



Manual do usuário

# AWS Certificate Manager



Versão 1.0

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Certificate Manager: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

---

# Table of Contents

O que é AWS Certificate Manager? .....	1
O ACM é o serviço certo para mim? .....	1
Características do certificado do ACM .....	2
Regiões compatíveis .....	8
Serviços integrados .....	8
Selos de site e logotipos de confiança .....	13
Cotas .....	14
Cotas gerais .....	14
Cotas de taxa de API .....	17
Definição de preço .....	19
Segurança .....	20
Proteção de dados .....	20
Segurança para chaves privadas de certificados .....	22
Identity and Access Management .....	23
Público .....	23
Como autenticar com identidades .....	24
Gerenciando acesso usando políticas .....	28
Como o AWS Certificate Manager funciona com o IAM .....	30
Exemplos de políticas baseadas em identidade .....	38
Referência de permissões da API do ACM .....	42
Políticas gerenciadas pela AWS .....	45
Uso de chaves de condição .....	47
Uso de funções vinculadas a serviço .....	53
Solução de problemas .....	56
Resiliência .....	59
Segurança da infraestrutura .....	59
Conceder permissões de acesso programático ao ACM .....	60
Práticas recomendadas .....	61
AWS CloudFormation .....	62
Fixação do certificado .....	62
Validação de domínio .....	63
Adição ou exclusão de nomes de domínio .....	63
Cancelamento do registro em log de transparência de certificado .....	64
Ativar AWS CloudTrail .....	65

Configuração .....	67
Cadastrar-se em uma Conta da AWS .....	67
Criar um usuário administrativo .....	68
Registrar um nome de domínio .....	69
(Opcional) Configurar e-mail .....	69
Banco de dados WHOIS .....	70
MX record (Registro MX) .....	70
(Opcional) Configurar CAA .....	71
Emitir e gerenciar certificados .....	74
Solicitação de um certificado público .....	75
Solicitar um certificado público usando o console .....	76
Solicitar um certificado público usando a CLI .....	78
Como solicitar um certificado de PKI privado .....	79
Configuração de acesso a uma CA privada .....	80
Solicitar um certificado de PKI privado usando o console do ACM .....	81
Solicitar um certificado de PKI privado usando a CLI .....	83
Validar propriedade de domínios .....	85
Validação por DNS .....	86
Validação de e-mail .....	92
Listar certificados .....	96
Descrever certificados .....	99
Excluir certificados .....	103
Instalando certificados do ACM; .....	104
Renovação gerenciada .....	105
Certificados confiáveis publicamente .....	107
Validação por DNS .....	107
Validação por e-mail .....	107
Certificados de PKI privada .....	109
Automatização da exportação de certificados renovados .....	109
Testar a renovação gerenciada .....	111
Verificar status da renovação .....	112
Verificar o status (console) .....	114
Verificar o status (API) .....	114
Verificar o status (CLI) .....	114
Verificar o status usando o Personal Health Dashboard (PHD) .....	114
Automatizando a validação por e-mail .....	116

Modelos de e-mail de validação .....	116
Validando um novo certificado .....	116
Validando um certificado para renovação .....	117
Fluxo de trabalho de validação .....	118
Importar certificados .....	120
Pré-requisitos .....	121
Formato do certificado .....	122
Importar certificado .....	124
Importar (console) .....	124
Importar (AWS CLI) .....	125
Reimportar um certificado .....	126
Reimportar (console) .....	127
Reimportar (AWS CLI) .....	127
Exportar certificado .....	129
Exportação de um certificado privado (console) .....	129
Exportar um certificado privado (CLI) .....	130
Marcar certificados do ACM .....	132
Restrições de tags .....	132
Gerenciar tags .....	133
Gerenciamento de tags (console) .....	133
Gerenciamento de tags (CLI) .....	135
Gerenciar tags .....	135
Monitoramento e registro em log .....	136
Amazon EventBridge .....	136
Eventos suportados .....	136
Exemplo de ações .....	141
CloudTrail .....	151
Ações da API com suporte .....	152
Chamadas de API para serviços integrados .....	166
CloudWatch métricas .....	171
Usar a API (exemplos de Java) .....	173
AddTagsToCertificate .....	173
DeleteCertificate .....	175
DescribeCertificate .....	177
ExportCertificate .....	180
GetCertificate .....	183

ImportCertificate .....	185
ListCertificates .....	189
RenewCertificate .....	191
ListTagsForCertificate .....	193
RemoveTagsFromCertificate .....	195
RequestCertificate .....	197
ResendValidationEmail .....	200
Solução de problemas .....	203
Solicitações de certificado .....	203
Prazo de solicitação encerrado .....	203
Falha na solicitação .....	204
Validação de certificado .....	205
Validação por DNS .....	206
Validação de e-mail .....	209
Renovação de certificado .....	214
Preparação para validação automática de domínio .....	214
Tratamento de falhas de renovação de certificado gerenciada .....	215
Outros problemas .....	217
Registros da CAA .....	218
Importação de certificado .....	219
Fixação do certificado .....	220
API Gateway .....	220
Falha inesperada .....	220
Problemas com a função vinculada ao serviço (SLR) do ACM .....	221
Tratamento de exceções .....	7
Tratamento de exceções de certificado privado .....	221
Conceitos .....	225
Certificado do ACM .....	225
CAs-raiz do ACM .....	228
Domínio de apex .....	228
Criptografia de chave assimétrica .....	228
Certificate Authority (Autoridade certificadora) .....	229
Registro de transparência de certificados .....	229
Domain Name System .....	230
Nomes de domínio .....	230
Criptografia e descriptografia .....	232

---

Nome de domínio totalmente qualificado (FQDN) .....	232
Infraestrutura de chave pública .....	232
Certificado raiz .....	232
Secure Sockets Layer (SSL) .....	232
HTTPS seguro .....	233
Certificados do servidor SSL .....	233
Criptografia de chave simétrica .....	233
Transport Layer Security (TLS) .....	233
Confiança .....	233
Histórico do documento .....	234
.....	ccxli

# O que é AWS Certificate Manager?

AWS Certificate Manager (ACM) lida com a complexidade de criar, armazenar e renovar certificados e chaves SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos. Você pode fornecer certificados para o seus [serviços integrados da AWS](#) emitindo-os diretamente com o ACM ou [importando](#) certificados de terceiros para o sistema de gerenciamento do ACM. Os certificados do ACM podem proteger nomes de domínio singulares, vários nomes de domínio específicos, domínios-curinga ou combinações desses. Você também pode usar o ACM para criar certificados-curinga SSL que podem proteger um número ilimitado de subdomínios. Você também pode [exportar](#) certificados ACM assinados por CA privada da AWS para uso em qualquer lugar em sua PKI interna.

## Note

O ACM não é destinado ao uso com um servidor Web independente. Se você quiser configurar um servidor seguro autônomo em uma instância do Amazon EC2, o tutorial a seguir tem instruções: [Configurar SSL/TLS no Amazon Linux 2023](#).

## Tópicos

- [O ACM é o serviço certo para mim?](#)
- [Características do certificado do ACM](#)
- [Regiões compatíveis](#)
- [Serviços integrados com AWS Certificate Manager](#)
- [Selos de site e logotipos de confiança](#)
- [Cotas](#)
- [Preços para AWS Certificate Manager](#)

## O ACM é o serviço certo para mim?

AWS oferece duas opções aos clientes que implantam certificados X.509 gerenciados. Escolha a melhor opção para as suas necessidades.

1. AWS Certificate Manager (ACM) — Esse serviço é para clientes corporativos que precisam de uma presença segura na Web usando TLS. Os certificados ACM são implantados por meio do Elastic Load Balancing, CloudFront Amazon, Amazon API Gateway e [AWS](#) outros serviços



integrados. A aplicação mais comum desse tipo é um site público seguro com requisitos de tráfego significativos. O ACM também simplifica o gerenciamento de segurança automatizando a renovação de certificados cuja validade está expirando. Você está no lugar certo para esse serviço.

2. CA privada da AWS—Esse serviço é para clientes corporativos que criam uma infraestrutura de chave pública (PKI) dentro da AWS nuvem e destina-se ao uso privado em uma organização. Com CA privada da AWS, você pode criar sua própria hierarquia de autoridade de certificação (CA) e emitir certificados com ela para autenticar usuários, computadores, aplicativos, serviços, servidores e outros dispositivos. Os certificados emitidos por uma CA privada não podem ser usados na Internet. Para mais informações, consulte o [Guia do usuário do CA privada da AWS](#).

## Características do certificado do ACM

Os certificados públicos fornecidos pelo ACM têm as características descritas nesta seção.

### Note

Essas características se aplicam apenas aos certificados fornecidos pelo ACM. Elas podem não se aplicar aos [certificados que você importar para o ACM](#).

### Autoridade certificadora e hierarquia

Os certificados públicos que você solicita por meio do ACM são obtidos da [Amazon Trust Services](#), uma [autoridade de certificação pública \(CA\)](#) gerenciada pela Amazon. As Amazon Root CAs 1 a 4 são assinadas por uma raiz mais antiga chamada Starfield G2 Root Certificate Authority - G2. A raiz Starfield é confiável em dispositivos Android a partir das versões mais novas do Gingerbread e, no iOS, a partir da versão 4.1 do sistema. As raízes da Amazon são consideradas confiáveis pelo iOS a partir da versão 11. Qualquer navegador, aplicação ou sistema operacional que inclua as raízes da Amazon ou Starfield confiará nos certificados públicos obtidos do ACM.

Os certificados leaf ou de entidade final emitido pelo ACM para os clientes derivam sua autoridade de uma CA raiz do Amazon Trust Services por meio de qualquer uma das várias CAs intermediárias. O ACM atribui aleatoriamente uma CA intermediária com base no tipo de certificado (RSA ou ECDSA) solicitado. Como a CA intermediária é selecionada aleatoriamente após a geração da solicitação, o ACM não fornece informações da CA intermediária.

## Confiança de navegadores e aplicações

Os certificados do ACM são da confiança de todos os principais navegadores, incluindo Google Chrome, Microsoft Internet Explorer e Microsoft Edge, Mozilla Firefox e Apple Safari. Os navegadores que confiam nos certificados do ACM exibem um ícone de cadeado na barra de status ou barra de endereço quando conectados por SSL/TLS a sites que usam os certificados ACM. Os certificados do ACM também são confiáveis para o Java.

## Rotação de CA intermediária e raiz

Para manter uma infraestrutura de certificados ágil e resiliente, a Amazon pode, a qualquer momento, optar por descontinuar uma CA intermediária sem aviso prévio. Mudanças desse tipo não têm impacto nos clientes. Para obter mais informações, consulte a postagem [“Amazon introduces dynamic intermediate certificate authorities”](#) (Amazon apresenta autoridades de certificação intermediárias dinâmicas) no blog.

No caso improvável de a Amazon descontinuar uma CA raiz, a alteração ocorrerá tão rapidamente quanto as circunstâncias exigirem. Devido ao grande impacto dessa mudança, a Amazon usará todos os mecanismos disponíveis para notificar os AWS clientes, incluindo o AWS Health Dashboard e-mail para os proprietários da conta e o contato com os gerentes técnicos da conta.

## Acesso ao firewall para revogação

Se um certificado de entidade final não for mais confiável, ele será revogado. OCSP e CRLs são os mecanismos padrão usados para verificar se um certificado foi revogado ou não. OCSP e CRLs são os mecanismos padrão usados para publicar informações de revogação. Alguns firewalls de clientes podem precisar de regras adicionais para permitir que esses mecanismos funcionem.

