación controlada de WHOIS	79
Importación de certificados	79
Asignación de certificados	80
Solicitudes de certificados	80
Tiempo de espera de solicitud de certificado agotado	80
Error de solicitud de certificado	80
Renovación de certificados	82
Validación de dominio	82
Proceso asíncrono	82
Validación de certificados	82
Validación incompleta	82
Dominios .IO	83
Historial de revisión	84

¿Qué es AWS Certificate Manager?

(AWS Certificate Manager ACM) facilita la compleja tarea de crear y gestionar certificados SSL/TLS para sus sitios web y aplicaciones basados en AWS. Puede utilizar los [certificados que proporciona ACM \(p. 15\)](#) (certificados de ACM) o los [certificados que importe a ACM \(p. 29\)](#).

No puede instalar un certificado de ACM directamente en su sitio web o aplicación. Debe instalar el certificado a través de uno de los servicios integrados con ACM. Para obtener más información acerca de estos servicios, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Para obtener más información general sobre ACM, consulte los siguientes temas.

Temas

- [Conceptos \(p. 1\)](#)
- [Características de los certificados de ACM \(p. 3\)](#)
- [Regiones admitidas \(p. 4\)](#)
- [Servicios integrados con AWS Certificate Manager \(p. 4\)](#)
- [Precintos del sitio y logotipos de confianza \(p. 6\)](#)
- [Límites \(p. 6\)](#)
- [prácticas recomendadas \(p. 7\)](#)
- [Precios de AWS Certificate Manager \(p. 8\)](#)

Conceptos

Esta sección presenta términos y conceptos básicos relacionados con AWS Certificate Manager (ACM).

Certificate Authority

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. El CA también gestiona normalmente la revocación de certificados.

Sistema de nombres de dominio

El sistema de nombres de dominio (DNS) es un sistema de nombramiento distribuido jerárquicamente para equipos y otros recursos conectados a Internet o a una red privada. DNS traduce los nombres de dominio textuales, como `http://aws.amazon.com`, en direcciones IP numéricas (protocolo de Internet).

Nombre de dominio

Un nombre de dominio completo (FQDN) es el nombre completo y legible para un equipo u otros recursos conectados a Internet. Por ejemplo, `aws.amazon.com` es el FQDN para Amazon Web Services. Un FQDN se compone de varias partes. En el ejemplo anterior, `aws` es el nombre del host ubicado en el dominio `amazon.com` y `.com` es el dominio de nivel superior. El sufijo `.com` se utiliza generalmente para representar la actividad comercial. Existen muchos dominios distintos de nivel superior, incluidos `.net` y `.edu`.

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 procedimiento paso a paso mediante el cual los datos de texto no cifrado se convierten en texto cifrado (encriptación) y el texto cifrado se vuelve a convertir en el texto cifrado original (proceso de 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 [Nombre de dominio](#) (p. 1).

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 autoridad de certificado normalmente existe dentro de una estructura jerárquica que contiene múltiples CA con relaciones principal-secundario claramente definidas entre ellas. Las CA secundarias 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. Ambos utilizan los certificados X.509 para autenticar el servidor y 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.

Seguridad de la capa de transporte (TLS)

Consulte [Capa de conexión segura \(SSL\)](#) (p. 2).

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.

Características de los certificados de ACM

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

Note

Estas características se aplican únicamente a los certificados proporcionados por ACM. Puede que no se apliquen a los [certificados que usted importe a ACM \(p. 29\)](#).

Validación de dominio (DV)

Los certificados de ACM son validados por dominio. Es decir, el campo de asunto de un certificado de ACM identifica un nombre de dominio y nada más. En la solicitud se envía un correo electrónico al propietario registrado de cada nombre de dominio. El propietario del dominio o un representante autorizado puede aprobar la solicitud del certificado siguiendo las instrucciones del correo electrónico. Para obtener más información, consulte [Validar propiedad de dominio \(p. 16\)](#).

Periodo de validez

El periodo de validez de los certificados de ACM actualmente es de 13 meses.

Renovación e implementación administradas

ACM administra el proceso de renovación de los certificados de ACM y el aprovisionamiento de los mismos una vez renovados. La renovación automática puede ayudarle a evitar el tiempo de inactividad debido a certificados configurados incorrectamente, revocados o expirados. Para obtener más información, consulte [Renovación administrada para certificados emitidos por Amazon de ACM \(p. 24\)](#).

Confianza de navegador y de aplicación

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 en una 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.

Varios nombres de dominio

Cada certificado de ACM debe incluir al menos un nombre de dominio totalmente cualificado (FQDN). Puede añadir nombres adicionales si lo desea. Por ejemplo, cuando cree un certificado de ACM para `www.example.com`, puede añadir el nombre `www.example.net` si los clientes pueden acceder a su sitio utilizando ambos 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 añadir el nombre `example.com`. Para obtener más información, consulte [Solicitar un certificado \(p. 15\)](#).

Nombres con comodines

ACM le 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 protege solo 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.

Algoritmos

En la actualidad, ACM es compatible con el cifrado RSA-2048 y los algoritmos hash SHA-256.

Excepciones

Tenga en cuenta lo siguiente:

- ACM no proporciona certificados de validación extendida (EV) ni certificados de validación de organización (OV).
- ACM solo proporciona certificados para protocolos SSL/TLS.
- No puede utilizar certificados de ACM para la firma de código o el cifrado de correos electrónicos.
- ACM solo admite ASCII con codificación UTF-8 para los nombres de dominio, incluidas las etiquetas que contienen "xn--" (Punycode). ACM no acepta entradas Unicode (etiquetas u) para nombres de dominio.
- ACM actualmente no le permite desactivar la [renovación de certificados administrada \(p. 24\)](#) de los certificados proporcionados por ACM. La renovación administrada no está disponible para los certificados que importe 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 puede descargar la clave privada para un certificado de ACM.
- No se puede asociar los certificados de ACM a instancias Amazon Elastic Compute Cloud (Amazon EC2).

Regiones admitidas

Visite [Regiones y puntos de conexión de AWS](#) en la AWS General Reference o la [Tabla de regiones de AWS](#) para ver la disponibilidad regional de ACM.

Al igual que la mayoría de los recursos de AWS, los certificados de ACM también son recursos regionales. Para utilizar un certificado con Elastic Load Balancing para el mismo nombre completo del dominio (FQDN) o el conjunto de FQDN en más de una región de AWS, debe solicitar o importar un certificado para cada región. En el caso de los certificados proporcionados por ACM, esto significa que debe validar cada nombre de dominio en el certificado de cada región. No puede copiar un certificado de una región en otra.

Para utilizar un certificado de ACM con Amazon CloudFront, debe solicitar o importar el certificado en la región US East (N. Virginia). Los certificados de ACM de esta región que estén asociados a una distribución de CloudFront se distribuyen a todas las ubicaciones geográficas configuradas para esa distribución.

Servicios integrados con AWS Certificate Manager

AWS Certificate Manager da soporte a un número creciente de servicios de AWS. No puede utilizar ACM para instalar directamente su certificado de ACM en su aplicación o sitio web basado en AWS. Debe utilizar uno de los siguientes servicios.

Elastic Load Balancing

Elastic Load Balancing distribuye automáticamente su tráfico entrante de aplicaciones en múltiples instancias 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 automáticamente su capacidad de gestión de solicitudes en respuesta al tráfico entrante. Para obtener más información sobre el balanceo de carga, consulte [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 Amazon EC2 de backend. ACM se integra con Elastic Load Balancing para implementar los certificados de ACM en el balanceador de carga. Para obtener más información, consulte la sección [Crear un Application Load Balancer](#).

Amazon CloudFront

Amazon CloudFront es un servicio web que acelera la distribución de su contenido web estático y dinámico para los usuarios finales mediante la entrega de su contenido desde una red mundial de ubicaciones de borde. Cuando un usuario final solicita contenido que usted distribuye a través de CloudFront, al usuario se le remite a la ubicación de borde que ofrece la latencia más baja. De este modo, se garantiza que el contenido se entrega con el máximo desempeño posible. Si el contenido se encuentra actualmente en dicha ubicación de borde, CloudFront lo entrega inmediatamente. Si el contenido no se encuentra actualmente en dicha ubicación de borde, CloudFront lo recupera del servidor web o el bucket de Amazon S3 que usted haya identificado como la fuente de contenido definitiva. Para obtener más información sobre CloudFront, consulte [Guía para desarrolladores de Amazon CloudFront](#).

Para distribuir contenido protegido a través de SSL/TLS, CloudFront requiere que los certificados SSL/TLS se instalen en la distribución de CloudFront o en la fuente de contenido de backend. ACM se integra con CloudFront para implementar certificados de ACM en la distribución de CloudFront. Para obtener más información, consulte la sección [Obtener un certificado SSL/TLS](#).

Note

Para utilizar un certificado de ACM con CloudFront, debe solicitar o importar el certificado en la región US East (N. Virginia).

AWS Elastic Beanstalk

Elastic Beanstalk le ayuda a implementar y administrar aplicaciones en la nube de AWS sin tener que preocuparse por la infraestructura en la que se ejecutan. 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, equilibrio de carga, escalado y monitorización de la salud. Elastic Beanstalk utiliza el servicio Elastic Load Balancing para crear un balanceador de carga. Para obtener más información sobre Elastic Beanstalk, consulte [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 la sección [Configuración de su balanceador de carga del entorno Elastic Beanstalk para terminar HTTPS](#).

Amazon API Gateway

Con API Gateway, puede publicar, mantener, supervisar y proteger sus operaciones de API. API Gateway crea para usted una distribución de CloudFront y utiliza AWS Certificate Manager cuando usted configura un nombre de dominio personalizado como su nombre de host de la API. Para obtener más información sobre API Gateway, consulte [Guía para desarrolladores de API Gateway](#). Para obtener más información acerca de cómo utilizar ACM con API Gateway, consulte la sección [Utilización de nombres de dominio personalizados como nombre de host API Gateway](#).

AWS CloudFormation

AWS CloudFormation le ayuda a diseñar y configurar sus recursos de Amazon Web Services. Puede crear una plantilla que describa los recursos de AWS que desee utilizar, como Elastic Load Balancing o API Gateway. A continuación, AWS CloudFormation se encarga de aprovisionar y configurar para

usted dichos recursos. No es necesario crear y configurar individualmente los recursos de AWS ni averiguar qué depende de qué. AWS CloudFormation se encarga de todo eso. Los certificados de ACM se incluyen como plantilla de recursos, lo que significa que AWS CloudFormation puede solicitar certificados de ACM que usted puede utilizar con servicios de AWS para permitir las conexiones seguras. Para obtener más información, consulte [AWS::CertificateManager::Certificate](#). Además, los certificados de ACM se incluyen con muchos de los recursos de AWS que usted puede configurar con AWS CloudFormation.

Note

Si crea un certificado de ACM con AWS CloudFormation, la pila AWS CloudFormation 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](#).

Precintos 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 precinto de sitio seguro que usted pueda utilizar 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 precintos y las insignias de este tipo pueden copiarse en sitios que no utilicen el servicio ACM, y es posible que sean utilizados de forma inadecuada para crear confianza con falsas pretensiones. Para proteger a nuestros clientes y la reputación de Amazon no permitimos que nuestra marca comercial y nuestro logotipo se utilicen de esta manera.

Límites

Los siguientes límites de AWS Certificate Manager (ACM) son aplicables a todas las regiones y cuentas de AWS. Para solicitar límites superiores, abra un caso en el [Centro de AWS Support](#). Las nuevas cuentas de AWS pueden comenzar con límites inferiores a los aquí descritos.

Elemento	Límite predeterminado
Número de certificados de ACM	100
Número de certificados importadas	100
Cantidad de nombres de dominio por certificado de ACM	10. Consulte la información a continuación de esta tabla.
Número de certificados de ACM al año	El doble del límite de su cuenta. Consulte la información a continuación de esta tabla.

Note

El límite de cantidad de nombres de dominio por certificado de ACM es aplicable solo a certificados proporcionados por ACM. Este límite no es aplicable a [los certificados que importa a ACM](#) (p. 29). Las secciones siguientes son aplicables solo a certificados proporcionados por ACM.

Número de certificados de ACM al año (últimos 365 días)

Puede solicitar hasta el doble del límite de certificados de ACM cada año. Por ejemplo, si el límite es de 25, puede solicitar hasta 50 certificados de ACM al año. Por supuesto, si solicita 50 certificados, debe eliminar 25 durante el año para mantenerse dentro de su límite. Si necesita más de 25 certificados, debe ponerse en contacto con el Centro de AWS Support.

Note

Aunque en la tabla anterior se indica que una cuenta puede poseer hasta 100 certificados de ACM, las nuevas cuentas de AWS pueden empezar con un límite inferior.

Cantidad de nombres de dominio por certificado de ACM

El límite predeterminado es 10 nombres de dominio por certificado de ACM. Ese límite puede ser superior. 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 su límite, abra un caso en el [Centro de AWS Support](#), pero antes de hacerlo, lea la siguiente información para conocer cómo añadir más nombres de dominio puede significar más trabajo administrativo para usted.