O exemplo a seguir de padrões-curinga de URL pode ser usado para identificar tráfego de revogação. Um caractere-curinga asterisco (\*) representa um ou mais caracteres alfanuméricos, um ponto de interrogação (?) representa um único caractere alfanumérico e uma marca de hash (#) representa um número.

- OCSP

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

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

- CRL

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

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

## Validação de domínio (DV)

Os certificados do ACM têm validação de domínio. Ou seja, o campo de assunto de um certificado do ACM identifica um nome de domínio e nada mais. Ao solicitar um certificado do ACM, você deve validar que possui ou controla todos os domínios especificados na solicitação. Você pode validar a propriedade usando e-mail ou DNS. Para ter mais informações, consulte [Validação de e-mail](#) e [Validação por DNS](#).

## Período de validade

O período de validade dos certificados do ACM atualmente é de 13 meses (395 dias).

## Renovação e implantação gerenciadas

O ACM gerencia o processo de renovação dos certificados do ACM e o provisionamento dos certificados após serem renovados. A renovação automática pode ajudá-lo a evitar tempo de inatividade devido a certificados configurados incorretamente, revogados ou expirados. Para ter mais informações, consulte [Renovação gerenciada para certificados do ACM](#).

## Vários nomes de domínio

Cada certificado do ACM deve incluir pelo menos um nome de domínio totalmente qualificado (FQDN), e você poderá adicionar mais nomes se quiser. Por exemplo, quando está criando um certificado do ACM para `www.example.com`, você também pode adicionar o nome `www.example.net` se os clientes puderem entrar em contato com o seu site usando qualquer um dos nomes. Isso também é verdadeiro para domínios vazios (também conhecidos como o apex de zona ou domínios nus). Ou seja, você pode solicitar um certificado do ACM para `www.example.com` e adicionar o nome `exemplo.com`. Para ter mais informações, consulte [Solicitação de um certificado público](#).

## Nomes curinga

O ACM permite que você use um asterisco (\*) no nome de domínio para criar um certificado do ACM contendo um nome-curinga, que pode proteger vários sites no mesmo domínio. Por exemplo, `*.example.com` protege `www.example.com` e `images.example.com`.

**Note**

Quando você solicita um certificado curinga, o asterisco (\*) deve estar na posição mais à esquerda do nome do domínio e só pode proteger um nível de subdomínio. Por exemplo, o **\*.example.com** pode proteger **login.example.com** e **test.example.com** mas não consegue proteger **test.login.example.com**. Note também que **\*.example.com** protege apenas os subdomínios de **example.com**, ele não protege o domínio vazio ou apex (**example.com**). No entanto, você pode solicitar um certificado que proteja um domínio vazio ou apex ou seus subdomínios, especificando vários nomes de domínio em sua solicitação. Por exemplo, você pode solicitar um certificado que proteja **example.com** e **\*.example.com**.

## Algoritmos-chave

Um certificado deve especificar um algoritmo e um tamanho de chave. Atualmente, os algoritmos de chave pública RSA e Elliptic Curve Digital Signature Algorithm (ECDSA) são suportados pelo ACM. O ACM pode solicitar a emissão de novos certificados utilizando algoritmos marcados com um asterisco (\*). Os algoritmos restantes são suportados somente para certificados [importados](#).

**Note**

Quando você solicita um certificado PKI privado assinado por uma CA AWS Private CA, a família de algoritmos de assinatura especificada (RSA ou ECDSA) deve corresponder à família de algoritmos da chave secreta da CA.

- RSA de 1024 bits (RSA\_1024)
- RSA de 2048 bits (RSA\_2048)\*
- RSA de 3072 bits (RSA\_3072)
- RSA de 4096 bits (RSA\_4096)
- ECDSA de 256 bits (EC\_prime256v1)\*
- ECDSA de 384 bits (EC\_secp384r1)\*
- ECDSA de 521 bits (EC\_secp521r1)

As chaves ECDSA são menores, oferecendo segurança comparável às chaves RSA, mas com maior eficiência computacional. No entanto, ECDSA não é suportado por todos os clientes da

rede. A tabela a seguir, adaptada do [NIST](#), mostra a força de segurança representativa de RSA e ECDSA com chaves de vários tamanhos. Todos os valores estão em bits.

Comparando segurança para algoritmos e chaves

Força de segurança	Tamanho da chave RSA	Tamanho da chave ECDSA
128	3072	256
192	7680	384
256	15360	512

A força de segurança, entendida como uma potência de 2, está relacionada ao número de tentativas necessárias para quebrar a criptografia. Por exemplo, uma chave RSA de 3072 bits e uma chave ECDSA de 256 bits podem ser recuperadas com não mais de  $2^{128}$  suposições.

Para obter informações para ajudá-lo a escolher um algoritmo, consulte a postagem do AWS blog [Como avaliar e usar certificados ECDSA em](#). AWS Certificate Manager

#### Important

Observe que os [serviços integrados](#) permitem apenas que sejam associados aos recursos os algoritmos e os tamanhos de chaves compatíveis. Além disso, o suporte será diferente se o certificado for importado para o IAM ou para o ACM. Para obter mais informações, consulte a documentação para cada serviço.

- Para o Elastic Load Balancing, consulte [Listeners HTTPS para seu Application Load Balancer](#).
- Para saber mais CloudFront, consulte [Protocolos e cifras SSL/TLS compatíveis](#).

## Punycode

É necessário satisfazer os seguintes requisitos de [Punycode](#) relacionados a [Internationalized Domain Names](#) (Nomes de domínio internacionalizados):

1. Nomes de domínio que comecem com o padrão “<character><character>--” devem corresponder a “xn--”.

2. Nomes de domínio que comecem com “xn--” também devem ser nomes de domínio internacionalizado válidos.

### Exemplos de Punycode

Nome do domínio	Satisfaz o n.º 1	Satisfaz o n.º 2	Permit	Observação
exemplo.com	n/a	n/a	✓	Não começa com “<character><character>--”
a--examp le.com	n/a	n/a	✓	Não começa com “<character><character>--”
abc--exam ple.com	n/a	n/a	✓	Não começa com “<character><character>--”
xn--xyz.com	Sim	Sim	✓	Nome de domínio internacionalizado válido (é resolvido para 簡.com)
xn--examp le.com	Sim	Não	✗	Não é um nome de domínio internacionalizado válido
ab--examp le.com	Não	Não	✗	Deve começar com “xn--”

### Exceções

Observe o seguinte:

- O ACM não fornece certificados de validação estendida (EV) nem certificados de validação de organização (OV).
- O ACM não fornece certificados para outros itens, exceto protocolos SSL/TLS.
- Não é possível usar certificados do ACM para criptografia de e-mail.
- Atualmente, o ACM não permite que você cancele a opção de [renovação de certificados gerenciados](#) para certificados do ACM. Além disso, a renovação gerenciada não está disponível para certificados importados para o ACM.

- Você não pode solicitar certificados para nomes de domínio pertencentes à Amazon, como aqueles que terminam em `amazonaws.com`, `cloudfront.net` ou `elasticbeanstalk.com`.
- Você não pode baixar a chave privada para um certificado do ACM.
- Você não pode instalar certificados do ACM diretamente em seu site ou aplicativo Amazon Elastic Compute Cloud (Amazon EC2). No entanto, você pode usar o certificado com qualquer serviço integrado. Para ter mais informações, consulte [Serviços integrados com AWS Certificate Manager](#).

## Regiões compatíveis

Acesse [Regiões e endpoints da AWS](#) em Referência geral da AWS ou a [Tabela de regiões da AWS](#) para ver a disponibilidade regional do ACM.

Os certificados no ACM são recursos regionais. Para usar um certificado com o Elastic Load Balancing para o mesmo nome de domínio totalmente qualificado (FQDN) ou conjunto de FQDNs em mais de uma AWS região, você deve solicitar ou importar um certificado para cada região. Para certificados fornecidos pelo ACM, isso significa que você deve revalidar cada nome de domínio no certificado para cada região. Você não pode copiar um certificado entre as regiões.

Para usar um certificado ACM com a Amazon CloudFront, você deve solicitar ou importar o certificado na região Leste dos EUA (Norte da Virgínia). Os certificados do ACM nessa região associados a uma CloudFront distribuição são distribuídos para todas as localizações geográficas configuradas para essa distribuição.

## Serviços integrados com AWS Certificate Manager

AWS Certificate Manager suporta um número crescente de AWS serviços. Você não pode instalar seu certificado ACM ou seu CA privada da AWS certificado privado diretamente em seu site ou aplicativo AWS baseado.

### Note

Certificados públicos do ACM podem ser instalados em instâncias do Amazon EC2 conectadas a um [Nitro Enclave](#), mas não a outras instâncias do Amazon EC2. Para obter informações sobre como configurar um servidor Web independente em uma instância do Amazon EC2 não conectada a um Nitro Enclave, consulte [Tutorial: Instalar um servidor Web](#)

[LAMP no Amazon Linux 2](#) ou [Tutorial: Instalar um servidor Web LAMP com o Amazon Linux AMI](#).

Os certificados do ACM são suportados pelos seguintes serviços:

### Elastic Load Balancing

O Elastic Load Balancing distribui automaticamente o tráfego de entrada dos aplicativos entre várias instâncias do Amazon EC2. Ele detecta instâncias com problemas de integridade e redireciona o tráfego automaticamente para instâncias íntegras até que as instâncias com problemas de integridade sejam restauradas. O Elastic Load Balancing escala automaticamente sua capacidade de gerenciamento de solicitações em resposta ao tráfego de entrada. Para mais informações sobre balanceamento de carga consulte o [Manual do usuário do Elastic Load Balancing](#).

Em geral, para servir conteúdo protegido por SSL/TLS, os balanceadores de carga exigem que os certificados SSL/TLS sejam instalados no balanceador de carga ou na instância do Amazon EC2 no backend. O ACM se integra ao Elastic Load Balancing para implantar certificados em seu balanceador de carga. Para obter mais informações, consulte [Create an Application Load Balancer](#) (Criar um Application Load Balancer)

### Amazon CloudFront

CloudFront A Amazon é um serviço web que acelera a distribuição de seu conteúdo web dinâmico e estático para usuários finais, entregando seu conteúdo de uma rede mundial de pontos de presença. Quando um usuário final solicita conteúdo por meio do qual você está servindo CloudFront, o usuário é encaminhado para o ponto de presença que fornece a menor latência. Isso garante que o conteúdo seja distribuído com a melhor performance possível. Se o conteúdo estiver atualmente nesse ponto de presença, CloudFront entrega-o imediatamente. Se o conteúdo não estiver atualmente nesse ponto de presença, CloudFront recupere-o do bucket ou servidor web do Amazon S3 que você identificou como a fonte de conteúdo definitiva. Para obter mais informações sobre CloudFront, consulte o [Amazon CloudFront Developer Guide](#).

Para fornecer conteúdo seguro via SSL/TLS, é CloudFront necessário que os certificados SSL/TLS sejam instalados na CloudFront distribuição ou na fonte de conteúdo de backup. O ACM é integrado CloudFront para implantar certificados ACM na CloudFront distribuição. Para obter mais informações, consulte [Obter um certificado do SSL/TLS](#).



**Note**

Para usar um certificado ACM com CloudFront, você deve solicitar ou importar o certificado na região Leste dos EUA (Norte da Virgínia).