Para que se pueda emitir un certificado de ACM, debe [validar la propiedad \(p. 16\)](#) de todos los nombres de dominio de la solicitud. Puede recibir hasta 8 correos electrónicos de validación por nombre de dominio, y deberá actuar sobre al menos uno de ellos en un plazo de 72 horas. Por ejemplo, si solicita un certificado con 5 nombres de dominio, recibirá hasta 40 correos electrónicos de validación y deberá actuar sobre al menos 5 de ellos en un plazo de 72 horas. A medida que la cantidad de nombres de dominio de la solicitud de certificado aumenta, el trabajo necesario para validar la titularidad de los dominios también.

Añadir o eliminar nombres de dominio

No se pueden añadir 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. Al igual que con cualquier certificado nuevo, debe [validar la propiedad \(p. 16\)](#) de todos los nombres de dominio de la solicitud, incluso los que ya se habían validado para el certificado original.

Por ejemplo, si el certificado tiene 5 nombres de dominio y desea añadir 4 más, debe solicitar un certificado nuevo con los 9 nombres de dominio. Esto se traduce en hasta 72 correos electrónicos, de los cuales habrá al menos 9 sobre los que deberá actuar en un plazo de 72 horas.

A medida que la cantidad de nombres de dominio de la solicitud de certificado aumente, el trabajo necesario para validar la titularidad de los dominios cada vez que desee realizar un cambio en los nombres de dominio en el certificado también aumentará.

prácticas recomendadas

Las prácticas recomendadas son recomendaciones que pueden ayudarle a utilizar AWS Certificate Manager (AWS Certificate Manager) con mayor eficacia. Las siguientes prácticas recomendadas se basan en experiencias reales de clientes de ACM actuales.

Temas

- [AWS CloudFormation \(p. 8\)](#)
- [Asignación de certificados \(p. 8\)](#)

AWS CloudFormation

Con AWS CloudFormation puede crear una plantilla que describa los recursos de AWS que desea utilizar. A continuación, AWS CloudFormation aprovisiona y configura dichos recursos. AWS CloudFormation permite aprovisionar recursos compatibles con ACM como Elastic Load Balancing, Amazon CloudFront y Amazon API Gateway. Para obtener más información, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Si utiliza AWS CloudFormation, puede crear y eliminar rápidamente varios entornos de pruebas, le recomendamos que no cree un certificado de ACM independiente para cada entorno. Al hacerlo, su certificado agotará rápidamente el límite del certificado. Para obtener más información, consulte [Límites \(p. 6\)](#). 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 en su lugar un único certificado comodín para `<*>.service.example.com`. Incluya el certificado comodín en la plantilla que AWS CloudFormation utiliza para crear su entorno de pruebas.

Asignación de certificados

La asignación de certificados, en ocasiones denominada asignación 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 de la autoridad de certificados (CA) raíz hasta los certificados CA subordinados, si procede, y hasta el certificado o el host remoto al final 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 la clave pública o el certificado del host remoto a la aplicación durante el desarrollo, o la aplicación puede agregar el certificado o la clave cuando se conecta por primera vez al host.

Warning

Le recomendamos que su aplicación no asigne un certificado de ACM. ACM realiza [Renovación administrada para certificados emitidos por Amazon de ACM \(p. 24\)](#) para renovar automáticamente sus certificados SSL/TLS emitidos por Amazon antes de que caduquen. Para renovar un certificado, ACM genera un nuevo par de claves pública y privada. Si su aplicación asigna el certificado de ACM y el certificado se renueva correctamente con una nueva clave pública, puede que la aplicación no se conecte a su dominio.

Si decide asignar 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 su aplicación al certificado importado. ACM no intenta renovar automáticamente los certificados importados.
- Asigne su aplicación a un certificado raíz [de Amazon](#).

Precios de AWS Certificate Manager

AWS no le aplicará ningún cargo por los certificados SSL/TLS que administre con AWS Certificate Manager. Solo pagará por los recursos de AWS que cree para ejecutar su sitio web o aplicación. Para

obtener información actualizada sobre los precios de ACM, consulte la página de [Precios de AWS Certificate Manager](#) en el sitio web de AWS.

Configuración

AWS Certificate Manager (ACM) le permite aprovisionar y administrar certificados SSL/TLS para sus aplicaciones y sitios web basados en AWS. Utilice ACM para crear (o importar) y administrar certificados. Para implementar el certificado en su sitio web o aplicación necesita utilizar otros servicios de AWS. Para obtener más información acerca de los servicios integrados con ACM, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#). Los siguientes temas tratan los pasos a seguir antes de poder utilizar ACM.

Note

Además de utilizar los certificados proporcionados por ACM, también puede importar certificados a ACM. Para obtener más información, consulte [Importar certificados \(p. 29\)](#).

Temas

- [Configurar IAM y AWS \(p. 10\)](#)
- [Registrar un nombre de dominio \(p. 11\)](#)
- [Configurar correo electrónico para su dominio \(p. 11\)](#)
- [Configurar su sitio web o aplicación \(p. 12\)](#)
- [\(Opcional\) Configuración de un registro de CAA \(p. 13\)](#)

Configurar IAM y AWS

Para poder utilizar ACM debe inscribirse en Amazon Web Services. Si lo desea, puede crear un usuario de IAM para limitar las acciones puede realizar cada usuario.

Suscribirse en AWS

Si todavía no es cliente de Amazon Web Services (AWS), debe inscribirse para poder utilizar ACM. Su cuenta se inscribe automáticamente en todos los servicios disponibles, pero solo se le cobrará por los que utilice. Si es cliente nuevo de AWS, puede comenzar de forma gratuita. Obtenga más información acerca de la [Capa gratuita de AWS](#).

Para inscribirse en una cuenta de AWS

1. Visite <https://aws.amazon.com/> y seleccione Inscribirse.
2. Siga las instrucciones en pantalla.

Note

Recibirá una llamada telefónica automatizada y deberá introducir el PIN proporcionado en el teclado del teléfono como parte del procedimiento de registro. También deberá proporcionar un número de tarjeta de crédito aunque se esté inscribiendo en la capa gratuita.

Creación de un usuario de IAM

Los servicios de Amazon Web Services requieren sus credenciales al obtener acceso a ellos para determinar si tiene permiso para usar sus recursos. La consola requiere su nombre de usuario y contraseña, y puede crear claves de acceso para utilizar la interfaz de línea de comandos o la API. Sin embargo, como sus credenciales raíz permiten acceso ilimitado, le recomendamos no utilizarlos en AWS. En su lugar, le recomendamos crear usuarios con permisos más limitados en AWS Identity and Access

Management (IAM). Es decir, crear un usuario de IAM y añadirlo a un grupo de IAM con un conjunto de permisos específico. Después podrá obtener acceso a AWS mediante una URL especial y las credenciales de usuario.

Por ejemplo, para crear un grupo de administrador y añadir usuarios al grupo, consulte [Creating an Administrator's Group](#) en [AWS Identity and Access Management User Guide](#). El usuario podrá iniciar sesión en la cuenta mediante una URL especial. Para obtener más información, consulte [Cómo inician sesión los usuarios en la cuenta](#).

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 acerca del registro de nombres de dominio con Amazon Route 53, consulte [Registering Domain Names Using Amazon Route 53](#) en la Guía para desarrolladores de Amazon Route 53.

Configurar correo electrónico para su dominio

Una vez registrado un nombre de dominio, utilice el sitio web del registrador para asociar sus direcciones de contacto con él. El registrador introduce las direcciones de correo electrónico de contacto en la base de datos WHOIS e introduce uno o más servidores de correo electrónico en los registros de intercambio de correo (MX) de un servidor DNS. ACM envía un correo electrónico de validación a las direcciones de contacto y a cinco direcciones administrativas formadas desde su registro MX. ACM envía hasta ocho correos electrónicos de validación cada vez que se crea un nuevo certificado, se renueva un certificado o se solicita nuevo correo de validación. El correo electrónico de validación contiene instrucciones para confirmar que el propietario del dominio o un representante designado aprueba el certificado de ACM. Para obtener más información sobre la validación, consulte [Validar propiedad de dominio \(p. 16\)](#). Si tiene problemas con el correo electrónico de validación, consulte [Solución de problemas del correo electrónico \(p. 76\)](#).

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 de 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

Registro MX

Al registrar su dominio, el registrador envía su registro de intercambio de correo (MX) a un servidor del sistema de nombres de dominio (DNS). Un registro MX indica qué servidores aceptan correo electrónico

para su dominio. El registro contiene un nombre de dominio completo (FQDN). Puede solicitar un certificado para dominios o subdominios de ápex.

Por ejemplo, si utiliza la consola para solicitar un certificado para `abc.xyz.example.com`, ACM primero intenta encontrar el registro MX de dicho subdominio. Si no se puede encontrar el registro, ACM realiza una búsqueda MX de `xyz.example.com`. Si no puede encontrar el registro, ACM realiza una búsqueda MX de `example.com`. Si no se puede encontrar el registro o no existe ningún registro MX, ACM elige el dominio original para el que se solicitó el certificado (`abc.xyz.example.com` en este ejemplo) y envía correos electrónicos a las siguientes cinco direcciones de administración comunes del sistema para el dominio o subdominio.

- `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`

Si utiliza la API [RequestCertificate](#) o el comando `request-certificate` de la AWS CLI, AWS no realiza una búsqueda del registro MX. En su lugar, `RequestCertificate` le permite especificar tanto el nombre de dominio como el nombre de un dominio de validación. Si especifica el parámetro opcional `ValidationDomain`, AWS envía aquí los cinco correos electrónicos anteriores en lugar de enviarlos a su dominio.

ACM siempre envía el correo electrónico de validación a las cinco direcciones comunes mostradas anteriormente si utiliza la consola, la API o la AWS CLI. Sin embargo, AWS solo realiza una búsqueda del registro MX cuando utiliza la consola para solicitar un certificado.

Configurar su sitio web o aplicación

Puede instalar su sitio web en una instancia de Amazon EC2 Linux o Windows. Para obtener más información sobre las instancias de Amazon EC2 de Linux, consulte la [Guía del usuario de Amazon Elastic Compute Cloud para Linux](#). Para obtener más información sobre las instancias de Amazon EC2 de Windows, consulte la [Guía del usuario de Amazon Elastic Compute Cloud para Microsoft Windows](#).

Aunque instale su sitio web en una instancia de Amazon EC2, no puede implementar directamente un certificado de ACM en dicha instancia. En su lugar, debe implementar su certificado a través de uno de los servicios integrados con ACM. Para obtener más información, consulte [Servicios integrados con AWS Certificate Manager](#) (p. 4).

Para poner en funcionamiento rápidamente su sitio web en Windows o Linux, consulte los siguientes temas.

Temas

- [Inicio rápido de Linux](#) (p. 12)
- [Inicio rápido de Windows](#) (p. 13)

Inicio rápido de Linux

Para crear su sitio web o aplicación en una instancia de Linux, puede elegir una imagen de máquina de Amazon (AMI) de Linux e instalar un servidor web Apache en ella. Para obtener más información, consulte el [Tutorial: Instalar un servidor web LAMP en Amazon Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Inicio rápido de Windows

Para adquirir un servidor de Microsoft Windows en el que pueda instalar su sitio web o aplicación, elija una AMI de Windows Server que se incluye con un servidor web Microsoft Internet Information Services (IIS). A continuación, utilice el sitio web predeterminado o cree uno nuevo. También puede instalar un servidor WIMP en su instancia Amazon EC2. Para obtener más información, consulte [Tutorial: instalación de un servidor WIMP en una instancia Amazon EC2 que ejecute Windows Server](#) en la Guía del usuario de Amazon EC2 para instancias de Windows.

(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 se permite a AWS Certificate Manager (ACM) emitir un certificado para su dominio o subdominio. Después de validar su dominio, ACM comprueba la presencia de registros de CAA para asegurarse de que puede emitir un certificado para usted. Puede elegir no configurar ningún registro de CAA para su dominio o dejar en blanco el registro si no desea permitir que ACM realice la comprobación de CAA. Un registro de CAA contiene los siguientes campos de datos:

flags

Especifica si ACM admite el valor del campo tag. 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 campo value tiene autorización para emitir un certificado para su dominio o subdominio.

issuewild

Indica que la CA de ACM especificada en el campo value 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. No obstante, si no dispone de un registro de CAA que especifique una de las cuatro CA de Amazon siguientes, 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.

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"
example.com.	CAA	0	issue	"amazon.com"
example.com.	CAA	0	issue	"amazontrust.com"
example.com.	CAA	0	issue	"awstrust.com"
example.com.	CAA	0	issue	"amazonaws.com"
example.com	CAA	0	issue	";"

Para obtener más información sobre cómo añadir o modificar registros DNS, consulte 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.

Introducción

Puede utilizar la consola, el AWS Command Line Interface (AWS CLI) o el SDK para empezar a utilizar AWS Certificate Manager. Los siguientes temas le ayudarán a comenzar con AWS Certificate Manager mediante el uso de la consola o el AWS CLI. Para obtener más información acerca del uso de SDK, consulte [Uso de la API de ACM \(p. 58\)](#).

Temas

- [Solicitar un certificado \(p. 15\)](#)
- [Validar propiedad de dominio \(p. 16\)](#)
- [Administrar certificados de ACM \(p. 20\)](#)
- [Instalar Certificados de ACM \(p. 23\)](#)

Solicitar un certificado

En las secciones siguientes se explica cómo utilizar la consola de ACM o la AWS CLI para solicitar un certificado de ACM. Si tiene problemas para solicitar un certificado, consulte [Solucionar problemas de solicitud de certificados \(p. 80\)](#). Si tiene problemas para solicitar un certificado para un dominio .IO, consulte [Solución de problemas de dominios .IO \(p. 83\)](#).

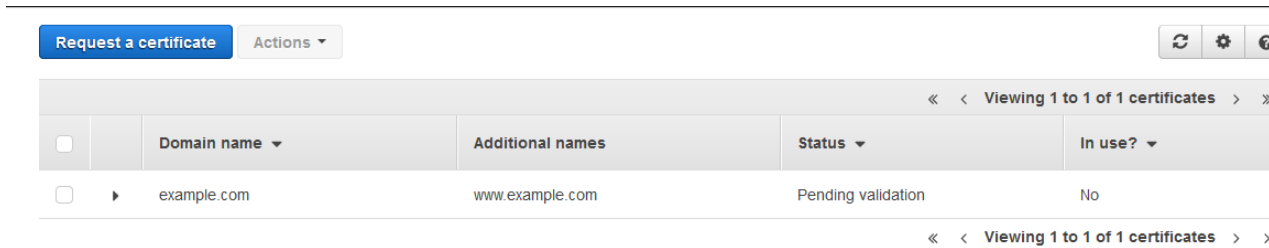
Para solicitar un certificado de ACM (consola)

1. Inicie sesión en la consola de administración de AWS y abra la consola de ACM en <https://console.aws.amazon.com/acm/home>. Si aparece la página de introducción, elija Get Started. De lo contrario, elija Request a certificate.
2. En la página Request a certificate, escriba su nombre de dominio. Puede utilizar un nombre de dominio completo (FQDN) como **www.example.com** o un nombre de dominio desnudo o ápex 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 **corp.example.com** y **images.example.com**. El nombre comodín aparecerá en el campo Subject y en la extensión Subject Alternative Name 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 **login.example.com** y **test.example.com**, pero no puede proteger **test.login.example.com**. Tenga en cuenta también que ***.example.com** protege solo los subdominios de **example.com**. No protege el dominio desnudo o ápex (**example.com**). Para proteger ambos, consulte el siguiente paso.

3. Para añadir más nombres de dominio al certificado de ACM, elija Add more names y escriba otro nombre de dominio en el cuadro de texto que se abra. Esto resulta útil para proteger tanto los dominios desnudos como los ápex (como **example.com**) y sus subdominios (***.example.com**).
4. Una vez que haya introducido los nombres de dominio válidos, elija Review and Request o Cancel para salir.
5. Si la página de revisión contiene la información correcta introducida para su solicitud, elija Confirm and request. La siguiente página muestra que el estado de su solicitud está pendiente de validación.



The screenshot shows the AWS Certificate Manager console. At the top, there is a 'Request a certificate' button and an 'Actions' dropdown. Below this is a table with the following columns: 'Domain name', 'Additional names', 'Status', and 'In use?'. The table contains one entry for 'example.com' with 'www.example.com' as an additional name, a status of 'Pending validation', and 'No' for 'In use?'. Navigation links like '<< < Viewing 1 to 1 of 1 certificates > >>' are visible at the top and bottom of the table.

	Domain name ▾	Additional names	Status ▾	In use? ▾
<input type="checkbox"/>	example.com	www.example.com	Pending validation	No

Antes de que pueda emitirse un certificado de ACM, un representante autorizado debe validar que fue solicitado. ACM envía un correo electrónico de validación a tres direcciones de contacto registradas en la base de datos WHOIS y a cinco direcciones de administración de sistemas comunes. Usted o un representante autorizado debe responder a uno de estos correos electrónicos. Para obtener más información, consulte [Validar propiedad de dominio \(p. 16\)](#).

Para solicitar un certificado de ACM (AWS CLI)

- Utilice el comando [certificado de solicitud](#) para solicitar un nuevo certificado de ACM en la línea de comando.

```
aws acm request-certificate --domain-name www.example.com
```

Consulte la [referencia AWS CLI](#) para obtener más información y ejemplos.

Validar propiedad de dominio

Note

La información en esta sección se aplica únicamente a los certificados proporcionados por ACM. ACM no valida la propiedad del dominio para [certificados que importe en ACM \(p. 29\)](#). Si tiene problemas para validar un certificado de ACM, consulte [Solución de problemas de validación de certificados \(p. 82\)](#). Si no recibe ningún correo electrónico, consulte [No he recibido el correo electrónico de validación \(p. 77\)](#).

En su solicitud de certificado puede especificar un nombre de dominio y varios nombres alternativos, hasta el límite permitido. Para obtener más información acerca de los límites, consulte [Límites \(p. 6\)](#). Antes de que la autoridad de certificados (CA) de Amazon pueda emitir un certificado para su sitio, AWS Certificate Manager (ACM) debe verificar que es el propietario o controla todos los dominios que ha especificado en la solicitud. ACM lo hace enviando un mensaje de correo de validación de dominio a las direcciones registradas para los dominios. Por cada nombre de dominio que incluya en su solicitud de certificado, se envía un correo electrónico a las 3 direcciones de contacto de WHOIS y a las 5 direcciones comunes del sistema para su dominio. Es decir, se enviará hasta 8 mensajes de correo electrónico por cada nombre de dominio que especifique en su solicitud. Por ejemplo, si especifica 1 solo nombre de dominio, recibirá hasta 8 mensajes de correo electrónico. Para validar, debe actuar sobre 1 de estos 8 mensajes en un plazo de 72 horas. Si especifica 3 nombres de dominio, recibirá hasta 24 mensajes. Para validar, debe actuar sobre 3 de los mensajes de correo electrónico, 1 por cada nombre especificado, en un plazo de 72 horas.

Se envía un correo electrónico a las siguientes tres direcciones de contacto registradas en WHOIS:

- Titularidad del dominio
- Contacto técnico
- Contacto administrativo

Note

Algunos registradores permiten ocultar la información de contacto en los listados de WHOIS y otros permiten sustituir la dirección de correo electrónico por una dirección privada (o proxy). Para evitar problemas en la recepción del correo electrónico de validación de dominio de ACM, asegúrese de que la información de contacto esté visible en WHOIS. Si el listado de WHOIS muestra una dirección de correo electrónico privada, asegúrese de que el correo electrónico enviado a dicha dirección se reenvíe a la dirección de correo electrónico real. O simplemente incluya su dirección de correo electrónico real.

Si utiliza la consola para solicitar un certificado, ACM realiza una búsqueda del registro MX para determinar qué servidores aceptan correo electrónico para su dominio y envía un correo electrónico a las cinco direcciones del sistema comunes siguientes para el primer dominio encontrado. Si utiliza la API `RequestCertificate` o el comando `request-certificate` de la AWS CLI, ACM no realiza una búsqueda del registro MX. En su lugar, envía un correo electrónico al nombre de dominio especificado en el parámetro `DomainName` o en el parámetro opcional `ValidationDomain`. Para obtener más información, consulte [Registro MX](#) (p. 11).

- `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 [Configurar correo electrónico para su dominio](#) (p. 11).

La consola muestra el destino de los mensajes de correo electrónico de validación para el primer nombre de dominio especificado en la solicitud. El correo electrónico se envía desde `no-reply@certificates.amazon.com`.

Status

Validation not complete
The status of this certificate request is "Pending validation". Further action is needed to validate and approve the certificate. [Learn more.](#)

Status	Pending validation
Detailed status	Email to validate the request was sent at 2017-04-07T01:43:33UTC but we have not yet received approval to issue the certificate for the following domains:
	<div><div>Example.com</div><div>postmaster@example.com administrator@example.com webmaster@example.com admin@example.com hostmaster@example.com</div></div>

Details

Type	Amazon Issued	Requested at	2017-04-07T01:43:33UTC
In use?	No	Public key info	RSA 2048-bit
Domain name	example.com	Signature algorithm	SHA256WITHRSA
Number of additional names	0	ARN	arn:aws:acm:us-east-1:123456789012:certificate-1234-1234-123456789012
Identifier	12345678-1234-1234-1234-123456789012		
Serial number	N/A		

Note

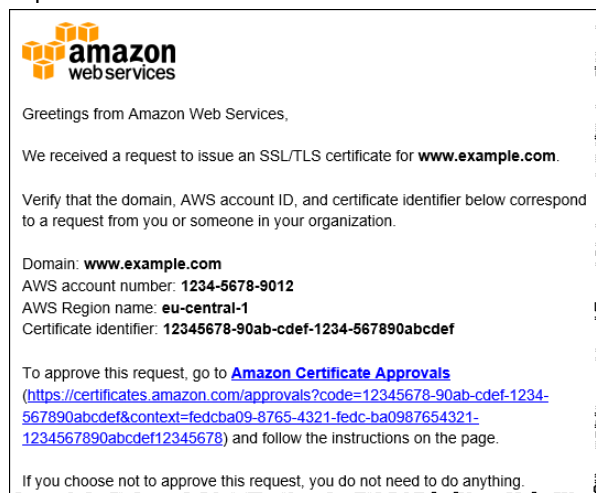
Existe una excepción al proceso descrito anteriormente. Si solicita un certificado de ACM para un nombre de dominio que empiece por `www` o un asterisco de comodín (`*`), ACM elimina las

letras **www** o el asterisco del principio y envía un correo a las direcciones administrativas. Estas direcciones se forman agregando el prefijo **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 hacerlo 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 direcciones administrativas comunes se forman de manera similar.

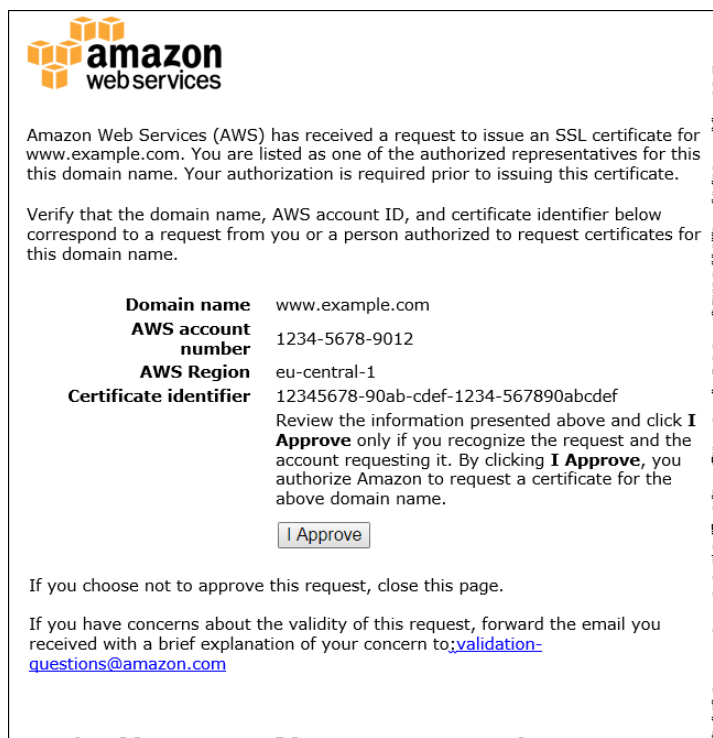
Note

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 hacerlo, especifique la opción **validationDomain** de la API [RequestCertificate](#) o el comando [request-certificate](#) de la AWS CLI. Esta característica no se admite actualmente en la consola.

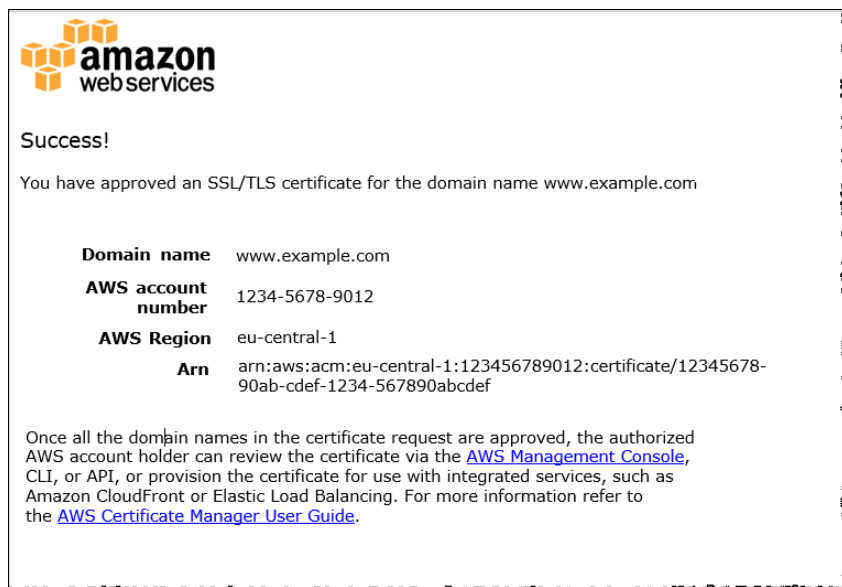
El siguiente ejemplo muestra el correo electrónico de validación que se envía por cada nombre de dominio especificado en la solicitud de certificado.



Elija el enlace que le envía al sitio web de aprobaciones de certificados de Amazon y, a continuación, elija **Approve**.