## Amazon Cognito

O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis. Os usuários podem fazer login diretamente com suas Conta da AWS credenciais ou por meio de terceiros, como Facebook, Amazon, Google ou Apple. Para obter mais informações sobre o Amazon Cognito, consulte o [Guia do desenvolvedor do Amazon Cognito](#).

Quando você configura um grupo de usuários do Cognito para usar um CloudFront proxy da Amazon, CloudFront pode implementar um certificado ACM para proteger o domínio personalizado. Quando for esse o caso, lembre-se de que você deve remover a associação do certificado CloudFront antes de excluí-lo.

## AWS Elastic Beanstalk

O Elastic Beanstalk ajuda você a implantar e gerenciar aplicativos AWS na nuvem sem se preocupar com a infraestrutura que executa esses aplicativos. AWS Elastic Beanstalk reduz a complexidade do gerenciamento. Basta fazer upload da aplicativo, e o Elastic Beanstalk automaticamente gerencia os detalhes de provisão de capacidade, balanceamento de carga, escalabilidade e monitoramento da integridade do aplicativo. O Elastic Beanstalk usa o serviço Elastic Load Balancing para criar um balanceador de carga. Para obter mais informações sobre o Elastic Beanstalk, consulte o [AWS Elastic Beanstalk Guia do desenvolvedor do Elastic Beanstalk](#).

Para escolher um certificado, você deve configurar o balanceador de carga para seu aplicativo no console do Elastic Beanstalk. Para obter mais informações, consulte [Configuração do o ambiente do balanceador de carga do Elastic Beanstalk para terminar o HTTPS](#).

## AWS App Runner

O App Runner é um AWS serviço que fornece uma maneira rápida, simples e econômica de implantar a partir do código-fonte ou de uma imagem de contêiner diretamente em um aplicativo web escalável e seguro na nuvem. AWS Você não precisa aprender novas tecnologias, decidir qual serviço de computação usar ou saber como provisionar e configurar AWS recursos. Para obter mais informações sobre o App Runner, consulte o [Guia do desenvolvedor do AWS App Runner](#).

Quando você associa nomes de domínio personalizados ao seu serviço App Runner, o App Runner cria internamente certificados que controlam a validade do domínio. Eles estão armazenados no ACM. O App Runner não exclui esses certificados durante um período de sete dias após um domínio ser desassociado do seu serviço ou após o serviço ser excluído. Todo esse processo é automatizado e você não precisa adicionar nem gerenciar certificados por conta própria. Para obter mais informações, consulte [Gerenciamento de nomes de domínio personalizados para um serviço App Runner](#) no Guia do desenvolvedor do AWS App Runner .

## Amazon API Gateway

Com a proliferação de dispositivos móveis e o crescimento da Internet das Coisas (IoT), tornou-se cada vez mais comum criar APIs que podem ser usadas para acessar dados e interagir com sistemas de back-end na AWS. Você pode usar o API Gateway para publicar, manter, monitorar e proteger suas APIs. Após implantar a API no API Gateway, você pode [configurar um nome de domínio personalizado](#) para simplificar o acesso a ela. Para configurar um nome de domínio personalizado, você deve fornecer um certificado SSL/TLS. Você pode usar o ACM para gerar ou importar o certificado. Para obter mais informações sobre o Amazon API Gateway, consulte o [Guia do desenvolvedor do Amazon API Gateway](#).

## AWS Enclaves Nitro

AWS O Nitro Enclaves é um recurso do Amazon EC2 que permite criar ambientes de execução isolados, chamados enclaves, a partir de instâncias do Amazon EC2. Os enclaves são máquinas virtuais separadas, reforçadas e altamente restritas. Eles fornecem apenas conectividade de soquete local segura com sua instância-pai. Eles não têm armazenamento persistente, acesso interativo ou rede externa. Os usuários não podem usar SSH em um enclave, e os dados e aplicativos dentro do enclave não podem ser acessados pelos processos, aplicativos ou usuários da instância-pai (incluindo raiz e administrador).

As instâncias do EC2 conectadas ao Nitro Enclaves suportam certificados do ACM. Para obter mais informações, consulte [AWS Certificate Manager para Nitro Enclaves](#).

### Note

Não é possível associar certificados do ACM a uma instância do EC2 que não esteja conectada a um Nitro Enclave.

## AWS CloudFormation

AWS CloudFormation ajuda você a modelar e configurar seus recursos da Amazon Web Services. Você cria um modelo que descreve os AWS recursos que deseja usar, como o Elastic Load Balancing ou o API Gateway. Em seguida, o AWS CloudFormation se encarrega de provisionar e configurar esses recursos para você. Você não precisa criar e configurar AWS recursos individualmente e descobrir o que depende do quê; AWS CloudFormation lida com tudo isso. Os certificados ACM são incluídos como um recurso de modelo, o que significa que AWS CloudFormation podem solicitar certificados ACM que você pode usar com AWS serviços para habilitar conexões seguras. Além disso, os certificados ACM estão incluídos em muitos dos AWS recursos com os quais você pode configurar. AWS CloudFormation

Para obter informações gerais sobre CloudFormation, consulte o [Guia AWS CloudFormation do usuário](#). Para obter informações sobre os recursos do ACM suportados pelo CloudFormation, consulte [AWS::CertificateManager::Certificate](#).

Com a poderosa automação fornecida pelo AWS CloudFormation, é fácil exceder sua [cota de certificados](#), especialmente com novas AWS contas. Recomendamos que você siga as [melhores práticas](#) do ACM para AWS CloudFormation.

### Note

Se você criar um certificado ACM com AWS CloudFormation, a AWS CloudFormation pilha permanecerá no estado CREATE\_IN\_PROGRESS. Todas as outras operações de stack são atrasadas até que você aja de acordo com as instruções no e-mail de validação do certificado. Para obter mais informações, consulte [Falha de recurso em estabilizar durante uma operação de criar, atualizar ou excluir stack](#).

## AWS Amplify

O Amplify é um conjunto de ferramentas e recursos específicos que permitem que desenvolvedores front-end web e móveis criem aplicativos completos de forma rápida e fácil. AWS O Amplify fornece dois serviços: Amplify Hosting e Amplify Studio. O Amplify Hosting fornece um fluxo de trabalho baseado em git para hospedar aplicações Web de pilha completa sem servidor com implantação contínua. O Amplify Studio é um ambiente de desenvolvimento visual que simplifica a criação de aplicações móveis e Web escaláveis e completas. Use o Studio para criar sua interface de usuário de front-end com um conjunto de componentes de ready-to-

use interface do usuário, criar um back-end de aplicativo e, em seguida, conectar os dois. Para obter informações sobre o Amplify, consulte o Guia do usuário da [AWS Amplify](#).

Se você conectar um domínio personalizado à aplicação, o console do Amplify emitirá um certificado ACM para protegê-lo.

## OpenSearch Serviço Amazon

O Amazon OpenSearch Service é um mecanismo de pesquisa e análise para casos de uso, como análise de log, monitoramento de aplicativos em tempo real e análise de fluxo de cliques. Para obter mais informações, consulte o [Amazon OpenSearch Service Developer Guide](#).

Ao criar um cluster de OpenSearch serviços que contém um [domínio e um endpoint personalizados](#), você pode usar o ACM para provisionar o Application Load Balancer associado com um certificado.

## AWS Network Firewall

AWS Network Firewall é um serviço gerenciado que facilita a implantação de proteções de rede essenciais para todas as suas Amazon Virtual Private Clouds (VPCs). Para obter mais informações sobre o Network Firewall, consulte o [Guia do desenvolvedor do AWS Network Firewall](#).

O firewall do Network Firewall integra-se ao ACM para a inspeção TLS. Caso use a inspeção TLS no Network Firewall, você deve configurar um certificado ACM para a descryptografia e a criptografia novamente do tráfego SSL/TLS que passa pelo seu firewall. Para obter informações sobre como o Network Firewall funciona com o ACM para a inspeção TLS, consulte [Requisitos para usar certificados SSL/TLS com configurações de inspeção TLS](#) no Guia do desenvolvedor do AWS Network Firewall .

## Selos de site e logotipos de confiança

A Amazon não fornece um selo de site nem permite que sua marca comercial seja usada dessa forma:

- AWS Certificate Manager (ACM) não fornece um selo de site seguro que você possa usar em seu site. Se quiser usar um selo de site, você obter um com um terceiro fornecedor. Recomendamos escolher um fornecedor que avalie e garanta a segurança de seu site ou práticas comerciais.
- A Amazon não permite que sua marca comercial ou logotipo sejam usados como uma etiqueta de certificado, selo de site ou logotipo de confiança. Selos e emblemas desse tipo podem ser

copiados para sites que não usam o serviço do ACM e podem ser usados de modo inadequado para estabelecer confiança sob alegações falsas. Para proteger nossos clientes e a reputação da Amazon, não permitimos que nossa marca comercial e logotipo sejam usados dessa forma.

## Cotas

As cotas de serviço AWS Certificate Manager (ACM) a seguir se aplicam a cada AWS região por cada AWS conta.

Para ver quais cotas podem ser ajustadas, consulte a [Tabela de cotas do ACM](#) no Guia geral de referência da AWS . Para solicitar aumentos de cota, abra um caso no [AWS Support Center](#).

### Cotas gerais

Item	Cota padrão
Número de certificados do ACM	2500
Certificados expirados e revogados continuam a contar para esse total.	
Os certificados assinados por uma CA de CA privada da AWS não contam para esse total.	
Número de certificados do ACM por ano (últimos 365 dias)	Duas vezes a cota da sua conta
É possível solicitar até duas vezes a cota de certificados do ACM por ano, por região e por conta. Por exemplo, se a cota for 2.500, você poderá solicitar até 5.000 certificados do ACM por ano em uma região e uma conta específicas. Você pode ter apenas 2.500 certificados em um dado momento. Para solicitar 5.000 certificados em um ano, você deverá excluir 2.500 durante o ano para ficar dentro da cota. Se precisar de mais de 2.500 certificados em	

Item	Cota padrão
um dado momento, entre em contato com o <a href="#">AWS Support Center</a> .  Os certificados assinados por uma CA de CA privada da AWS não contam para esse total.	
Número de certificados importados	2.500
Número de certificados importados por ano (últimos 365 dias)	Duas vezes a cota da sua conta

Item	Cota padrão
<p data-bbox="110 226 755 304">Número de nomes de domínio por certificado do ACM</p> <p data-bbox="110 352 776 478">A cota padrão é de 10 nomes de domínio para cada certificado do ACM. Sua cota pode ser maior.</p> <p data-bbox="110 527 782 703">O primeiro nome de domínio que você envia é incluído como o nome comum (CN) do assunto do certificado. Todos os nomes são incluídos na extensão nome de assunto alternativo.</p> <p data-bbox="110 751 781 1165">Você pode solicitar até 100 nomes de domínio. Para solicitar um aumento na sua cota, crie uma solicitação no console de Cotas de Serviço para o serviço ACM. No entanto, antes de abrir um caso, entenda como a adição de nomes de domínio pode criar mais trabalho administrativo quando você usa a validação de e-mail. Para ter mais informações, consulte <a href="#">Validação de domínio</a>.</p> <p data-bbox="110 1213 776 1480">A cota para o número de nomes de domínio por certificado do ACM se aplica apenas aos certificados fornecidos pelo ACM. Essa cota não se aplica aos certificados importados para o ACM. As seções a seguir se aplicam apenas aos certificados do ACM.</p>	10

Item	Cota padrão
<p>Número de CAs privadas</p> <p>O ACM é integrado com AWS Private Certificate Authority (CA privada da AWS). Você pode usar o console do ACM ou a API do ACM para solicitar certificados privados de uma autoridade de certificação privada (CA) existente hospedada por. AWS CLI CA privada da AWS Esses certificados são gerenciados no ambiente do ACM e têm as mesmas restrições que os certificados públicos emitidos pelo ACM. Para ter mais informações, consulte <a href="#">Como solicitar um certificado de PKI privado</a>. Você também pode emitir certificados privados usando o CA privada da AWS serviço independente. Para obter mais informações, consulte <a href="#">Emitir um certificado privado de entidade final</a>.</p> <p>Uma CA privada que tenha sido excluída será contabilizada em sua cota até o final de seu período de restauração. Para obter mais informações, consulte <a href="#">Excluir a CA privada</a>.</p>	200
Número de certificados privados por CA (vida útil)	1.000.000

## Cotas de taxa de API

As cotas de serviço da API do ACM a seguir se aplicam a cada região e a cada conta. O ACM restringe as solicitações de API a cotas diferentes, dependendo da operação de API. A restrição significa que o ACM rejeita uma solicitação que de outra forma seria válida porque ela excede a cota de número de solicitações por segundo da operação. Quando uma solicitação é rejeitada, o ACM retorna um erro de `ThrottlingException`. A tabela a seguir lista cada operação de API e a cota à qual o ACM restringe as solicitações para aquela operação.



**Note**

Além das ações de API listadas na tabela abaixo, o ACM também pode chamar a ação `IssueCertificate` externa da CA privada da AWS. Para obter up-to-date informações sobre cotas tarifárias `IssueCertificate`, consulte os [endpoints e as cotas](#) para CA privada da AWS

requests-per-second Cota R para cada operação da API do ACM

Chamada de API	Solicitações por segundo
<code>AddTagsToCertificate</code>	5
<code>DeleteCertificate</code>	10
<code>DescribeCertificate</code>	10
<code>ExportCertificate</code>	5
<code>GetAccountConfiguration</code>	1
<code>GetCertificate</code>	10
<code>ImportCertificate</code>	1
<code>ListCertificates</code>	8
<code>ListTagsForCertificate</code>	10
<code>PutAccountConfiguration</code>	1
<code>RemoveTagsFromCertificate</code>	5
<code>RenewCertificate</code>	5
<code>RequestCertificate</code>	5
<code>ResendValidationEmail</code>	1
<code>UpdateCertificateOptions</code>	5

Para obter mais informações, consulte [Referência de API do AWS Certificate Manager](#).

## Preços para AWS Certificate Manager

Você não está sujeito a uma cobrança adicional para certificados SSL/TLS que gerencia com o AWS Certificate Manager. Você paga somente pelos AWS recursos criados para executar seu site ou aplicativo. Para obter as informações mais recentes sobre preços do ACM, consulte a página [AWS Certificate Manager de preços de serviços](#) no AWS site.

# Segurança em AWS Certificate Manager

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam AWS Certificate Manager, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Certificate Manager (ACM). Os tópicos a seguir mostram como configurar o ACM para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do ACM.

## Tópicos

- [Proteção de dados em AWS Certificate Manager](#)
- [Identity and Access Management para o AWS Certificate Manager](#)
- [Resiliência em AWS Certificate Manager](#)
- [Segurança da infraestrutura no AWS Certificate Manager](#)
- [Práticas recomendadas](#)

## Proteção de dados em AWS Certificate Manager

O modelo de [responsabilidade AWS compartilhada modelo](#) se aplica à proteção de dados em AWS Certificate Manager. Conforme descrito neste modelo, AWS é responsável por proteger a

infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o ACM ou outro Serviços da AWS usando o console, a API ou os AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Segurança para chaves privadas de certificados

Quando você [solicita um certificado público](#), o AWS Certificate Manager (ACM) gera um par de chaves pública/privada. Para [certificados importados](#), você gera o par de chaves. A chave pública se torna parte do certificado. O ACM armazena o certificado e sua chave privada correspondente e usa AWS Key Management Service (AWS KMS) para ajudar a proteger a chave privada. O processo funciona deste modo:

1. Na primeira vez que você solicita ou importa um certificado em uma AWS região, o ACM cria um certificado gerenciado AWS KMS key com o alias `aws/acm`. Essa chave KMS é exclusiva em cada AWS conta e em cada AWS região.
2. O ACM usa essa chave do KMS para criptografar a chave privada do certificado. O ACM armazena apenas uma versão criptografada da chave privada; o ACM não armazena a chave privada em formato de texto simples. O ACM usa a mesma chave KMS para criptografar as chaves privadas de todos os certificados em uma AWS conta específica e em uma região específica. AWS
3. Quando você associa o certificado com um serviço que está integrado ao AWS Certificate Manager, o ACM envia o certificado e a chave privada criptografada para o serviço. Também é criada uma concessão AWS KMS que permite que o serviço use a chave KMS para descriptografar a chave privada do certificado. Para obter mais informações sobre concessões, consulte [Usando concessões](#) no Guia do desenvolvedor do AWS Key Management Service . Para obter mais informações sobre os serviços suportados pelo ACM, consulte [Serviços integrados com AWS Certificate Manager](#).

### Note

Você tem controle sobre a AWS KMS concessão criada automaticamente. Se você excluir essa concessão por qualquer motivo, perderá a funcionalidade do ACM para o serviço integrado.

4. Os serviços integrados usam a chave do KMS para descriptografar a chave privada. Em seguida, o serviço usa o certificado e a chave privada descriptografada (texto sem formatação) para estabelecer canais de comunicação segura (sessões SSL/TLS) com seus clientes.
5. Quando o certificado é desassociado de um serviço integrado, a concessão criada na etapa 3 é baixada. Isso significa que o serviço não pode mais usar a chave do KMS para descriptografar a chave privada do certificado.

# Identity and Access Management para o AWS Certificate Manager

AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda o administrador no controle de segurança de acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do ACM. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

## Tópicos

- [Público](#)
- [Como autenticar com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como o AWS Certificate Manager funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#)
- [Permissões da API do ACM: referência de ações e recursos](#)
- [Políticas gerenciadas pela AWS para o AWS Certificate Manager](#)
- [Como usar chaves de condição com o ACM](#)
- [Uso de uma função vinculada ao serviço \(SLR\) com o ACM](#)
- [Solução de problemas de identidade e acesso AWS Certificate Manager](#)

## Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho realizado no ACM.

**Usuário do serviço:** se você usa o serviço ACM para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do ACM para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no ACM, consulte [Solução de problemas de identidade e acesso AWS Certificate Manager](#).

**Administrador do serviço:** se você for o responsável pelos recursos do ACM na empresa, provavelmente terá acesso total ao ACM. Cabe a você determinar quais funcionalidades e recursos do ACM os usuários do serviço devem acessar. Assim, você deve enviar solicitações

ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Analise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o ACM, consulte [Como o AWS Certificate Manager funciona com o IAM](#).

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao ACM. Para visualizar exemplos de políticas baseadas em identidade do ACM que podem ser usadas no IAM, consulte [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#).

## Como autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Você deve ser autenticado (ter feito login em AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode ter feito login em AWS como uma identidade federada usando credenciais fornecidas por meio de origem de identidade. AWS IAM Identity Center Os usuários do IAM Identity Center [Centro de Identidade], a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário que você seja, você pode fazer login no AWS Management Console ou no portal de acesso da AWS. Para obter mais informações sobre como fazer login em AWS, consulte [Como Fazer Login na sua Conta da AWS](#) no Início de Sessão da AWS Manual do usuário.

Se você acessar AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte [Assinando Solicitações de API AWS](#) no Guia do Usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte [Autenticação Multifator](#) no AWS IAM Identity Center Guia do Usuário. [Usar a autenticação multifator \(MFA\) na AWS](#) no Guia do Usuário do IAM.

## Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do usuário do IAM.

## Identidade federada

Como prática recomendada, exija que usuários - inclusive os que precisem de acesso administrativo - usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades web, o AWS Directory Service, o Diretório do Identity Center ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma origem de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no AWS IAM Identity Center Manual do Usuário do.

## Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte [Altere Chaves de Acesso Regularmente para Casos de Uso que exijam Credenciais de Longo Prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários



usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um nome de grupo IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando Criar um Usuário do IAM \(Ao Invés de uma Função\)](#) no Guia do Usuário do IAM.

## Perfis do IAM

Um [perfil do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM em AWS Management Console [alternando perfis](#). É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou mesmo usando URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte [Usando Funções do IAM](#) no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado — para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criando um Perfil para um Provedor de Identidades Terceirizado](#) no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no AWS IAM Identity Center Manual do Usuário.
- Permissões de usuários temporárias do IAM — um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas,

consulte [Como as Funções do IAM Diferem das Políticas Baseadas em Recurso](#) no Guia do Usuário do IAM.

- Acesso entre serviços — alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.
- Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você deve ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhamento de sessões de acesso](#).
- Função de Serviço — uma função de serviço é uma [função do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criando um Perfil para Delegar Permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.
- Função vinculada a serviço — uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.
- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicativos em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso e armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte [Quando Criar uma Função do IAM \(em Vez de um Usuário\)](#) no Guia do Usuário do IAM.

## Gerenciando acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão Geral das Políticas JSON](#) no Guia do Usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e sob quais condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM as funções e os usuários podem assumir as funções.

As políticas do IAM definem permissões para uma ação, independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte [Criar Políticas do IAM](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política

gerenciada ou uma política em linha, consulte [Selecionar entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

## Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. Saiba mais sobre ACLs em [Configurações da lista de controle de acesso \(ACL\)](#) no Guia do Desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

A AWS oferece suporte a tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações

sobre limites de permissões, consulte [Limites de Permissões para Entidades do IAM](#) no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, inclusive cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte [Como os SCPs Funcionam](#) no AWS OrganizationsManual do Usuário do.
- Políticas de sessão — são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Saiba como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos consultando [Lógica da Avaliação de Políticas](#) no Guia do Usuário do IAM.

## Como o AWS Certificate Manager funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao ACM, saiba quais recursos do IAM estão disponíveis para uso com o ACM.

### Recursos do IAM que você pode usar com o AWS Certificate Manager

Atributos do IAM	Compatível com o ACM
<a href="#">Políticas baseadas em identidade</a>	Sim
<a href="#">Políticas baseadas em recursos</a>	Não

Atributos do IAM	Compatível com o ACM
<a href="#">Ações das políticas</a>	Sim
<a href="#">Recursos de políticas</a>	Sim
<a href="#">Chaves de condição de política (específicas do serviço)</a>	Sim
<a href="#">ACLs</a>	Não
<a href="#">ABAC (etiquetas em políticas)</a>	Parcial
<a href="#">Credenciais temporárias</a>	Sim
<a href="#">Permissões de entidade principal</a>	Sim
<a href="#">Perfis de serviço</a>	Não
<a href="#">Funções vinculadas ao serviço</a>	Sim

Para obter uma visão geral de como o ACM e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte [Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

## Políticas baseadas em identidade para o ACM

Suporta com políticas baseadas em identidade	Sim
--	-----

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Saiba como criar uma política baseada em identidade consultando [Criando Políticas do IAM](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Saiba mais sobre todos os elementos que

podem ser usados em uma política JSON consultando [Referência de Elementos de Política JSON do IAM](#) no Guia do Usuário do IAM.