Después de elegir Approve, se abre un sitio web para indicar que la solicitud se ha realizado correctamente.



Puede volver a la consola de ACM haciendo clic en un enlace en la página de éxito. La columna Status en la consola muestra Issued para indicar que se ha emitido el certificado de ACM.

Request a certificate Actions ▾

<input type="checkbox"/>	Domain name ▾	Additional names	Status ▾	In use? ▾
<input type="checkbox"/>	▶ www.example.com	example.com	Issued	No

« < Viewing 1 to 1 of 1

Administrar certificados de ACM

Una vez que haya [solicitado](#) (p. 15) uno o más certificados y AWS Certificate Manager los haya proporcionado, puede administrar dichos certificados desde la Consola de administración de AWS o el AWS CLI. También puede administrar los [certificados importados](#) (p. 29).

Administrar certificados de ACM (consola)


Puede utilizar la consola ACM para obtener información o eliminar un certificado de ACM. Para los certificados proporcionados por ACM también puede hacer que ACM reenvíe el correo electrónico de validación.

Mostrar la información de certificados de ACM

Cada uno de los certificados de ACM ocupa una fila en la consola. De forma predeterminada, se muestran las siguientes columnas en cada certificado:

- Domain Name: el nombre de dominio totalmente cualificado para el certificado.
- Additional Names: nombres adicionales compatibles con este certificado.
- Status: estado del certificado. Puede ser cualquiera de los siguientes valores:
 - Pending validation
 - Issued
 - Inactivo
 - Expired
 - Revoked
 - Failed
 - Timed out
- In Use? si el certificado de ACM se relaciona activamente con un servicio AWS como Elastic Load Balancing o CloudFront. El valor puede ser No o Yes.

Personalizar la pantalla de la consola

Puede seleccionar las columnas que desee visualizar eligiendo el icono del engranaje () de la esquina superior derecha de la consola. Puede seleccionar de entre las siguientes columnas.

Show columns ×

Select which columns you would like to show/hide:

- ☒ Domain name
- ☒ Additional names
- ☐ Created at
- ☒ Status
- ☐ Signature algorithm
- ☐ Key algorithm
- ☐ Not before
- ☐ Not after
- ☐ Subject
- ☐ Issuer
- ☐ Revocation reason
- ☐ Serial
- ☐ Revoked at
- ☒ In use?
- ☐ Arn

Metadatos de certificado de visualización

Para mostrar los metadatos del certificado de ACM, elija la flecha situada a la izquierda inmediata del nombre de dominio. La consola muestra información similar a la siguiente.

[Request a certificate](#) Actions ▾

<input type="checkbox"/>	Domain name ▾	Additional names	Status ▾	In use? ▾
<input type="checkbox"/>	example.com	www.example.com	Issued	Yes

Status

Status Issued

Detailed status AWS issued the certificate at 2015-12-15T20:44:52UTC

Details

In use?	Yes	Created	2015-12-15T20:43:44UTC
Domain name	example.com	Not before	2015-12-15T00:00:00UTC
Number of additional names	1	Validity days	397
Additional names	www.example.com	Valid through	2017-01-15 (381 days)
Identifier	12345678-1234-1234-1234-123456789012	Public key info	RSA 2048-bit
Serial number	07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b	Signature algorithm	SHA-256 with RSA
Associated resources	arn:aws:cloudfront::123456789012:distribution/E12KXPQHVSVC	ARN	arn:aws:acm:us-east-1:123456789012:cert

Eliminar un certificado de ACM

En la lista de certificados, seleccione la casilla de verificación del certificado de ACM que desee borrar. En Actions, seleccione Delete.

Note

No puede eliminar un certificado de ACM que se esté utilizando en otro servicio de AWS. Para eliminar un certificado que esté en uso, primero debe eliminar la asociación del certificado.

Volver a enviar el correo electrónico de validación (certificados proporcionados por ACM)

Puede aprobar una solicitud de certificado de ACM a través de un token de validación que ACM envíe al representante autorizado. No obstante, puesto que el correo electrónico de validación necesario para el proceso de aprobación puede ser bloqueado por filtros de spam o perderse en el camino, el token de validación caduca automáticamente después de 72 horas. Si el representante registrado no recibe el correo electrónico original o si el token ha vencido, puede solicitar que el correo electrónico sea reenviado. Para ello, seleccione la casilla de verificación del certificado de ACM, elija **Actions** y, a continuación, elija **Resend validation email**. Si el periodo de 72 horas ha expirado y el estado del certificado ha cambiado a **Timed out**, no podrá volver a enviar el correo electrónico de validación.

Note

La información anterior se aplica únicamente a los certificados proporcionados por ACM. El correo electrónico de validación no es necesario para los [certificados que importe a ACM](#) (p. 29).

Administrar certificados de ACM (AWS CLI)

Puede utilizar el AWS CLI para obtener información acerca de un certificado expedido, eliminar un certificado o volver a enviar el correo electrónico de validación.

Recuperar los campos de certificado de ACM

Puede utilizar el comando de [certificado de descripción](#) para recuperar información sobre un certificado.

```
aws acm describe-certificate --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Eliminar un certificado de ACM

Puede utilizar el comando de [certificado de borrado](#) para eliminar un certificado.

```
aws acm delete-certificate --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Volver a enviar el correo electrónico de validación (certificados proporcionados por ACM)

Puede utilizar el [correo electrónico de validación del reenvío](#) para enviar de nuevo el correo electrónico de validación.

```
aws acm resend-validation-email --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012 --validation-domain example.com
```

Note

La orden del [correo electrónico de validación del reenvío](#) se aplica únicamente a los certificados proporcionados por ACM. El correo electrónico de validación no es necesario para los [certificados que importe a ACM](#) (p. 29).

Instalar Certificados de ACM

No puede utilizar ACM para instalar directamente su certificado de ACM en su aplicación o sitio web basado en AWS. Debe utilizar uno de los servicios integrados con ACM. Para obtener más información, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Renovación administrada para certificados emitidos por Amazon de ACM

ACM proporciona renovación administrada para los certificados SSL/TLS que tenga y haya emitido Amazon. Esto significa que ACM intenta renovar los certificados antes de que caduquen. Si es posible, ACM renueva los certificados automáticamente sin ninguna acción por su parte.

Note

La renovación automática no está disponible para los [certificados importados \(p. 29\)](#) ni para los certificados asociados con zonas alojadas privadas de Route 53. Debe renovar estos certificados manualmente. Para obtener más información, consulte [Cómo funciona la validación de dominio manual](#).

Note

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 \(p. 4\)](#). Si tiene certificados para el mismo nombre de dominio en varias regiones de AWS, ACM renueva cada uno de estos certificados de manera independiente.

Important

Su certificado de ACM debe estar asociado activamente con un servicio de AWS compatible para que se pueda renovar automáticamente. Para obtener información acerca de los recursos que admite ACM, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Para obtener más información sobre la renovación de certificados administrados, consulte los siguientes temas. Si tienes problemas con la renovación administrada, consulte [Solución de problemas de renovación administrada de certificados \(p. 82\)](#).

Temas

- [Cómo funciona la validación de dominios \(p. 24\)](#)
- [Configurar su dominio de validación automática \(p. 26\)](#)
- [Comprobar el estado de renovación de un certificado \(p. 27\)](#)
- [Solicitar un correo electrónico de validación de dominio para renovación de certificado \(p. 28\)](#)

Cómo funciona la validación de dominios

Antes de renovar un certificado, ACM intenta validar automáticamente cada nombre de dominio del certificado. Para obtener más información, consulte [Cómo funciona la validación automática de dominios \(p. 25\)](#). Si ACM no puede validar automáticamente un nombre de dominio, ACM le avisa de que debe realizar las acciones necesarias para validarlo manualmente. Para obtener más información, consulte [Cómo funciona la validación de dominio manual \(p. 25\)](#). Una vez que todos los nombres de dominio de un certificado están validados, ACM renueva el certificado.

Cómo funciona la validación automática de dominios

Para validar un dominio, ACM envía solicitudes HTTPS periódicas automatizada al mismo. Para los dominios que comienzan por `www.`, ACM también envía solicitudes HTTPS al dominio principal. Por ejemplo, si su dominio es `www.example.com`, ACM envía solicitudes periódicas a `www.example.com` y `example.com`. Para los dominios que no comienzan por `www.`, ACM también envía solicitudes de HTTPS a `www.doma.in`. ACM trata los nombres de dominio comodín (por ejemplo, `*.example.com`) de la misma manera que el dominio principal. Para ver ejemplos, consulte la siguiente tabla.

Note

Si algún intento de conexión HTTPS es correcto, ACM intenta renovar el certificado automáticamente.

Ejemplos de nombres de dominio que ACM utiliza para la validación automática

Nombre de dominio en el certificado	Nombres de dominio que ACM utiliza para la validación automática
example.com	example.com www.ejemplo.com
www.ejemplo.com	www.ejemplo.com example.com
*.example.com	example.com www.ejemplo.com
subdomain.example.com	subdomain.example.com www.subdomain.example.com
www.subdomain.example.com	www.subdomain.example.com subdomain.example.com
*.subdomain.example.com	subdomain.example.com www.subdomain.example.com

Si ACM establece correctamente una conexión HTTPS, ACM examina el certificado que es devuelto para garantizar que coincida con el que ACM está renovando. Si el certificado coincide con, ACM considera validado el nombre de dominio.

Cómo funciona la validación de dominio manual

Si ACM no puede validar automáticamente uno o más nombres de dominio en un certificado, ACM le avisa de que debe realizar las acciones necesarias para validar manualmente el dominio. Un dominio puede requerir la validación manual por las siguientes razones:

- ACM no puede establecer una conexión HTTPS con el dominio.
- El certificado que se devuelve en la respuesta a las solicitudes HTTPS de ACM no coincide con el que ACM está renovando.

Cuando han pasado 45 días desde el vencimiento de su certificado y uno o más nombres de dominio del certificado requieren validación manual, ACM le avisa de las siguientes formas:

Mediante correo electrónico

ACM le envía un correo electrónico de validación de dominio para cada nombre de dominio que requiera la validación manual. Para garantizar que recibe este correo electrónico, [configure el correo electrónico de su dominio \(p. 11\)](#). El correo electrónico contiene información sobre el certificado de ACM y el nombre de dominio que necesita para validar. El correo electrónico incluye un enlace que puede seguir para validar el nombre de dominio. Este enlace vence después de 72 horas. En caso necesario, puede utilizar la consola AWS Certificate Manager o la API ACM para solicitar que ACM reenvíe el correo electrónico de validación de dominio. Para obtener más información, consulte [Solicitar un correo electrónico de validación de dominio para renovación de certificado \(p. 28\)](#).

Mediante notificación en su AWS Personal Health Dashboard

ACM envía notificaciones a su [AWS Personal Health Dashboard](#) para hacerle saber que una renovación pendiente del certificado requiere una acción por su parte. ACM envía estas notificaciones cuando han pasado 45 días, 30 días, 15 días, 7 días, 3 días y 1 día desde el vencimiento del certificado y uno o más nombres de dominio del certificado requieren la validación manual. Estas notificaciones solo son informativas; para validar manualmente un nombre de dominio, debe seguir el enlace del correo electrónico de validación de dominio.

Configurar su dominio de validación automática

ACM intenta renovar automáticamente sus certificados SSL/TLS emitidos por Amazon antes de que caduquen para que no se requiera ninguna acción por su parte. Para renovar su certificado de forma automática, se debe cumplir lo siguiente:

- ACM debe ser capaz de establecer una conexión HTTPS con cada dominio del certificado.
- Por cada conexión, el certificado que se devuelve debe coincidir con el que ACM esté renovando.

Para aumentar la probabilidad de que ACM pueda renovar su certificado de forma automática, haga lo siguiente:

Utilice el certificado con un recurso de AWS

Asegúrese de que el certificado esté en uso con un recurso de AWS compatible. Para obtener información acerca de los recursos que admite AWS, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Configure el recurso para aceptar solicitudes HTTPS desde Internet

Asegúrese de que el recurso de AWS que tiene su certificado de ACM como el balanceador de carga Elastic Load Balancing o la distribución de CloudFront, esté configurado para aceptar solicitudes HTTPS desde Internet.

Configure DNS para dirigir su nombre de dominio al recurso que aloja su certificado de ACM

Asegúrese de que las solicitudes HTTPS para los nombres de dominio en el certificado se dirijan al recurso que tiene su certificado.

Comprobar el estado de renovación de un certificado

Utilice la consola de AWS Certificate Manager o la API de ACM para comprobar el estado de la [renovación administrada](#) (p. 24) de ACM de un certificado emitido por Amazon.

Temas

- [Comprobar el estado de la renovación de un certificado \(consola\)](#) (p. 27)
- [Comprobar el estado de la renovación de un certificado \(API de ACM\)](#) (p. 27)
- [Significado del estado de la renovación de un certificado](#) (p. 27)

Para comprobar el estado de la renovación de un certificado (consola)

1. Abra la consola de AWS Certificate Manager en <https://console.aws.amazon.com/acm/home>.
2. Amplíe el certificado cuyo estado de renovación está comprobando. En la sección Details busque el estado de renovación del certificado en Renewal Status. Para obtener más información acerca del significado del estado, consulte [Significado del estado de la renovación de un certificado](#) (p. 27). Si no ve la etiqueta Renewal Status, quiere decir que ACM no ha comenzado el proceso de renovación administrada de ese certificado.