## Exemplos de políticas baseadas em identidade para o ACM

Para visualizar exemplos de políticas baseadas em identidade do ACM, consulte [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#).

## Políticas baseadas em recursos no ACM

Oferece suporte a políticas baseadas em recursos	Não
--	-----

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

## Ações de políticas para o ACM

Oferece suporte a ações de políticas	Sim
--------------------------------------	-----

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do ACM, consulte [Ações definidas pelo AWS Certificate Manager](#) na Referência de autorização do serviço.

As ações de políticas no ACM usam o seguinte prefixo antes da ação:

```
acm
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Para visualizar exemplos de políticas baseadas em identidade do ACM, consulte [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#).

## Recursos de políticas para o ACM

Oferece suporte a recursos de políticas	Sim
---	-----

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como



prática recomendada, especifique um recurso usando seu [Nome de Recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (\*) para indicar que a instrução se aplica a todos os recursos.

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

Para obter uma lista dos tipos de recursos do ACM e seus ARNs, consulte [Recursos definidos pelo AWS Certificate Manager](#) na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada recurso, consulte [Ações definidas pelo AWS Certificate Manager](#).

Para visualizar exemplos de políticas baseadas em identidade do ACM, consulte [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#).

## Chaves de condição de políticas para o ACM

Suporta chaves de condição de política específicas de serviço	Sim
---	-----

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem [operadores de condição](#), como “igual a” ou “menor que”, para corresponder a condição da política aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica OR. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos de Política do IAM: Variáveis e Tags](#) no Guia do Usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte [AWSChaves de Contexto de Condição Globais da](#) no Guia do Usuário do IAM.

Para ver uma lista de chaves de condição do ACM, consulte [Chaves de condição do AWS Certificate Manager](#) na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte [Ações definidas pelo AWS Certificate Manager](#).

Para visualizar exemplos de políticas baseadas em identidade do ACM, consulte [Exemplos de políticas baseadas em identidade para o AWS Certificate Manager](#).

## ACLs no ACM

Oferece suporte a ACLs

Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## ABAC com ACM

Oferece suporte a ABAC (tags em políticas)

Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a muitos recursos da AWS. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre a tag no [elemento de condição](#) de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte [O que é ABAC?](#) no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

## Usar credenciais temporárias com o ACM

Oferece suporte a credenciais temporárias	Sim
---	-----

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para informações adicionais, inclusive quais Serviços da AWS funcionam com credenciais temporárias, consulte [Serviços da AWS que Funcionam com o IAM](#) no Guia do Usuário do IAM.

Você estará usando credenciais temporárias se fizer login no AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para uma Função \(Console\)](#) no Guia do Usuário do IAM.

Você pode criar credenciais temporárias de forma manual usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

## Permissões de entidade principal entre serviços para o ACM

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim
--	-----

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você deve ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhamento de sessões de acesso](#).

## Perfis de serviço do ACM

Oferece suporte a perfis de serviço Não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criando um Perfil para Delegar Permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

### Warning

Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do ACM. Edite os perfis de serviço somente quando o ACM orientar você a fazê-lo.

## Funções vinculadas ao serviço para o ACM

Oferece suporte a perfis vinculados ao serviço Sim

Uma função vinculada ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte [AWSServiços que Funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Função Vinculada ao Serviço.. Selecione o link Sim para visualizar a documentação da função vinculada a serviço desse serviço.

## Exemplos de políticas baseadas em identidade para o AWS Certificate Manager

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do ACM. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a AWS API. Para conceder permissões de usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a funções, e os usuários podem assumir as funções.

Saiba como criar uma política baseada em identidade do IAM usando esses exemplos de documento da política JSON consultando [Criando Políticas do IAM](#) no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo ACM, incluindo o formato dos ARNs para cada tipo de recurso, consulte [Ações, recursos e chaves de condição do AWS Certificate Manager](#) na Referência de autorização do serviço.

### Tópicos

- [Melhores práticas de políticas](#)
- [Usar o console do ACM](#)
- [Permitir que usuários visualizem suas próprias permissões](#)
- [Lista de certificados](#)
- [Recuperação de um certificado](#)
- [Importação de um certificado](#)
- [Exclusão de um certificado](#)

### Melhores práticas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do ACM sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usar as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo — para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso. Para obter mais informações, consulte [Políticas Gerenciadas pela AWS](#) ou [AWS Políticas Gerenciadas para Funções de Trabalho](#) no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo — ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e Permissões no IAM](#) no Guia do Usuário do IAM.
- Utilize condições nas políticas do IAM para restringir ainda mais o acesso — você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte [Condição de Elementos de Política JSON do IAM](#) no Guia do Usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM para garantir permissões seguras e funcionais — o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam o idioma de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e ações recomendadas para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de Política do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configurando Acesso à API Protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas Recomendadas de Segurança no IAM](#) no Guia do Usuário do IAM.

## Usar o console do ACM

Para acessar o console do AWS Certificate Manager, você deve ter um conjunto mínimo de permissões. Essas permissões devem autorizar você a listar e visualizar detalhes sobre os recursos na sua Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou funções) com essa política.

Não é necessário conceder permissões mínimas do console para usuários fazendo chamadas somente para AWS CLI ou para a API do AWS. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e perfis ainda possam usar o console do ACM, anexe também a política do ACM *AWSCertificateManagerReadOnly* gerenciada pela AWS às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

## Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
```

```

    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

## Lista de certificados

A política a seguir permite que um usuário liste todos os certificados do ACM na conta do usuário.

```

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

```

### Note

Esta permissão é necessária para que os certificados do ACM apareçam nos consoles do Elastic Load Balancing e do CloudFront.

## Recuperação de um certificado

A política a seguir permite que um usuário recupere um certificado específico do ACM.

```

{

```



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

## Importação de um certificado

A política a seguir permite que um usuário importe um certificado.

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

## Exclusão de um certificado

A política a seguir permite que um usuário exclua um certificado específico do ACM.

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

## Permissões da API do ACM: referência de ações e recursos

Ao configurar o controle de acesso e gravar políticas de permissões que você possa anexar a um usuário ou perfil do IAM, é possível usar a tabela a seguir como referência. A primeira coluna na tabela lista cada operação da API do AWS Certificate Manager. Especifique as ações em um elemento `Action` de política. As colunas remanescentes fornecem informações adicionais:

Você pode usar os elementos de política do IAM em suas políticas do ACM para expressar condições. Para obter uma lista completa, consulte [Chaves disponíveis](#) no Manual do usuário do IAM.

### Note

Para especificar uma ação, use o prefixo `acm:` seguido do nome da operação da API (por exemplo, `acm:RequestCertificate`).

## Permissões e operações da API do ACM

Operações de API do ACM	Permissões obrigatórias (operações de API)	Recursos
<a href="#">AddTagsToCertificate</a>	<code>acm:AddTagsToCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>
<a href="#">DeleteCertificate</a>	<code>acm&gt;DeleteCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>
<a href="#">DescribeCertificate</a>	<code>acm:DescribeCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>
<a href="#">ExportCertificate</a>	<code>acm:ExportCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>
<a href="#">GetAccountConfiguration</a>	<code>acm:GetAccountConfiguration</code>	*
<a href="#">GetCertificate</a>	<code>acm:GetCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>

Operações de API do ACM	Permissões obrigatórias (operações de API)	Recursos
<a href="#">ImportCertificate</a>	acm:ImportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/*  or  *
<a href="#">ListCertificates</a>	acm:ListCertificates	*
<a href="#">ListTagsForCertificate</a>	acm:ListTagsForCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">PutAccountConfiguration</a>	acm:PutAccountConfiguration	*
<a href="#">RemoveTagsFromCertificate</a>	acm:RemoveTagsFromCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">RequestCertificate</a>	acm:RequestCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/*  or  *
<a href="#">ResendValidationEmail</a>	acm:ResendValidationEmail	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">UpdateCertificateOptions</a>	acm:UpdateCertificateOptions	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>

## Políticas gerenciadas pela AWS para o AWS Certificate Manager

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes da AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) no Manual do usuário do IAM.

### AWSCertificateManagerReadOnly

Esta política oferece acesso somente de leitura a certificados do ACM; ela permite que os usuários descrevam, relacionem e recuperem certificados do ACM.

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

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

Para visualizar essa política gerenciada pela AWS no console, vá para <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly>.

## AWSCertificateManagerFullAccess

Esta política fornece acesso total a todos os recursos e ações do ACM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/AWSServiceRoleForCertificateManager*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

```

    }
  ]
}

```

Para visualizar esta política gerenciada pela AWS no console, vá para <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess>.

## Atualizações do ACM para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o ACM desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página [Histórico do documento](#) do ACM.

Alteração	Descrição	Data
Adicionado GetAccountConfiguration suporte para a política <a href="#">AWSCertificateManagerReadOnly</a> .	A política AWSCertificateManagerReadOnly agora inclui permissão para chamar a ação de API GetAccountConfiguration .	3 de março de 2021
O ACM começa a rastrear alterações	O ACM começou a rastrear alterações para suas políticas gerenciadas pela AWS.	3 de março de 2021

## Como usar chaves de condição com o ACM

O AWS Certificate Manager usa [chaves de condição](#) do AWS Identity and Access Management (IAM) para limitar o acesso a solicitações de certificados. Com chaves de condição de políticas do IAM ou políticas de controle de serviços (SCP), é possível criar solicitações de certificado que estejam em conformidade com as diretrizes da sua organização.

**Note**

Combine as chaves de condição do ACM com [chaves de condição globais](#) da AWS, como `aws:PrincipalArn`, para restringir ainda mais as ações a usuários ou perfis específicos.

## Condições compatíveis com o ACM

### Operações da API do ACM e condições compatíveis

Chave de condição	Operações da API do ACM compatíveis	Type	Descrição
<code>acm:ValidationMethod</code>	<a href="#">RequestCertificate</a>	String (EMAIL, DNS)	Filtrar solicitações com base no <a href="#">método de validação</a> do ACM
<code>acm:DomainNames</code>	<a href="#">RequestCertificate</a>	ArrayOfString	Filtro baseado em <a href="#">nomes de domínio</a> na solicitação do ACM
<code>acm:KeyAlgorithm</code>	<a href="#">RequestCertificate</a>	Segmento	Filtrar solicitações com base no <a href="#">algoritmo e no tamanho da chave</a> do ACM
<code>acm:CertificateTransparencyLogging</code>	<a href="#">RequestCertificate</a>	String (ENABLED, DISABLED)	Filtrar solicitações com base na <a href="#">preferência do log de transparência de certificados</a> do ACM
<code>acm:CertificateAuthority</code>	<a href="#">RequestCertificate</a>	ARN	Filtrar solicitações com base nas <a href="#">autoridades</a>

Chave de condição	Operações da API do ACM compatíveis	Type	Descrição
			<a href="#">de certificação</a> na solicitação do ACM

### Exemplo 1: restringir o método de validação

A política a seguir nega novas solicitações de certificado usando o método [Validação por e-mail](#), exceto para uma solicitação feita usando o perfil `arn:aws:iam::123456789012:role/AllowedEmailValidation`.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "acm:RequestCertificate",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "acm:ValidationMethod": "EMAIL"
      },
      "ArnNotLike": {
        "aws:PrincipalArn": [ "arn:aws:iam::123456789012:role/
AllowedEmailValidation" ]
      }
    }
  }
}
```

### Exemplo 2: prevenir domínios curinga

A política a seguir nega qualquer nova solicitação de certificado ACM que use domínios curinga.