Note

Es posible que pasen varias horas hasta que los cambios de estado del certificado aparezcan en la consola.

Para comprobar el estado de la renovación de un certificado (API de ACM)

Utilice la operación [DescribeCertificate](#) de la API de ACM. El siguiente ejemplo muestra cómo hacerlo con la [AWS Command Line Interface \(AWS CLI\)](#).

```
$ aws acm describe-certificate --certificate-arn arn:aws:acm:us-east-2:111122223333:certificate/97b4deb6-8983-4e39-918e-ef1378924e1e
```

En la respuesta, observe el valor del campo RenewalStatus. Para obtener más información acerca del significado del estado, consulte [Significado del estado de la renovación de un certificado](#) (p. 27). Si no ve el campo RenewalStatus, significa que ACM no ha comenzado el proceso de renovación administrado de este certificado.

Note

Es posible que pasen varias horas hasta que los cambios de estado del certificado se reflejen en el campo RenewalStatus.

Significado del estado de la renovación de un certificado

Existen cuatro estados de renovación de certificado.

Pending automatic renewal

ACM está intentando validar automáticamente los nombres de dominio en el certificado. No tiene que hacer nada.

Pending validation

ACM no pudo validar automáticamente uno o varios de los nombres de dominio del certificado. Debe tomar medidas para validar estos nombres de dominio. De lo contrario, el certificado no se renovará. Busque un correo electrónico de ACM y, a continuación, siga el enlace que incluye para validar su dominio.

Correcto

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

Failed

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 \(p. 15\)](#).

Solicitar un correo electrónico de validación de dominio para renovación de certificado

Una vez configuradas las direcciones de correo electrónico de contacto de su dominio (consulte [Configurar correo electrónico para su dominio \(p. 11\)](#)), puede utilizar la consola 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:

- El estado de renovación del certificado está pendiente de validación. Para obtener más información sobre cómo determinar el estado de renovación del certificado, consulte [Comprobar el estado de renovación de un certificado \(p. 27\)](#).
- No ha recibido o no puede encontrar el correo electrónico de validación de dominio original que ACM envió para la renovación del certificado.

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

1. Abra la consola de AWS Certificate Manager en <https://console.aws.amazon.com/acm/home>.
2. Seleccione la casilla de verificación situada al lado del certificado que requiere la validación manual del dominio. A continuación, elija Actions, Resend validation email.

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

Utilice la operación [ResendValidationEmail](#) 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:us-east-2:111122223333:certificate/97b4deb6-8983-4e39-918e-ef1378924e1e
--domain subdomain.example.com
--validation-domain example.com
```

Importar certificados a AWS Certificate Manager

Además de solicitar certificados SSL/TLS proporcionados por AWS Certificate Manager (ACM), puede importar certificados obtenidos fuera de AWS. Posiblemente necesite o quiera hacerlo porque ha obtenido un certificado de un tercer emisor, o porque los certificados proporcionados por ACM no cumplen ciertos requisitos.

Después de importar un certificado SSL/TLS obtenido fuera de AWS y asociarlo con servicios integrados con ACM, puede volver a importarlo y sus asociaciones se mantendrán.

Después de importar un certificado, puede utilizarlo con los [servicios de AWS integrados con ACM \(p. 4\)](#). Los certificados importados funcionan de la misma manera que los proporcionados por ACM, aunque con una excepción importante: ACM no ofrece [renovación administrada \(p. 24\)](#) para los certificados importados.

Important

El cliente es responsable de vigilar la fecha de vencimiento de los certificados importados y de renovarlos antes de que se venzan. Si importara un certificado nuevo con el mismo ARN que el del certificado vencido, el certificado nuevo sustituirá al antiguo. Además, ACM asociará el nuevo certificado con los mismos servicios y recursos que el antiguo.

Important

Le recomendamos que no asigne un certificado de ACM. Para obtener más información, consulte [Asignación de certificados \(p. 8\)](#) y [Solución de problemas de asignación de certificados \(p. 80\)](#).

Para renovar un certificado importado, puede obtener un nuevo certificado del emisor y, a continuación, importarlo a ACM, o puede [solicitar un nuevo certificado \(p. 15\)](#) de ACM.

En ACM, todos los certificados son recursos regionales, incluso los importados. Para utilizar el mismo certificado con balanceadores de carga de Elastic Load Balancing en diferentes regiones de AWS, debe importarlo a cada una de las regiones en las que desee utilizarlo. Para utilizar un certificado con Amazon CloudFront, debe importarlo a la región US East (N. Virginia). Para obtener más información, consulte [Regiones admitidas \(p. 4\)](#).

Para más información acerca de cómo importar certificados a ACM, consulte los siguientes temas. Si tiene problemas al importar un certificado, consulte [Solucionar problemas de importación de certificados \(p. 79\)](#).

Temas

- [Requisitos previos para la importación de certificados \(p. 29\)](#)
- [Importar un certificado \(p. 30\)](#)
- [Reimportar un certificado \(p. 31\)](#)

Requisitos previos para la importación de certificados

Para importar un certificado SSL/TLS en ACM, debe proporcionar el certificado y su clave privada. Si el certificado no está autofirmado, también debe proporcionar una cadena de certificados. Si el certificado es

autofirmado, si lo desea puede indicar una cadena. Además, el certificado debe satisfacer los siguientes criterios:

- El certificado debe contener una clave pública RSA de 1024 bits o 2048 bits. El algoritmo RSA utiliza dos claves relacionadas distintas pero relacionadas matemáticamente, una pública y otra privada. La clave pública se puede compartir con cualquiera. La clave privada debe mantenerse en secreto. Cuando compra un certificado SSL/TLS de una autoridad de certificación (CA), crea una solicitud de certificado que contiene su clave pública y que firma con su clave privada. Cuando cree un certificado autofirmado, también utilizará la clave privada.
- El certificado debe ser un certificado SSL/TLS X.509 de versión 3. No puede importar un certificado para firmar código, cifrar correos electrónicos ni ningún otro uso. El certificado debe contener una clave pública RSA, el nombre de dominio completo cualificado (FQDN) para su sitio web e información sobre la autoridad expedidora. El certificado puede ser autofirmado por la clave privada relacionada con su clave pública o por la clave privada de una CA emisora. Puede instalar un certificado SSL/TLS en su servidor web para permitir conexiones seguras entre su servidor y un navegador web.
- El 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.
- La clave privada no debe estar cifrada. No puede importar una clave privada que esté protegida por una contraseña o frase de contraseña.
- El certificado, la clave privada y la cadena de certificados deben tener todos codificación PEM. PEM son las siglas de correo de privacidad mejorada, pero nunca se ha adoptado ampliamente como estándar de correo en Internet. En lugar de ello, el formato PEM se utiliza a menudo para representar un certificado o una solicitud de certificado. Dispone de codificación base64 y se sitúa entre un encabezado `-----BEGIN CERTIFICATE-----` y un pie de página `-----END CERTIFICATE-----`.

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

Importar un certificado

Puede importar un certificado a ACM utilizando la Consola de administración de AWS, el AWS CLI o la API de ACM. Los siguientes temas le muestran cómo utilizar la Consola de administración de AWS y el AWS CLI.

Temas

- [Importar mediante la consola \(p. 30\)](#)
- [Importe utilizando el AWS CLI \(p. 31\)](#)

Importar mediante la consola

El siguiente ejemplo muestra cómo importar un certificado con la Consola de administración de AWS.

1. Abra la consola de ACM en <https://console.aws.amazon.com/acm/home>.
2. Seleccione Import a certificate.
3. Haga lo siguiente:
 - a. En el Certificate body, pegue el certificado codificado en PEM para importar.
 - b. En Certificate private key, pegue la clave privada codificada en PEM y sin cifrar que coincida con la clave pública del certificado.

- c. (Opcional) En Certificate chain, pegue la cadena de certificados codificada en PEM.
4. Seleccione Review and import.
5. Revise la información sobre su certificado y, a continuación, seleccione Import.

Importe utilizando el AWS CLI

El siguiente ejemplo muestra cómo importar un certificado con [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 file://Certificate.pem
                             --certificate-chain file://CertificateChain.pem
                             --private-key file://PrivateKey.pem
```

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

Reimportar un certificado

Si ha importado un certificado y lo ha asociado a otros servicios de AWS, puede reimportar dicho certificado antes de que venza mientras preserva las asociaciones del servicio de AWS del certificado original. Para obtener más información acerca de los servicios de AWS integrados con ACM, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).

Temas

- [Reimportar utilizando la consola \(p. 31\)](#)
- [Reimportar utilizando el AWS CLI \(p. 32\)](#)

Reimportar utilizando la consola

El siguiente ejemplo muestra cómo reimportar un certificado con la Consola de administración de AWS.

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) EnCertificate chain, pegue la cadena de certificados codificada en PEM. La cadena de certificados incluye el certificado de entidad final, cero o más certificados para todas las autoridades intermedias emisoras de certificación y el certificado raíz.
7. Seleccione Review and import.
8. Revise la información acerca de su certificado. Si no hay errores, elija Reimport.

Reimportar utilizando el AWS CLI

El siguiente ejemplo muestra cómo reimportar un certificado con [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`.
- 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 file://Certificate.pem
                             --certificate-chain file://CertificateChain.pem
                             --private-key file://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.

Etiquetar certificados de AWS Certificate Manager

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

También puede crear etiquetas personalizadas que se adapten mejor a sus necesidades. Por ejemplo, puede proporcionar una etiqueta `Environment = Prod` o `Environment = Beta` a varios certificados de ACM para identificar el entorno para el que está pensado cada certificado. 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 que utilice para su sitio web `example.com`.

Temas

- [Restricciones de las etiquetas \(p. 33\)](#)
- [Gestión de etiquetas \(p. 34\)](#)

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 el límite 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 su uso en los [Grupos de recursos y el Editor de etiquetas](#) de Consola de administración de AWS.

Gestión 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.

Administración de etiquetas (Consola)

Puede utilizar la Consola de administración de AWS para añadir, eliminar o editar etiquetas. También puede mostrar etiquetas en columnas.

Adición de una etiqueta (Consola)

Utilice el siguiente procedimiento para añadir etiquetas utilizando la consola de ACM.

Para añadir una etiqueta a un certificado (consola)

1. Inicie sesión en la Consola de administración de AWS 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.

Eliminación de una etiqueta (Consola)

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

Para eliminar una etiqueta (consola)

1. Inicie sesión en la Consola de administración de AWS 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.
5. Elija la X situada al lado de la etiqueta que desea eliminar.
6. Seleccione Save.

Edición de una etiqueta (Consola)

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

Para editar una etiqueta (consola)


1. Inicie sesión en la Consola de administración de AWS 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.
5. Modifique la clave o el valor de la etiqueta que desea cambiar.

6. Seleccione Save.

Visualización de etiquetas en columnas (Consola)

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 Consola de administración de AWS; y abra la consola de AWS Certificate Manager en <https://console.aws.amazon.com/acm/home>.
2. Seleccione las etiquetas que desea mostrar en columnas seleccionando el icono del engranaje  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.

Administración de etiquetas (AWS Command Line Interface)

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

- [add-tags-to-certificate](#)
- [list-tags-for-certificate](#)
- [remove-tags-from-certificate](#)

Administración de etiquetas (API de AWS Certificate Manager)

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

- [AddTagsToCertificate](#)
- [ListTagsForCertificate](#)
- [RemoveTagsFromCertificate](#)

Autenticación y control de acceso

Obtener acceso a ACM requiere credenciales que puede utilizar AWS para autenticar las solicitudes. Las credenciales deben tener permisos para acceder a los recursos AWS como certificados de ACM. En las secciones siguientes se incluyen detalles sobre cómo puede utilizar [AWS Identity and Access Management \(IAM\)](#) y ACM para ayudar a proteger sus recursos controlando quién puede obtener acceso a los mismos.

Temas

- [Autenticación \(p. 36\)](#)
- [Control de acceso \(p. 37\)](#)

Autenticación

Puede tener acceso a AWS como cualquiera de los siguientes tipos de identidades:

- **Usuario raíz de la cuenta de AWS:** Cuando crea por primera vez una cuenta de AWS, comienza únicamente por una identidad de inicio de sesión único que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se obtiene acceso a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, siga las [prácticas recomendadas para utilizar el usuario raíz únicamente cuando cree su primer usuario de IAM](#). A continuación, guarde en un lugar seguro las credenciales del usuario raíz y utilícelas solo para realizar unas cuantas tareas de administración de servicios y cuentas.
- **Usuario de IAM:** un [usuario de IAM](#) es una identidad dentro de su cuenta de AWS que tiene permisos personalizados específicos (por ejemplo, permisos para crear a directory in ACM). Puede utilizar un nombre de usuario de IAM y una contraseña para iniciar sesión en páginas web seguras de AWS, como la de [Consola de administración de AWS](#), los [foros de discusión de AWS](#) o el [AWS Support Center](#).

Además de un nombre de usuario y una contraseña, también puede generar [claves de acceso](#) para cada usuario. Puede utilizar estas claves cuando obtenga acceso a los servicios de AWS mediante programación, ya sea a través de [uno de los varios SDK](#) o mediante la [AWS Command Line Interface \(CLI\)](#). El SDK y las herramientas de CLI usan claves de acceso para firmar criptográficamente su solicitud. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. ACM admite Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre las solicitudes de autenticación, consulte [Signature Version 4 Signing Process](#) en la AWS General Reference.

- **Rol de IAM:** An [IAM role](#) is an IAM identity that you can create in your account that has specific permissions. It is similar to an IAM user, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:
- **Acceso de usuario federado:** Instead of creating an IAM user, you can use existing user identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an [identity](#)

[provider](#). For more information about federated users, see [Federated Users and Roles](#) in the Guía del usuario de IAM.

- **Acceso al servicio de AWS:** You can use an IAM role in your account to grant an AWS service permissions to access your account's resources. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see [Creating a Role to Delegate Permissions to an AWS Service](#) in the Guía del usuario de IAM.
- **Aplicaciones que se ejecutan en Amazon EC2:** You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances](#) in the Guía del usuario de IAM.

Control de acceso

Puede tener credenciales válidas para autenticar las solicitudes, pero a menos que tenga permisos no podrá crear ni obtener acceso a los recursos de ACM. Por ejemplo, debe disponer de permiso para crear, importar, recuperar o enumerar los certificados.

Los siguientes temas describen cómo administrar los permisos. Le recomendamos que lea primero la información general.

- [Introducción a la administración de acceso a sus recursos de ACM \(p. 37\)](#)
- [Políticas administradas por AWS \(p. 39\)](#)
- [Políticas administradas por el cliente \(p. 40\)](#)
- [Políticas insertadas \(p. 40\)](#)
- [Permisos API de ACM: Referencia de recursos y acciones \(p. 43\)](#)

Introducción a la administración de acceso a sus recursos de ACM

Todos los recursos de AWS pertenecen a una cuenta de AWS y los permisos para crear o acceder a los recursos se definen en las políticas de permisos de dicha cuenta. Un administrador de la cuenta puede asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y roles). Algunos servicios (incluido ACM) también permiten adjuntar políticas de permisos a los recursos.

Note

Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte [Creating an Admin User and Group](#) en la Guía del usuario de IAM.

Al gestionar permisos, puede decidir quién obtiene los permisos, los recursos para los que obtienen los permisos y las acciones específicas permitidas.

Temas

- [Recursos y operaciones de ACM \(p. 38\)](#)
- [Titularidad de los recursos \(p. 38\)](#)
- [Administración de acceso a certificados de ACM \(p. 38\)](#)

Recursos y operaciones de ACM

En ACM, el recurso principal es un certificado. Los certificados tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente lista.

- Certificado de ACM

Formato de ARN:

```
arn:aws:acm:AWS region:AWS account ID:certificate/Certificate ID
```

Ejemplo de ARN:

```
arn:aws:acm:us-west-2:123456789012:certificate/12345678-12ab-34cd-56ef-12345678
```

Titularidad de los recursos

El propietario del recurso es la cuenta de AWS que ha creado un recurso. Es decir, el propietario del recurso es la cuenta de AWS de la entidad principal que autentica la solicitud que ha creado el recurso. (Una entidad puede ser un usuario raíz de la cuenta de AWS un usuario de IAM o un rol de IAM.) Los siguientes ejemplos ilustran cómo funciona.

- Si utiliza las credenciales de un usuario raíz de la cuenta de AWS para crear un certificado de ACM, su cuenta de AWS es la propietaria del certificado.
- Si crea un usuario de AWS en su cuenta de IAM, puede conceder a dicho usuario permiso para crear un certificado de ACM. Sin embargo, la propietaria del certificado será la cuenta a la que pertenece el usuario.
- Si crea un rol de AWS en su cuenta de IAM y le concede permiso para crear un certificado de ACM, cualquiera que pueda asumir el rol puede crear un certificado. Sin embargo, la propietaria del certificado es la cuenta a la que pertenece ese rol.

Administración de acceso a certificados de ACM

Una política de permisos describe quién tiene acceso a qué. En esta sección se explican las opciones disponibles para crear políticas de permisos.

Note

En esta sección se explica cómo se utiliza IAM en el contexto de ACM. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte la [Guía del usuario de IAM](#). Para obtener más información sobre la sintaxis y descripciones de la política de IAM, consulte [AWS IAM Policy Reference](#)

Puede utilizar IAM para crear políticas que apliquen permisos a usuarios, grupos y roles de IAM. Estas políticas se denominan políticas basadas en identidades. IAM ofrece los siguientes tipos de políticas basadas en identidades:

- Políticas administradas por AWS: las políticas creadas y administradas por AWS. Estas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su cuenta de AWS.

- Políticas administradas por clientes: políticas que crea y administra en su cuenta de AWS y que se pueden adjuntar a varios usuarios, grupos y roles. Tiene un control más preciso cuando se utilizan políticas administradas por el cliente que cuando se utilizan políticas administradas por AWS.
- Políticas insertadas: políticas que crea y administra, y que integra directamente en un único usuario, grupo o rol.

Otros servicios, como Amazon S3, admiten también políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de Amazon S3 para administrar los permisos de acceso a dicho bucket. ACM no admite políticas basadas en recursos.

Políticas administradas por AWS

Las políticas administradas por AWS son políticas independientes basadas en la identidad que usted puede adjuntar a varios usuarios, grupos y funciones de su cuenta AWS. Las políticas administradas por AWS son creadas y administradas por AWS. Las siguientes políticas administradas por AWS están disponibles para ACM. Para obtener más información acerca de cómo adjuntar políticas administradas a un usuario, grupo o función, consulte [Trabajar con políticas administradas](#) en [Guía del usuario de IAM](#).

Para utilizar una política administrada de AWS, un usuario con privilegios administrativos debe adjuntar la política a un usuario, función o grupo. Para obtener más información acerca de cómo adjuntar las políticas administradas por AWS, consulte [Attaching Managed Policies](#) en [Guía del usuario de IAM](#).

Temas

- [AWSCertificateManagerReadOnly](#) (p. 39)
- [AWSCertificateManagerFullAccess](#) (p. 39)

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"
    ],
    "Resource": "*"
  }
}
```

Para ver esta política administrada de 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": "*"
  }]
}
```

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

Políticas administradas por el cliente

Las políticas administradas son políticas independientes basadas en la identidad que usted crea y que puede adjuntar a varios usuarios, grupos o funciones de su cuenta de AWS. Puede administrar y crear políticas con la Consola de administración de AWS, la AWS Command Line Interface (AWS CLI) o la API de IAM. Para obtener más información acerca de cómo utilizar la consola para administrar las políticas administradas por el cliente, consulte los siguientes temas en [Guía del usuario de IAM](#).

- [Attaching Managed Policies](#)
- [Detaching Managed Policies](#)
- [Creating Customer Managed Policies](#)
- [Editing Customer Managed Policies](#)
- [Editing Customer Managed Policies](#)
- [Deleting Versions of Customer Managed Policies](#)
- [Eliminación de las políticas administradas por el cliente](#)

Para obtener más información sobre el uso de las API, consulte [Working with Managed Policies Using the AWS CLI or the IAM API](#)

Políticas insertadas

Las políticas insertadas son aquellas que se crean y administran, y se integran directamente en un único usuario, grupo o rol. Los siguientes ejemplos de políticas muestran cómo asignar permisos para realizar acciones de ACM. Para obtener más información acerca de cómo asociar políticas insertadas, consulte [Working with Inline Policies](#) en la [Guía del usuario de IAM](#). Utilice la Consola de administración de AWS, la AWS Command Line Interface (AWS CLI) o la API de IAM para crear e integrar políticas insertadas.

Temas

- [Creación de una lista de certificados \(p. 41\)](#)
- [Recuperación de un certificado \(p. 41\)](#)
- [Importación de un certificado \(p. 41\)](#)
- [Borrar un certificado \(p. 41\)](#)
- [Acceso de solo lectura a ACM \(p. 42\)](#)
- [Acceso completo a ACM \(p. 42\)](#)
- [Acceso de administrador a todos los recursos de AWS \(p. 43\)](#)

Creación de una lista de certificados

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

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

Note

Se necesita este permiso para que los certificados de ACM aparezcan en las consolas de Elastic Load Balancing y CloudFront.

Recuperación de un certificado

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

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "acm:GetCertificate",
    "Resource": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
  }
}
```

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:ap-northeast-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
  }
}
```

Borrar un certificado

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

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "acm:DeleteCertificate",
    "Resource": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
  }
}
```

Acceso de solo lectura a ACM

La siguiente política le permite un usuario describir e incluir en la lista un certificado de ACM y recuperar dicho certificado y la cadena de certificados.

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

Note

Esta política está disponible como política administrada de AWS en la Consola de administración de AWS. Para obtener más información, consulte [AWSCertificateManagerReadOnly](#) (p. 39). Para ver la política administrada en la consola, visite <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly>.

Acceso completo a ACM

La siguiente política le permite a un usuario realizar cualquier acción de ACM.

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

Note

Esta política está disponible como política administrada de AWS en la Consola de administración de AWS. Para obtener más información, consulte [AWSCertificateManagerFullAccess](#) (p. 39). Para ver la política administrada en la consola, visite <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess>.

Acceso de administrador a todos los recursos de AWS

La siguiente política le permite a un usuario realizar cualquier acción en cualquier recurso de AWS.

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

Note

Esta política está disponible como política administrada de AWS en la Consola de administración de AWS. Para ver la política administrada en la consola, visite <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AdministratorAccess>.

Permisos API de ACM: Referencia de recursos y acciones

A la hora de configurar el [control de acceso \(p. 37\)](#) y de escribir una política de permisos que pueda adjuntar a una identidad de IAM (políticas basadas en identidad), puede utilizar la siguiente tabla lista como referencia. La primera columna de la tabla enumera cada operación de la API de ACM. 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 [Available Keys](#) 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 API de ACM

Operaciones de la API de ACM	Permisos necesarios (acciones de la API)	Recursos
AddTagsToCertificate	<code>acm:AddTagsToCertificate</code>	<code>arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID</code>
DeleteCertificate	<code>acm:DeleteCertificate</code>	<code>arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID</code>
DescribeCertificate	<code>acm:DescribeCertificate</code>	<code>arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID</code>
GetCertificate	<code>acm:GetCertificate</code>	<code>arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID</code>
ImportCertificate	<code>acm:ImportCertificate</code>	<code>arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID</code>

Operaciones de la API de ACM	Permisos necesarios (acciones de la API)	Recursos
ListCertificates	acm:ListCertificates	arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID
ListTagsForCertificate	acm:ListTagsForCertificate	arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID
RemoveTagsFromCertificate	acm:RemoveTagsFromCertificate	arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID
RequestCertificate	acm:RequestCertificate	arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID
ResendValidationEmail	acm:ResendValidationEmail	arn:aws:acm:AWS_region:AWS_account_ID:certificate_ID

Uso de AWS CloudTrail

Puede utilizar CloudTrail para registrar las llamadas a la API que realiza AWS Certificate Manager y los servicios integrados con ACM tal y como se explica en los temas siguientes.

Temas

- [Registro de llamadas a la API de AWS Certificate Manager con AWS CloudTrail \(p. 45\)](#)
- [Registro de llamadas a la API relacionadas con ACM \(p. 53\)](#)

Registro de llamadas a la API de AWS Certificate Manager con AWS CloudTrail

AWS Certificate Manager (ACM) se integra con AWS CloudTrail, un servicio que captura las llamadas a la API, proporciona los archivos de registro a un bucket Amazon Simple Storage Service (Amazon S3) que especifique y mantiene el historial de llamadas a las API. CloudTrail captura las llamadas a la API desde la consola de AWS Certificate Manager, la CLI o desde el código. Con la información recopilada por CloudTrail, puede identificar la solicitud que se realizó a ACM, la dirección IP desde la que se realizó la solicitud, quién la realizó y cuándo, etcétera.

Para obtener más información sobre CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la [Guía del usuario de AWS CloudTrail](#).

Cuando habilita el registro de CloudTrail en su cuenta de AWS, las llamadas a la API realizadas a acciones de ACM se registran en archivos de registro CloudTrail. Los registros ACM se escriben con otros registros de servicio AWS. CloudTrail determina cuándo crear y escribir en un nuevo archivo de registro en función del período de tiempo y del tamaño del archivo.

Se admiten las siguientes acciones ACM:

- [AddTagsToCertificate](#)
- [DeleteCertificate](#)
- [DescribeCertificate](#)
- [GetCertificate](#)
- [ImportCertificate](#)
- [ListCertificates](#)
- [ListTagsForCertificate](#)
- [RemoveTagsFromCertificate](#)
- [RequestCertificate](#)
- [ResendValidationEmail](#)

Cada entrada de log contiene información sobre quién generó la solicitud. La información de identidad del usuario que figura en la entrada de registro le ayudará a determinar si la solicitud se hizo con credenciales de usuario IAM o raíz, con credenciales de seguridad temporal para un rol o un usuario federado, o por otro servicio AWS. Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#).

Puede almacenar los archivos de log en su bucket todo el tiempo que desee, y también puede definir reglas de ciclo de vida de Amazon S3 para archivar o eliminar archivos de log automáticamente. De forma predeterminada, los archivos log se cifran mediante el cifrado del servidor (SSE) de Amazon S3.

Puede hacer que CloudTrail publique notificaciones de Amazon SNS cuando se entreguen los nuevos archivos de registro, si desea realizar una acción rápida al recibir un registro. Para obtener más información, consulte [Configuring Amazon SNS Notifications for CloudTrail](#) en la Guía del usuario AWS CloudTrail.

También puede agregar archivos de registro de AWS Certificate Manager de varias regiones de AWS y de varias cuentas de AWS en un solo bucket de Amazon S3. Para obtener más información, consulte [Receiving CloudTrail Log Files from Multiple Regions](#) y [Receiving CloudTrail Log Files from Multiple Accounts](#).

Los archivos de registro de CloudTrail contienen una o varias entradas de registro, donde en cada entrada se enumeran varios eventos con formato JSON. Una entrada de registro representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Las entradas de registro no se muestran en ningún orden concreto. Es decir, no representan un rastro ordenado de las llamadas a API públicas. Para obtener más información acerca de los campos que componen una entrada de registro, consulte la [referencia de los eventos de CloudTrail](#).

Para ejemplos de posibles entradas ACM CloudTrail, consulte los siguientes temas.

Temas

- [Adición de etiquetas a un certificado \(p. 46\)](#)
- [Borrar un certificado \(p. 47\)](#)
- [Descripción de un certificado \(p. 47\)](#)
- [Recuperación de un certificado \(p. 48\)](#)
- [Importar un certificado \(p. 49\)](#)
- [Creación de una lista de certificados \(p. 50\)](#)
- [Visualización de etiquetas de un certificado \(p. 51\)](#)
- [Eliminar etiquetas de un certificado \(p. 51\)](#)
- [Solicitud de un certificado \(p. 52\)](#)
- [Reenviando correo electrónico de validación \(p. 53\)](#)

Adición de etiquetas a un certificado

El siguiente ejemplo de CloudTrail 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/12345678-1234-1234-1234-123456789012"
    },
    responseElements: null,
    requestID: "ffd7ddb1b-fbfe-11e5-ba7b-5f4e988901f9",
    eventID: "4e7b10bb-7010-4e60-8376-0cac3bc860a5",
    eventType: "AwsApiCall",
    recipientAccountId: "123456789012"
  }
}
```