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



```

    "Action": "acm:RequestCertificate",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringLike": {
        "acm:DomainNames": [
          "${*}.*"
        ]
      }
    }
  }
}

```

### Exemplo 3: restringir domínios certificados

A política a seguir nega qualquer nova solicitação de certificado ACM que não termine com `*.amazonaws.com`

```

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

```

A política pode ser ainda mais restrita a subdomínios específicos. Essa política só permitiria solicitações em que cada domínio correspondesse a pelo menos um dos nomes de domínio condicionais.

```

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

```

```

    "Effect": "Deny",
    "Action": "acm:RequestCertificate",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringNotLike": {
        "acm:DomainNames": ["support.amazonaws.com", "developer.amazonaws.com"]
      }
    }
  }
}

```

#### Exemplo 4: restringir algoritmo da chave

A política a seguir usa a chave de condição `StringNotLike` para permitir somente certificados solicitados com o algoritmo de chave ECDSA de 384 bits (`EC_secp384r1`).

```

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

```

A política a seguir usa a chave de condição `StringLike` e o curinga `*` para evitar solicitações de novos certificados no ACM com qualquer algoritmo de chave RSA.

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "acm:RequestCertificate",

```

```

    "Resource": "*",
    "Condition": {
      "StringLike": {
        "acm:KeyAlgorithm": "RSA*"
      }
    }
  }
}

```

## Exemplo 5: restringir a autoridade de certificação

A política a seguir só permitiria solicitações de certificados privados usando o ARN da autoridade de certificação privada (PCA) fornecido.

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "acm:RequestCertificate",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "acm:CertificateAuthority": "arn:aws:acm-
pca:region:account:certificate-authority/CA_ID"
      }
    }
  }
}

```

Esta política usa a condição `acm:CertificateAuthority` para permitir somente solicitações de certificados publicamente confiáveis emitidos pela Amazon Trust Services. Configurando o ARN da autoridade de certificação como `false` impede solicitações de certificados privados da PCA.

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "acm:RequestCertificate",

```

```
    "Resource": "*",
    "Condition": {
      "Null" : {
        "acm:CertificateAuthority": "false"
      }
    }
  }
}
```

## Uso de uma função vinculada ao serviço (SLR) com o ACM

AWS Certificate Manager usa uma [função vinculada ao serviço AWS Identity and Access Management](#) (IAM) para permitir renovações automáticas de certificados ACM gerenciados. Uma função vinculada a serviço (SLR) é uma função do IAM que é vinculada diretamente a um serviço do ACM. As SLRs são predefinidas pelo ACM e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

A SLR facilita a configuração do ACM porque você não precisa adicionar manualmente as permissões necessárias para a assinatura automática de certificados. O ACM define as permissões dessa função vinculada ao serviço e, a menos que definido em contrário, somente o ACM pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços que suportam SLRs, consulte [Serviços da AWS compatíveis com o IAM](#) e procure os serviços que contêm Yes (Sim) na coluna Service-Linked Role (Função vinculada ao serviço). Escolha um Yes (Sim) com um link para visualizar a documentação da SLR desse serviço.

### Permissões de SLR para o ACM

O ACM usa uma SLR denominada Política de função de serviço do Amazon Certificate Manager.

A AWSServiceRoleForCertificateManager SLR confia nos seguintes serviços para assumir a função:

- `acm.amazonaws.com`

A política de permissões da função permite que o ACM realize as seguintes ações nos recursos especificados:

- Ações: `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` ativadas ""

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma SLR. Para obter mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

#### Important

O ACM pode alertar você de que não é possível determinar se existe uma SLR na sua conta. Se a necessária permissão do `iam:GetRole` já foi concedida à SLR do ACM para sua conta, o alerta não será repetido depois que a SLR for criada. Se ocorrer novamente, você ou o administrador da conta podem precisar conceder a permissão do `iam:GetRole` ao ACM ou associar sua conta à política `AWSCertificateManagerFullAccess` gerenciada pelo ACM.

## Criação da a SLR para o ACM

Você não precisa criar manualmente a SLR usada pelo ACM. Quando você emite um certificado ACM usando a AWS Management Console AWS CLI, a ou a AWS API, o ACM cria a SLR para você na primeira vez que você escolhe uma CA privada para assinar seu certificado.

Se você encontrar mensagens informando que o ACM não pode determinar se existe uma SLR em sua conta, isso pode significar que sua conta não concedeu a permissão de leitura necessária. CA privada da AWS Isso não impedirá que a SLR seja instalado e você ainda poderá emitir certificados, mas o ACM não poderá renovar os certificados automaticamente até que você resolva o problema. Para ter mais informações, consulte [Problemas com a função vinculada ao serviço \(SLR\) do ACM](#).

#### Important

Essa SLR pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos suportados por essa função. Além disso, se você estava usando o serviço ACM antes de 1º de janeiro de 2017, quando ele começou a oferecer suporte a SLRs, o ACM criou a `AWSServiceRoleForCertificateManager` função em sua conta. Para saber mais, consulte [New Role Appeared in My IAM Account](#).

Se você excluir essa SLR e precisar criá-la novamente, poderá usar um destes métodos:

- No console do IAM, escolha Role, Create role, Certificate Manager para criar uma nova função com o caso de CertificateManagerServiceRolePolicyuso.
- Usando a API IAM [CreateServiceLinkedRole](#) ou o AWS CLI comando correspondente [create-service-linked-role](#), crie uma SLR com o nome do acm.amazonaws.com serviço.

Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

## Criação da SLR para o ACM

O ACM não permite que você edite a função vinculada ao AWSServiceRoleForCertificateManager serviço. Depois que criar uma SLR, você não pode alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Excluindo a SLR para o ACM

Normalmente, você não precisa excluir a AWSServiceRoleForCertificateManager SLR. No entanto, você pode excluir a função manualmente usando o console do IAM, o AWS CLI ou a AWS API. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Regiões suportadas para SLRs do ACM

O ACM suporta o uso de SLRs em todas as regiões em que tanto o ACM quanto CA privada da AWS o ACM estão disponíveis. Para obter mais informações, consulte [AWS Regiões e endpoints](#).

Nome da região	Identidade da região	Suporte no ACM
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
Oeste dos EUA (Norte da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
Ásia-Pacífico (Mumbai)	ap-south-1	Sim

Nome da região	Identidade da região	Suporte no ACM
Ásia-Pacífico (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Zurique)	eu-central-2	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim
Europa (Paris)	eu-west-3	Sim
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	Sim
AWS GovCloud (Leste dos EUA) Leste	us-gov-east-1	Sim

## Solução de problemas de identidade e acesso AWS Certificate Manager

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o ACM e o IAM.

### Tópicos

- [Não tenho autorização para executar uma ação no ACM](#)
- [Não estou autorizado a solicitar um certificado no ACM](#)
- [Não estou autorizado a executar iam:PassRole](#)

- [Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do ACM](#)

## Não tenho autorização para executar uma ação no ACM

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso `my-example-widget` fictício, mas não tem as permissões `acm:GetWidget` fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `acm:GetWidget`.

Se você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a solicitar um certificado no ACM

Se você receber esse erro, o administrador do ACM ou PKI definiu regras que impedem que você solicite o certificado em seu estado atual.

O exemplo de erro a seguir ocorre quando um usuário do IAM tenta usar o console para solicitar um certificado usando opções configuradas com um DENY pelo administrador da organização.

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

Nesse caso, a solicitação deve ser feita novamente de uma forma que esteja de acordo com as políticas definidas pelo administrador. Ou a política precisa ser atualizada para permitir a solicitação do certificado.



## Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o ACM.

Alguns Serviços da AWS permitem que você passe uma função existente para o serviço, em vez de criar uma nova função de serviço ou função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no ACM. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do ACM

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar políticas para conceder às pessoas acesso aos seus recursos.

Saiba mais consultando o seguinte:

- Para saber se o ACM oferece suporte a esses recursos, consulte [Como o AWS Certificate Manager funciona com o IAM](#).
- Saiba como conceder acesso a seus recursos em todos os Contas da AWS pertencentes a você, consulte [Fornecendo Acesso a um Usuário do IAM em Outro Conta da AWS Pertencente a Você](#) no Guia de Usuário do IAM.
- Saiba como conceder acesso a seus recursos para terceiros Contas da AWS consultando [Fornecendo Acesso a Contas da AWS Pertencentes a Terceiros](#) no Guia do Usuário do IAM.

- Saiba como conceder acesso por meio da federação de identidades consultando [Concedendo Acesso a Usuários Autenticados Externamente \(Federação de Identidades\)](#) no Guia do Usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

## Resiliência em AWS Certificate Manager

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

## Segurança da infraestrutura no AWS Certificate Manager

Como serviço gerenciado, AWS Certificate Manager é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o ACM pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

## Conceder permissões de acesso programático ao ACM

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho  (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções da interface que deseja utilizar. <ul style="list-style-type: none"> <li>Para o AWS CLI, consulte <a href="#">Configurando o AWS CLI para uso AWS IAM Identity Center</a> no Guia do AWS Command Line Interface usuário.</li> <li>Para AWS SDKs, ferramentas e AWS APIs, consulte a <a href="#">autenticação do IAM Identity Center no Guia</a> de referência de AWS SDKs e ferramentas.</li> </ul>
IAM	Use credenciais temporárias para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções em <a href="#">Como usar credenciais temporárias com AWS recursos</a> no Guia do usuário do IAM.

Qual usuário precisa de acesso programático?	Para	Por
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. <ul style="list-style-type: none"> <li>• Para isso AWS CLI, consulte <a href="#">Autenticação usando credenciais de usuário do IAM</a> no Guia do AWS Command Line Interface usuário.</li> <li>• Para AWS SDKs e ferramentas, consulte <a href="#">Autenticar usando credenciais de longo prazo</a> no Guia de referência de AWS SDKs e ferramentas.</li> <li>• Para AWS APIs, consulte <a href="#">Gerenciamento de chaves de acesso para usuários do IAM</a> no Guia do usuário do IAM.</li> </ul>

## Práticas recomendadas

As melhores práticas são recomendações que podem ajudar você a usar AWS Certificate Manager (AWS Certificate Manager) com mais eficiência. As melhores práticas a seguir são baseadas em experiência real de clientes atuais do ACM.

### Tópicos

- [AWS CloudFormation](#)
- [Fixação do certificado](#)
- [Validação de domínio](#)
- [Adição ou exclusão de nomes de domínio](#)

- [Cancelamento do registro em log de transparência de certificado](#)
- [Ativar AWS CloudTrail](#)

## AWS CloudFormation

Com AWS CloudFormation você pode criar um modelo que descreva os AWS recursos que você deseja usar. AWS CloudFormation em seguida, provisiona e configura esses recursos para você. AWS CloudFormation pode provisionar recursos que são suportados pelo ACM, como Elastic Load Balancing, Amazon e CloudFront Amazon API Gateway. Para ter mais informações, consulte [Serviços integrados com AWS Certificate Manager](#).

Se você costuma AWS CloudFormation criar e excluir rapidamente vários ambientes de teste, recomendamos que você não crie um certificado ACM separado para cada ambiente. Se fizer isso, você esgotará rapidamente sua cota de certificados. Para ter mais informações, consulte [Cotas](#). Em vez disso, crie um certificado curinga que abranja todos os nomes de domínio que você estiver usando para testes. Por exemplo, se você cria repetidamente certificados do ACM para nomes de domínio que diferem em apenas pelo número de versão, como `<version>.service.example.com`, crie um único certificado-curinga para `<*>.service.example.com`. Inclua o certificado curinga no modelo AWS CloudFormation usado para criar seu ambiente de teste.

## Fixação do certificado

A fixação do certificado, também conhecido como fixação SSL, é um processo que você pode usar em seu aplicativo para validar um host remoto ao associar esse host diretamente com seu certificado X.509 ou chave pública em vez de com uma hierarquia de certificado. O aplicativo, portanto, usa a associação para contornar a validação da cadeia de certificados SSL/TLS. O processo típico de validação do SSL verifica as assinaturas em toda a cadeia de certificados, do certificado da autoridade de certificação (CA) raiz até os certificados da CA subordinada, se houver. Ele também verifica o certificado do host remoto na parte inferior da hierarquia. O aplicativo pode, em vez disso, fazer a fixação do certificado para o host remoto, para informar que apenas esse é um certificado confiável e não o certificado raiz ou qualquer outro na cadeia. Você pode adicionar o certificado do host remoto ou a chave pública a seu aplicativo durante o desenvolvimento. Como alternativa, o aplicativo pode adicionar o certificado ou a chave quando se conecta ao host pela primeira vez.

### Warning

Recomendamos que o seu aplicativo não fixe um certificado do ACM. O ACM executa [Renovação gerenciada para certificados do ACM](#) para renovar automaticamente seus certificados SSL/TLS emitidos pela Amazon antes sua validade expire. Para renovar um certificado, o ACM gera um novo par de chaves pública/privada. Se o seu aplicativo fixar o certificado do ACM e o certificado for renovado com sucesso com uma nova chave pública, o aplicativo talvez não consiga se conectar ao seu domínio.

Se você decidir fazer a fixação de um certificado, as opções a seguir não impedirão que o aplicativo se conecte ao seu domínio:

- [Importe o seu próprio certificado](#) para o ACM e, em seguida, fixe seu aplicativo no certificado importado. O ACM não tenta renovar automaticamente certificados importados.
- Se você estiver usando um certificado público, fixe o aplicativo a todos os [certificados raiz da Amazon](#) disponíveis. Se você estiver usando um certificado privado, fixe o aplicativo ao certificado raiz da CA.

## Validação de domínio

Antes que a autoridade de certificação (CA) da Amazon possa emitir um certificado para seu site, AWS Certificate Manager (ACM) deve verificar se você possui ou controla todos os domínios que você especificou em sua solicitação. Você pode executar uma verificação usando o e-mail ou o DNS. Para ter mais informações, consulte [Validação por DNS](#) e [Validação de e-mail](#).

## Adição ou exclusão de nomes de domínio

Você não pode adicionar nem remover nomes de domínio de um certificado do ACM existente. Em vez disso, você deve solicitar um novo certificado com a lista revisada de nomes de domínio. Por exemplo, se seu certificado tiver cinco nomes de domínio e você desejar adicionar mais quatro, deverá solicitar um novo certificado com todos os nove nomes de domínio. Assim como com qualquer novo certificado, você deve validar a propriedade de todos os nomes de domínio na solicitação, incluindo nomes previamente validados no certificado original.

Se usar a validação de e-mail, você receberá até oito mensagens de e-mail de validação para cada domínio, e pelo menos uma delas deverá ser respondida em 72 horas. Por exemplo, quando solicita um certificado com cinco nomes de domínio, você recebe até 40 mensagens de e-mail de validação,

e pelo menos cinco delas devem ser respondidas em 72 horas. À medida que o número de nomes de domínio na solicitação de certificado aumenta, o trabalho necessário para validar a propriedade dos domínios por e-mail também aumenta.

Se você usar a validação por DNS, deverá gravar um novo registro de DNS no banco de dados para o FQDN que deseja validar. O ACM envia o registro a ser criado e, posteriormente, consulta o banco de dados para determinar se o registro foi adicionado. A adição do registro confirma que você possui ou controla o domínio. No exemplo anterior, ao solicitar um certificado com cinco nomes de domínio, você deve criar cinco registros de DNS. Recomendamos usar a validação de DNS, quando possível.

## Cancelamento do registro em log de transparência de certificado

### Important

Independentemente das ações executadas para excluir o registro em log de transparência de certificado, seu certificado ainda pode ser registrado por qualquer cliente ou indivíduo que tenha acesso ao endpoint público ou privado ao qual você associa o certificado. Porém, o certificado não conterá um carimbo de data/hora de certificado (SCT) assinado. Apenas a CA emissora pode incorporar um SCT em um certificado.

Desde 30 de abril de 2018, o Google Chrome não confia mais em certificados SSL/TLS públicos não registrados em um log de transparência de certificados. Portanto, desde 24 de abril de 2018, a CA da Amazon começou a publicar todos os novos certificados e as renovações em pelo menos dois logs públicos. Após o registro de um certificado, ele não pode ser removido. Para ter mais informações, consulte [Registro de transparência de certificados](#).

O registro em log é realizado automaticamente ao solicitar um certificado ou quando ele é renovado, mas é possível cancelar essa opção. Os motivos comuns para essa escolha incluem preocupações sobre segurança e privacidade. Por exemplo, o registro de nomes de domínio internos do host fornece a possíveis invasores informações sobre redes internas não seriam públicas de outra forma. Além disso, podem vazarem nomes de produtos e sites novos ou ainda não lançados.

Para desativar o registro de transparência ao solicitar um certificado, use o `options` parâmetro do AWS CLI comando [request-certificate](#) ou da operação da [RequestCertificate](#) API. Se seu certificado foi emitido antes de 24 de abril de 2018 e você deseja garantir que ele não seja registrado durante a renovação, você pode usar o [update-certificate-options](#) comando ou a operação da [UpdateCertificateOptions](#) API para optar por não participar.

## Limitações

- Não é possível usar o console para habilitar ou desabilitar o registro em log de transparência.
- Não é possível alterar o status de registro após um certificado entrar em seu período de renovação, geralmente 60 dias antes da expiração da validade do certificado. Nenhuma mensagem de erro é gerada se uma alteração de status falhar.

Após o registro de um certificado, ele não pode ser removido do log. O cancelamento depois disso não terá efeito. Se você cancelar o registro ao solicitar um certificado e depois optar por incluí-lo novamente, seu certificado não será registrada enquanto não for renovado. Se você quiser que o certificado seja registrado imediatamente, recomendamos que emita um novo.

O exemplo a seguir mostra como usar o comando [request-certificate](#) para desabilitar a transparência do certificado ao solicitar um novo certificado.

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