Borrar un certificado

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [DeleteCertificate](#).

```
{
  "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/12345678-1234-1234-1234-123456789012"
    },
    "responseElements": null,
    "requestID": "6b0f5bb9-ec9c-11e5-a28b-51e7e3169e0f",
    "eventID": "08f18f8a-a827-4924-b864-afaf98517793",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }
}
```

Descripción de un certificado

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [DescribeCertificate](#).

Note

El log de CloudTrail de la `DescribeCertificate` acción no muestra información sobre el certificado de ACM que especifica. Puede consultar información acerca del certificado en la consola, la AWS Command Line Interface o la API [DescribeCertificate](#).

```
{
  "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/12345678-1234-1234-1234-123456789012"
    },
    "responseElements": null,
    "requestID": "74b91d83-ec9c-11e5-ac34-d1e4dfe1a11b",
    "eventID": "7779b6da-75c2-4994-b8c1-af3ad47b518a",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }]
}
```

Recuperación de un certificado

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [GetCertificate](#).

```
{
  "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"
  }
}
```

Importar un certificado

El siguiente ejemplo muestra la entrada de registro de CloudTrail que registra una llamada a la operación de API [ImportCertificate](#) 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/6ae06649-
ea82-4b58-90ee-dc05870d7e99"
},
"requestID": "cf1f3db7-8a4b-11e6-88c8-196af94bb7be",
"eventID": "fb443118-bfaa-4c90-95c1-beef21e07f8e",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

Creación de una lista de certificados

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [ListCertificates](#).

Note

El registro de CloudTrail de la acción `ListCertificates` no muestra sus certificados de ACM. Puede ver la lista de certificados mediante la utilización de la consola, el AWS Command Line Interface o la API [ListCertificates](#).

```
{
  "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": "cdfel051-88aa-4aa3-8c33-a325270bff21",  
    "eventType": "AwsApiCall",  
    "recipientAccountId": "123456789012"  
  }  
}
```

Visualización de etiquetas de un certificado

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [ListTagsForCertificate](#).

Note

El log de CloudTrail de la acción `ListTagsForCertificate` no muestra las etiquetas. Puede ver la lista de etiquetas mediante la consola, la AWS Command Line Interface o la API [ListTagsForCertificate](#).

```
{  
  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"  
  }  
}]  
}
```

Eliminar etiquetas de un certificado

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [RemoveTagsFromCertificate](#).

```
{  
  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

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [RequestCertificate](#).

```
{
  "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"
    }
  ]
}
```

Reenviando correo electrónico de validación

El siguiente ejemplo de CloudTrail muestra los resultados de una llamada a la API [ResendValidationEmail](#).

```
{
  "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"
  }
]
```

Registro de llamadas a la API relacionadas con ACM

Puede utilizar CloudTrail para auditar las llamadas a la API realizadas por los servicios que se integran con ACM. Para obtener más información en relación con el uso de CloudTrail, consulte la [Guía del usuario de AWS CloudTrail](#). Los siguientes ejemplos muestran los tipos de registros que pueden ser generados en función de los recursos de AWS en los que aprovisiona el certificado de ACM.

Temas

- [Creación de un balanceador de carga \(p. 54\)](#)
- [Registrar una instancia Amazon EC2 con un balanceador de carga \(p. 54\)](#)

- [Cifrando una clave privada \(p. 55\)](#)
- [Descifrando una clave privada \(p. 56\)](#)

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 utilizando un certificado 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"
}
```

Registrar una instancia Amazon EC2 con un balanceador de carga

Cuando aprovisiona su sitio web o aplicación en una instancia Amazon Elastic Compute Cloud (Amazon EC2), el balanceador de carga debe ser consciente de dicha instancia. Esto puede lograrse a través de la consola de Elastic Load Balancing o la AWS Command Line Interface. El siguiente ejemplo muestra una llamada a `RegisterInstancesWithLoadBalancer` para un balanceador de carga denominado `LinuxTest` en la cuenta de AWS 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 `Encrypt` llamada 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 asociado a un certificado de ACM. El descifrado se realiza en AWS y la clave descifrada nunca deja 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"
  }
}
```

Uso de la API de ACM

Puede utilizar la API de AWS Certificate Manager para interactuar con el servicio mediante programación enviando solicitudes HTTP. Para obtener más información, consulte [Referencia de la API de AWS Certificate Manager](#).

Además de la API de web (o API de HTTP), puede utilizar los SDK y 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 \(p. 58\)](#)
- [Borrar un certificado \(p. 60\)](#)
- [Descripción de un certificado \(p. 61\)](#)
- [Recuperación de un certificado y una cadena de certificados \(p. 63\)](#)
- [Importación de un certificado \(p. 65\)](#)
- [Creación de una lista de certificados \(p. 67\)](#)
- [Listado de etiquetas de certificados \(p. 68\)](#)
- [Eliminación de etiquetas de un certificado \(p. 70\)](#)
- [Solicitud de un certificado \(p. 71\)](#)
- [Reenviando correo electrónico de validación \(p. 73\)](#)

Adición de etiquetas a un certificado

El siguiente ejemplo muestra cómo utilizar la función [AddTagsToCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.AddTagsToCertificateRequest;
import com.amazonaws.services.certificatemanager.model.AddTagsToCertificateResult;
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.services.certificatemanager.model.TooManyTagsException;

import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSSStaticCredentialsProvider;
import com.amazonaws.regions.Regions;

import java.util.ArrayList;
```

```
/**
 * This sample demonstrates how to use the AddTagsToCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameters:
 *   CertificateArn - The ARN of the certificate to which to add one or more tags.
 *   Tags - An array of Tag objects to add.
 */

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 tags.
        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 and specify the ARN of the certificate.
        AddTagsToCertificateRequest req = new AddTagsToCertificateRequest();

        req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");
        req.setTags(tags);

        // Add tags to the specified certificate.
        AddTagsToCertificateResult result = null;
        try {
            result = client.addTagsToCertificate(req);
        }
        catch(InvalidArnException ex)
        {
            throw ex;
        }
        catch(InvalidTagException ex)
        {
            throw ex;
        }
    }
}
```



```

        catch(ResourceNotFoundException ex)
        {
            throw ex;
        }
        catch(TooManyTagsException ex)
        {
            throw ex;
        }

        // Display the result.
        System.out.println(result);
    }
}

```

Borrar un certificado

El siguiente ejemplo muestra cómo utilizar la función [DeleteCertificate](#). Si lo realiza correctamente, la función 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.AWSSStaticCredentialsProvider;
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

El siguiente ejemplo 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,  
  }  
}
```

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.AWSSStaticCredentialsProvider;  
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.AWSSStaticCredentialsProvider;
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:
 * CertificateArn - 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 AWSSStaticCredentialsProvider(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.AWSSStaticCredentialsProvider;
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
  }
  ]
}
```

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.AWSSStaticCredentialsProvider;
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 AWSSStaticCredentialsProvider(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.AWSSStaticCredentialsProvider;
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.AWSSStaticCredentialsProvider;
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 AWSSStaticCredentialsProvider(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}
```

Reenviando 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.AWSSStaticCredentialsProvider;
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.

```
{}
```

Seguridad de la clave privada de ACM

Al [solicitar un certificado \(p. 15\)](#), AWS Certificate Manager (ACM) genera un par de claves pública/privada. Sin embargo, en el caso de [certificados importados \(p. 29\)](#), 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 utiliza AWS Key Management Service (AWS KMS) para ayudar a protegerla. El proceso ocurre de la siguiente manera:

1. La primera vez que solicita o importa un certificado a una región de AWS, ACM crea una clave maestra de cliente (CMK) administrada por AWS en AWS KMS con el alias `aws/acm`. Esta CMK es única para cada cuenta y región de AWS.
2. ACM utiliza esta CMK para cifrar la clave privada del certificado. ACM almacena solo una versión cifrada de la clave privada (ACM no almacena la clave privada como texto no cifrado). ACM utiliza la misma CMK para cifrar las claves privadas de todos los certificados en una cuenta de AWS y una región de AWS específicos.
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 crea implícitamente una concesión en AWS KMS que le permite al servicio utilizar la CMK en AWS KMS para descifrar la clave privada del certificado. Para obtener más información acerca de concesiones, consulte [Using Grants](#) en la AWS Key Management Service Developer Guide. Para obtener más información acerca de servicios compatibles con ACM, consulte [Servicios integrados con AWS Certificate Manager \(p. 4\)](#).
4. Los servicios integrados utilizan CMK en AWS 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 CMK en AWS KMS para descifrar la clave privada del certificado.

Solución de problemas

Consulte los siguientes temas si tienes problemas al utilizar AWS Certificate Manager.

Temas

- [Solución de problemas con la autorización de la autoridad de certificación \(CAA\) \(p. 76\)](#)
- [Solución de problemas del correo electrónico \(p. 76\)](#)
- [Solucionar problemas de importación de certificados \(p. 79\)](#)
- [Solución de problemas de asignación de certificados \(p. 80\)](#)
- [Solucionar problemas de solicitud de certificados \(p. 80\)](#)
- [Solución de problemas de renovación administrada de certificados \(p. 82\)](#)
- [Solución de problemas de validación de certificados \(p. 82\)](#)
- [Solución de problemas de dominios .IO \(p. 83\)](#)

Solución de problemas con la autorización de la autoridad de certificación (CAA)

Puede utilizar registros DNS de CAA para especificar que la autoridad 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, compruebe los registros DNS de CAA. Si este mensaje de error aparece después de que su solicitud de un certificado de ACM se haya validado correctamente, debe actualizar los registros de CAA y volver solicitar un certificado. El campo value de al menos uno de los registros de CAA debe contener uno de los siguientes nombres de dominio:

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

Si no desea que ACM realice la comprobación de CAA, no configure ningún registro de CAA para su dominio o deje en blanco sus registros de CAA. Para obtener más información sobre cómo crear un registro de CAA, consulte [\(Opcional\) Configuración de un registro de CAA \(p. 13\)](#).

Solución de problemas del correo electrónico

Consulte los siguientes temas si tiene problemas con el correo electrónico de validación.

Temas

- [No he recibido el correo electrónico de validación \(p. 77\)](#)
- [Correo electrónico enviado al subdominio \(p. 78\)](#)
- [Información de contacto oculta \(p. 78\)](#)

- [Renovación de certificados \(p. 79\)](#)
- [Limitación controlada de WHOIS \(p. 79\)](#)

No he recibido el correo electrónico de validación

Cuando solicita un certificado de validación de dominio ACM, se envía un correo electrónico a tres direcciones de contacto especificadas en WHOIS y a cinco direcciones administrativas comunes. Para obtener más información, consulte [Validar propiedad de dominio \(p. 16\)](#). 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 cuenta de AWS a menos que el propietario también se enumere como contacto de dominio en WHOIS. Revise la lista de direcciones de correo electrónico que se muestran en la consola ACM (o devueltas de la CLI o la API) 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, los contactos del registrador de dominios, técnicos y administrativos de WHOIS pueden no estar disponibles públicamente y, por tanto, AWS no puede llegar a 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 utilizar una dirección de privacidad, como las que se ofrecen a través de WhoisGuard o PrivacyGuard.

Para los dominios comprados a partir de la protección de la privacidad Route 53, la protección de privacidad está activada por defecto y su dirección de correo electrónico se asigna a la dirección de correo electrónico `whoisprivacyservice.org` o `contact.gandi.net`. 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 compra con Route 53 se habilitará aunque elija que su información de contacto sea pública. Por ejemplo, Route 53 no puede deshabilitar mediante programación la protección de privacidad para el dominio de nivel superior .ca. 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 acerca de la configuración del correo electrónico para su dominio, consulte la documentación de su proveedor de servicios de correo electrónico y siga las instrucciones de [Configurar correo electrónico para su dominio \(p. 11\)](#). Si está utilizando Amazon WorkMail, consulte [Trabajar con usuarios](#) en la Guía del administrador de Amazon WorkMail.

Después de hacer disponibles 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 Consola de administración de AWS. 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 del asistente Request a Certificate de ACM. Las direcciones de correo electrónico listadas son aquellas a las que se ha enviado el correo electrónico.

Póngase en contacto con el Centro de soporte

Si, después de revisar las instrucciones anteriores, todavía no recibe el correo electrónico de validación del dominio, visite el [Centro AWS Support](#) y cree un caso. 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 comprueba 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 [Validar propiedad de dominio \(p. 16\)](#). 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. Para una discusión detallada de cómo configurar su correo electrónico y de cómo funciona ACM con DNS y la base de datos de WHOIS, consulte [Configurar correo electrónico para su dominio \(p. 11\)](#).

En lugar de utilizar la consola, puede usar la opción `ValidationDomain` de la API [RequestCertificate](#) o el comando `request-certificate` de la AWS CLI 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 una búsqueda del registro 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 que se ha completado su configuración de WHOIS, y siempre y cuando su solicitud de certificado no haya agotado el tiempo de espera, puede decidir volver a enviar 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 ahora pública.

Renovación 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 utilizando 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 ahora públicas.

Limitación controlada de WHOIS

A veces ACM no puede ponerse en contacto con el servidor de WHOIS ni siquiera después de haber enviado varias solicitudes al 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 [AWS Support](#) para que le ayuden a encontrar la solución.

Solucionar problemas de importación de certificados

Antes de importar un certificado a ACM, debe asegurarse de que el certificado, la clave privada y la cadena de certificados estén codificados en PEM. También debe asegurarse de que la clave privada no esté cifrada. Los certificados deben ser similares a los siguientes ejemplos.

Example Certificado codificado en PEM

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

Example Clave privada sin cifrar y codificada en PEM

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

Example Cadena de certificados codificada en PEM

Una cadena de certificados contiene uno o más certificados. El siguiente ejemplo contiene tres certificados, pero una cadena de certificados podría contener más o menos.

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

-----END CERTIFICATE-----

Solución de problemas de asignación de certificados

Para renovar un certificado, ACM genera un nuevo par de claves pública y privada. Si su aplicación utiliza [Asignación de certificados](#) (p. 8) (también conocido como asignación SSL) para asignar un certificado de ACM, es posible que la aplicación no se pueda conectar al dominio una vez que AWS haya renovado el certificado. Por este motivo, le 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](#) (p. 29) y, a continuación, asigne su aplicación al certificado importado. ACM no proporciona una renovación administrada de los certificados importados.
- Asigne su aplicación a un certificado raíz [de Amazon](#).

Solucionar problemas de solicitud de certificados

Consulte los siguientes temas si tiene problemas al solicitar un certificado de ACM.

Temas

- [Tiempo de espera de solicitud de certificado agotado](#) (p. 80)
- [Error de solicitud de certificado](#) (p. 80)

Tiempo de espera de solicitud de certificado agotado

El tiempo de espera de las solicitudes de certificados de ACM se agota si no se validan en 72 horas. Para solucionarlo, elimine la solicitud y elija Request a certificate para empezar de nuevo. Para obtener más información acerca de cómo aprobar una solicitud de certificado, consulte [Validar propiedad de dominio](#) (p. 16).

Error de solicitud de certificado

Una solicitud de un certificado de ACM puede presentar un error. Si esto ocurre, las explicaciones a continuación pueden ayudarle a entender el motivo del error y sugieren medidas para solucionarlo.

Motivos de los errores

- [Contactos no disponibles](#) (p. 80)
- [Dominio no permitido](#) (p. 81)
- [Se requiere verificación adicional](#) (p. 81)
- [Dominio público no válido](#) (p. 81)
- [Otros](#) (p. 82)

Contactos no disponibles

ACM no ha podido encontrar una dirección de correo electrónico para validar uno o varios de los nombres de dominio incluidos en la solicitud de certificado. 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 contar con un registro de intercambio de correo (MX) para que los servidores de correo electrónico de ACM sepan adónde enviar el [correo electrónico de validación de dominio \(p. 16\)](#).

Realizar una de las tareas anteriores es suficiente para solucionar este problema; no es necesario hacer ambas. Después de solucionar el problema, solicite un certificado nuevo. Si una solicitud de certificado ha presentado un error, no puede volver a enviarla.

Para obtener más información acerca de cómo asegurarse de recibir correos electrónicos de validación de dominio de ACM, consulte [Configurar correo electrónico para su dominio \(p. 11\)](#) o [No he recibido el correo electrónico de validación \(p. 77\)](#). Si sigue estos pasos y sigue apareciendo el mensaje No Available Contacts, [informe de ello a AWS](#) para que podamos investigar el problema.

Dominio no permitido

ACM no permite solicitudes de certificado para uno o varios nombres de dominio de la solicitud de certificado. Por lo general, esto se debe a que uno o varios de los nombres de dominio de la solicitud de certificado aparecen en la lista de sitios no seguros de Navegación segura de Google o en la de sitios de phishing válidos de PhishTank. Para solucionar este problema, puede:

- Buscar su nombre de dominio en el sitio web de [Estado del sitio según Navegación segura de Google](#). Si su dominio se considera inseguro, consulte el sitio web de [ayuda de Google para sitios web pirateados](#) para informarse acerca de qué puede hacer. Si cree que su dominio es seguro, consulte [Solicitar una revisión](#) de Google.
- Buscar su nombre de dominio en la [página de inicio de PhishTank](#). Si su dominio se considera de phishing, consulte el sitio de [ayuda de Google para sitios web pirateados](#) o el de [ayuda de Webmaster Hacked de StopBadware](#) para informarse acerca de qué puede hacer. Si cree su dominio es seguro, consulte la página de [preguntas frecuentes de PhishTank](#) para obtener información acerca de cómo informar de un falso positivo.

Después de solucionar el problema, solicite un certificado nuevo. Si una solicitud de certificado ha presentado un error, no puede volver a enviarla.

Se requiere verificación adicional

ACM requiere información adicional para procesar esta solicitud de certificado. Para proporcionar esta información, póngase en contacto con AWS Support desde el [Centro de soporte](#). Si no tiene un plan de soporte contratado, publique un hilo nuevo en el [Foro de debate de AWS Certificate Manager](#).

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. Este error se produce cuando la solicitud de certificado incluye estos nombres de dominio.

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 example.invalidpublicdomain porque

"invalidpublicdomain" no es un dominio de nivel superior válido. Si sigue apareciendo este motivo de error, póngase en contacto con AWS Support desde el [Centro de soporte](#). Si no tiene un plan de soporte contratado, publique un hilo nuevo en el [Foro de debate de AWS Certificate Manager](#).

Otros

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 de ortográfico que haya podido haber en la solicitud. Si sigue apareciendo este motivo de error, póngase en contacto con AWS Support desde el [Centro de soporte](#). Si no tiene un plan de soporte contratado, publique un hilo nuevo en el [Foro de debate de AWS Certificate Manager](#).

Solución de problemas de renovación administrada de certificados

Consulte los siguientes temas si surgen problemas con la [Renovación administrada para certificados emitidos por Amazon de ACM \(p. 24\)](#).

Temas

- [Validación de dominio \(p. 82\)](#)
- [Proceso asíncrono \(p. 82\)](#)

Validación de dominio

Antes de renovar el certificado, ACM intenta validar automáticamente sus nombres de dominio. Sin embargo, en algunos casos ACM necesita que siga ciertos pasos para validar manualmente un dominio. ACM renueva un certificado solo después de todos sus nombres de dominio hayan sido validados de forma automática o manual. Para obtener más información, consulte [Cómo funciona la validación de dominios \(p. 24\)](#).

Proceso asíncrono

[Renovación administrada para certificados emitidos por Amazon de ACM \(p. 24\)](#) 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 validan, puede haber un retraso antes de que ACM obtenga el nuevo certificado. Puede producirse un retraso adicional entre el momento en el 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 problemas de validación de certificados

Consulte el siguiente tema si su validación parece bloqueada en estado pendiente.

Validación incompleta

Si el estado de la solicitud del certificado de ACM es Pending validation, la solicitud está pendiente de aprobación. Para que se apruebe, el representante autorizado debe responder al correo electrónico de validación enviado a las direcciones de contacto registradas de WHOIS y a otras direcciones comunes de

correo electrónico para el dominio solicitado. Para obtener más información acerca de cómo aprobar una solicitud, consulte [Validar propiedad de dominio \(p. 16\)](#).

Important

Si su solicitud incluye más de un nombre de dominio en el certificado, debe aprobar cada nombre de dominio que haya incluido. Si no recibe un correo electrónico de validación para cada nombre de dominio incluido en la solicitud, consulte [No he recibido el correo electrónico de validación \(p. 77\)](#).

Solución de problemas de dominios .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. Cuando se realiza una búsqueda WHOIS, solo se devuelve información ofuscada del registrador. Por lo tanto, ACM no puede enviar un correo electrónico de validación a las tres direcciones de contacto registradas a continuación, que suelen estar disponibles en WHOIS.

- Titularidad del dominio
- Contacto técnico
- Contacto administrativo

Sin embargo, ACM envía correos electrónicos de validación a las siguientes cinco direcciones de sistema comunes en las que *your_domain* es el nombre de dominio introducido al solicitar el certificado inicialmente y *.io* es el dominio de nivel superior.

- administrator@*your_domain*.io
- hostmaster@*your_domain*.io
- postmaster@*your_domain*.io
- webmaster@*your_domain*.io
- admin@*your_domain*.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. De no estarlo, no recibirá un correo electrónico de validación y no se podrá emitir su certificado de ACM.

Historial de revisión

En la siguiente tabla se describe el historial de versiones de la documentación de AWS Certificate Manager.

Última actualización de la documentación: 12 de octubre de 2017

Cambio	Descripción	Fecha de la versión
Nuevo contenido	Se han añadido nuevos ejemplos de código de Java para Uso de la API de ACM (p. 58).	12 de octubre de 2017
Nuevo contenido	Se ha añadido información acerca de los registros de CAA a (Opcional) Configuración de un registro de CAA (p. 13).	21 de septiembre de 2017
Nuevo contenido	Se ha añadido información sobre dominios .IO a Solución de problemas (p. 76).	07 de julio de 2017
Nuevo contenido	Se ha añadido información sobre reimportación de un certificado a Reimportar un certificado (p. 31).	07 de julio de 2017
Nuevo contenido	Se ha añadido información acerca de asignación de certificados a prácticas recomendadas (p. 7) y a Solución de problemas (p. 76).	07 de julio de 2017
Nuevo contenido	Se ha añadido AWS CloudFormation a Servicios integrados con AWS Certificate Manager (p. 4).	27 de mayo de 2017
Update	Se ha añadido más información a Límites (p. 6).	27 de mayo de 2017
Nuevo contenido	Se ha añadido documentación sobre Autenticación y control de acceso (p. 36).	28 de abril de 2017
Update	Se ha añadido un gráfico para mostrar el destino del correo electrónico de validación. Consulte Validar propiedad de dominio (p. 16).	21 de abril de 2017
Update	Se ha añadido información sobre la configuración de correo electrónico para su dominio. Consulte Configurar correo electrónico para su dominio (p. 11).	6 de abril de 2017

Cambio	Descripción	Fecha de la versión
Update	Se ha añadido información sobre la comprobación del estado de renovación del certificado en la consola. Consulte Comprobar el estado de renovación de un certificado (p. 27) .	28 de marzo de 2017
Update	Se ha actualizado la documentación para utilizar Elastic Load Balancing.	21 de marzo de 2017
Nuevo contenido	Se ha añadido soporte para AWS Elastic Beanstalk y Amazon API Gateway. Consulte Servicios integrados con AWS Certificate Manager (p. 4) .	21 de marzo de 2017
Update	Se ha actualizado la documentación sobre Renovación administrada (p. 24) .	20 de febrero de 2017
Nuevo contenido	Se ha añadido documentación sobre Importar certificados (p. 29) .	13 de octubre de 2016
Nuevo contenido	Se ha añadido soporte de AWS CloudTrail para acciones de ACM. Consulte Registro de llamadas a la API de AWS Certificate Manager con AWS CloudTrail (p. 45) .	25 de marzo de 2016
Nueva guía	Esta versión presenta AWS Certificate Manager.	21 de enero de 2016