```

O comando anterior gera o ARN do seu novo certificado.

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

Se você já tem um certificado e não quer que ele seja registrado quando for renovado, use o [update-certificate-options](#) comando. Esse comando não retorna um valor.

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

## Ativar AWS CloudTrail

Ative o CloudTrail registro antes de começar a usar o ACM. CloudTrail permite que você monitore suas AWS implantações recuperando um histórico de chamadas de AWS API para sua conta,



incluindo chamadas de API feitas por meio do AWS Management Console, dos AWS SDKs, do e da Amazon Web AWS Command Line Interface Services de nível superior. Você também pode identificar quais usuários e contas chamaram as APIs do ACM, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Você pode se CloudTrail integrar aos aplicativos usando a API, automatizar a criação de trilhas para sua organização, verificar o status de suas trilhas e controlar como os administradores ativam e desativam o CloudTrail login. Para obter mais informações, consulte [Criação de uma trilha](#). Vá para [Usando CloudTrail com AWS Certificate Manager](#) para ver exemplos de trilhas para ações do ACM.

# Configuração

Com o AWS Certificate Manager (ACM), você pode provisionar e gerenciar certificados SSL/TLS para seus sites e aplicações baseados na AWS. Você usa o ACM para criar ou importar e, em seguida, gerenciar um certificado. Você deve usar outros serviços da AWS para implantar o certificado no seu site ou aplicativo. Para obter mais informações sobre os serviços integrados com o ACM, consulte [Serviços integrados com AWS Certificate Manager](#). Os tópicos a seguir discutem as etapas que você precisa desempenhar antes de usar o ACM.

## Tópicos

- [Cadastrar-se em uma Conta da AWS](#)
- [Criar um usuário administrativo](#)
- [Registrar um nome de domínio](#)
- [\(Opcional\) Configurar e-mail para seu domínio](#)
- [\(Opcional\) Configurar um registro de CAA](#)

## Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

Parte do procedimento de aplicação envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, [atribua acesso administrativo a um usuário administrativo](#) e use somente o usuário raiz para realizar as [tarefas que exigem acesso do usuário raiz](#).

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando <https://aws.amazon.com/> e selecionando Minha conta.

## Criar um usuário administrativo

Depois de se inscrever em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

### Proteger seu Usuário raiz da conta da AWS

1. Faça login no [AWS Management Console](#) como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua senha.

Para obter ajuda ao fazer login usando o usuário raiz, consulte [Fazer login como usuário raiz](#) no Guia do usuário do Início de Sessão da AWS.

2. Ative a autenticação multifator (MFA) para o usuário raiz.

Para obter instruções, consulte [Habilitar um dispositivo MFA virtual para o usuário raiz de sua conta da Conta da AWS para seu \(console\)](#) no Guia do usuário do IAM.

### Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte [Enabling AWS IAM Identity Center](#) no Manual do Usuário do AWS IAM Identity Center.

2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configure user access with the default Diretório do Centro de Identidade do IAM](#) no Manual do Usuário do AWS IAM Identity Center.

### Login como usuário administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte [Fazer login no portal de acesso da AWS](#), no Guia do usuário do Início de Sessão da AWS.

## Registrar um nome de domínio

Um nome de domínio totalmente qualificado (FQDN) é o nome exclusivo de uma organização ou indivíduo na Internet seguido por uma extensão de domínio de nível superior, como .com ou .org. Se não tiver um nome de domínio registrado, você pode registrar um por meio do Amazon Route 53 ou de dezenas de outros registradores comerciais. Normalmente você acessa o site do registrador e solicita um nome de domínio. O registrador consulta o WHOIS para determinar se o FQDN solicitado está disponível. Se estiver, o registrador geralmente lista os nomes relacionados que diferem por extensão de domínio e lhe dá uma oportunidade de adquirir qualquer um dos nomes disponíveis. O registro geralmente dura por um período determinado, como um ou dois anos, e deve ser renovado antes do término desse período.

Para obter mais informações sobre o registro de nomes de domínio com o Amazon Route 53, consulte [Registro de nomes de domínio usando o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

### (Opcional) Configurar e-mail para seu domínio

#### Note

As etapas a seguir são necessárias apenas se você usar validação por e-mail para confirmar que possui ou controla o FQDN (nome de domínio totalmente qualificado) especificado na solicitação do certificado. O ACM exige que você valide propriedade ou controle antes de emitir um certificado. Você pode usar a validação de e-mail ou a validação de DNS. Para obter mais informações sobre a validação de e-mail, consulte [Validação de e-mail](#). Se você puder editar sua configuração de DNS, recomendamos usar a validação de domínio de DNS, em vez da validação de e-mail. A validação de DNS elimina a necessidade de configurar um e-mail para o nome do domínio. Para obter mais informações sobre a validação de DNS, consulte [Validação por DNS](#).

Use o site de seu registrador para associar seus endereços de contato a seu nome de domínio. O registrador adiciona os endereços de e-mail dos contatos no banco de dados WHOIS e adiciona um ou mais servidores de e-mail aos registros do servidor de mensagens (MX) de um servidor DNS. Se você optar por usar a validação de e-mail, o ACM enviará um e-mail aos endereços de contato e a cinco endereços administrativos comuns formados em seu registro MX. O ACM envia até oito mensagens de e-mail de validação toda vez que você cria um novo certificado, renova um certificado

ou solicita um novo e-mail de validação. O e-mail de validação contém instruções para confirmar que o proprietário do domínio ou um representante designado aprova o certificado do ACM. Para ter mais informações, consulte [Validação de e-mail](#). Se você tiver problemas com o e-mail de validação, consulte [Solução de problemas de validação de e-mail](#).

## Banco de dados WHOIS

O banco de dados WHOIS contém informações de contato para o seu domínio. Para validar sua identidade, o ACM envia um e-mail para os seguintes três endereços no WHOIS. Você deve ter certeza de que suas informações de contato são públicas ou de que os e-mails enviados para um endereço oculto é encaminhado para o seu endereço de e-mail real.

- Domínio registrado
- Contato técnico
- Contato administrativo

## MX record (Registro MX)

Quando você registrar seu domínio, o registrador enviará o registro MX (mail exchanger) a um servidor Domain Name System (DNS). Um registro MX indica quais servidores aceitam e-mail para o seu domínio. O registro contém um nome de domínio totalmente qualificado (FQDN). Você pode solicitar um certificado para domínios apex ou subdomínios.

Por exemplo, se você usar o console para solicitar um certificado para `abc.xyz.exemplo.com`, o ACM primeiro tenta encontrar o registro MX para esse subdomínio. Se o registro não puder ser encontrado, o ACM executa uma consulta de MX para `xyz.exemplo.com`. Se o registro não puder ser encontrado, o ACM executa uma consulta de MX para `exemplo.com`. Se o registro não puder ser encontrado ou se não houver nenhum registro MX, o ACM escolherá o domínio original para o qual o certificado foi solicitado (`abc.xyz.exemplo.com` neste exemplo). O ACM envia e-mail aos seguintes cinco endereços de administração comuns do sistema do domínio ou do subdomínio:

- `administrator@your_domain_name`
- `hostmaster@your_domain_name`
- `postmaster@your_domain_name`
- `webmaster@your_domain_name`
- `admin@your_domain_name`

**Tip**

Você pode substituir o domínio para o qual suas mensagens de validação são enviadas. Se você usa a operação de [ResendValidationEmail](#)API ou o [resend-validation-email](#)AWS CLI comando, AWS não executa uma pesquisa MX. Em vez disso, você fornecerá o nome do domínio registrado e o nome de um domínio de validação personalizado, e a AWS enviará as cinco mensagens de e-mail anteriores ao domínio de validação e não ao seu domínio registrado.

O ACM sempre envia e-mails de validação aos cinco endereços comuns listados anteriormente, quer você esteja usando o console, a API ou a AWS CLI. No entanto, a AWS executa uma consulta de MX somente quando você usa o console para solicitar um certificado.

Se você não receber o e-mail de validação, consulte [E-mail de validação não recebido](#) para obter informações sobre as possíveis causas e soluções.

## (Opcional) Configurar um registro de CAA

Opcionalmente, você pode configurar um registro DNS de Autorização da autoridade de certificação (CAA) para especificar que o AWS Certificate Manager (ACM) tem permissão para emitir um certificado para seu domínio ou subdomínio. Após validar seu domínio, o ACM verifica a presença de registros de CAA para ter certeza de que pode emitir um certificado para você. Você pode optar por não configurar um registro de CAA para seu domínio se não quiser habilitar a verificação de CAA.

Um registro de CAA contém os seguintes campos de dados:

### flags

Especifica se o valor do campo tag é suportado pelo ACM. Defina este valor como 0.

### conteúdo

O campo tag pode ter um dos seguintes valores. Observe que o campo iodef é ignorado no momento.

### issue

Indica que a CA do ACM que você especifica no campo value (valor) está autorizada a emitir um certificado para seu domínio ou subdomínio.

## issuewild

Indica que a CA do ACM que você especificou no campo value (valor) está autorizada a emitir um certificado-curinga para seu domínio ou subdomínio. Um certificado curinga se aplica ao domínio ou subdomínio e a todos os seus subdomínios.

## value

O valor deste campo depende do valor do campo tag. Você deve colocar esse valor entre aspas ("").

### Quando a tag for issue

O campo value contém o nome de domínio da CA. Esse campo pode conter o nome de uma CA que não seja uma CA da Amazon. No entanto, se você não tiver um registro de CAA que especifique uma das quatro CAs da Amazon a seguir, o ACM não pode emitir um certificado para seu domínio ou subdomínio:

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

O campo value também pode conter um ponto e vírgula (;) para indicar que nenhuma CA deve ter permissão para emitir um certificado para seu domínio ou subdomínio. Use este campo se decidir em algum momento que você não deseja mais um certificado emitido para um determinado domínio.

### Quando a tag for issuewild

O campo value será o mesmo para quando a tag for issue, exceto pelo fato de que o valor se aplica a certificados curinga.

Quando há um registro de CAA issuewild presente que não inclui um valor de CA do ACM, nenhum curinga pode ser emitido pelo ACM. Se não houver issuewild presente, mas houver um registro issue da CAA para o ACM, os curingas poderão ser emitidos pelo ACM.

## Example Exemplo de registros de CAA

Nos exemplos a seguir, seu nome de domínio é fornecido primeiro e seguido pelo tipo de registro (CAA). O campo flags é sempre 0. O campo tags pode ser issue ou issuewild. Se o campo for issue

e você digitar o nome de domínio de um servidor CA no campo value, o registro de CAA indicará que o servidor especificado tem permissão para enviar o certificado solicitado. Se você digitar um ponto e vírgula ";" no campo value, o registro de CAA indicará que nenhuma CA tem permissão para emitir um certificado. A configuração dos registros de CAA varia de acordo com o provedor DNS.

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

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

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

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

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

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

Para obter mais informações sobre como adicionar ou modificar registros de DNS, verifique com seu provedor de DNS. O Route 53 suporta registros de CAA. Se o Route 53 for seu provedor de DNS, consulte [Formato de CAA](#) para obter mais informações sobre como criar um registro.



# Emissão e gerenciamento certificados

Os certificados do ACM podem ser usados para estabelecer comunicações seguras na internet ou em uma rede interna. É possível solicitar um certificado publicamente confiável diretamente do ACM ("certificado do ACM") ou importar um certificado publicamente confiável emitido por terceiros. Certificados autoassinados também são suportados. Para provisionar a PKI interna da sua organização, é possível emitir certificados do ACM assinados por uma autoridade de certificação privada (CA) criada e gerenciada pela [CA privada da AWS](#). A CA pode residir em sua conta ou ser compartilhada com você por uma outra conta.

## Note

Certificados públicos do ACM podem ser instalados em instâncias do Amazon EC2 conectadas a um [Nitro Enclave](#), mas não a outras instâncias do Amazon EC2. Para obter informações sobre como configurar um servidor Web independente em uma instância do Amazon EC2 não conectada a um Nitro Enclave, consulte [Tutorial: Instalar um servidor Web LAMP no Amazon Linux 2](#) ou [Tutorial: Instalar um servidor Web LAMP com o Amazon Linux AMI](#).

## Note

Como os certificados assinados por uma CA privada não são confiáveis por padrão, os administradores devem instalá-los em armazenamentos de confiança do cliente.

[Para começar a emitir certificados, entre no AWS Management Console e abra o console do ACM em <https://console.aws.amazon.com/acm/home>](#). Se a página introdutória for exibida, escolha Get Started (Iniciar). Caso contrário, escolha Certificate Manager (Gerenciador de certificados) ou Private CAs (CAs privadas) no painel de navegação à esquerda.

## Tópicos

- [Solicitação de um certificado público](#)
- [Como solicitar um certificado de PKI privado](#)
- [Validação da propriedade de domínios](#)
- [Lista dos certificados gerenciados pelo ACM](#)

- [Descrição dos certificados do ACM](#)
- [Exclusão dos certificados gerenciados pelo ACM](#)
- [Instalando certificados do ACM;](#)

## Solicitação de um certificado público

As seções a seguir discutem como usar o console do ACM ou AWS CLI solicitar um certificado público do ACM. Após solicitar um certificado público, você deverá concluir um dos procedimentos descritos em [Validação da propriedade de domínios](#).

Os certificados públicos do ACM seguem o padrão X.509 e estão sujeitos às seguintes restrições:

- Nomes: você deve usar nomes de assunto compatíveis com DNS. Para ter mais informações, consulte [Nomes de domínio](#).
- Algoritmo: Para criptografia, o algoritmo de chave privada do certificado deve ser RSA de 2.048 bits, ECDSA de 256 bits ou ECDSA de 384 bits.
- Expiração: cada certificado é válido por 13 meses (395 dias).
- Renovação: o ACM tenta renovar um certificado privado automaticamente após 11 meses.

Se você tiver problemas ao solicitar um certificado, consulte [Solução de problemas de solicitações de certificado](#).

Para solicitar um certificado para usar uma PKI privada CA privada da AWS, consulte [Como solicitar um certificado de PKI privado](#).

### Note

Os administradores podem usar [políticas de chaves condicionais](#) do ACM para controlar como os usuários finais emitem novos certificados. Essas chaves condicionais permitem que restrições sejam colocadas em domínios, métodos de validação e outros atributos relacionados a uma solicitação de certificado.

### Note

Certificados publicamente confiáveis do ACM serão registrados automaticamente em pelo menos dois bancos de dados de transparência de certificados, a menos que você

cancela essa opção. No momento, não é possível usar o console para cancelar. Você deve usar o AWS CLI ou a API do ACM. Para ter mais informações, consulte [Cancelamento do registro em log de transparência de certificado](#). Para obter informações gerais sobre logs de transparência, consulte [Registro de transparência de certificados](#).

## Tópicos

- [Solicitar um certificado público usando o console](#)
- [Solicitar um certificado público usando a CLI](#)

## Solicitar um certificado público usando o console

Para solicitar um certificado público do ACM (console)

1. Faça login no AWS Management Console e abra o console do ACM em <https://console.aws.amazon.com/acm/home>.

Selecione Request a certificate.

2. Na seção Domain names (Nomes de domínio), digite seu nome de domínio.

É possível usar um nome de domínio totalmente qualificado (FQDN), como **www.example.com** ou um nome de domínio vazio ou apex, como **example.com**. Você também pode usar um asterisco (\*) como um caractere curinga na posição mais à esquerda para proteger vários nomes de site no mesmo domínio. Por exemplo, **\*.example.com** protege **corp.example.com** e **images.example.com**. O nome-curinga será exibido no campo Subject (Assunto) e na extensão Subject Alternative Name (Nome alternativo do assunto) do certificado do ACM.

Quando você solicita um certificado-curinga, o asterisco (\*) deve estar na posição mais à esquerda do nome do domínio e só pode proteger um nível de subdomínio. Por exemplo, o **\*.example.com** pode proteger **login.example.com** e **test.example.com** mas não consegue proteger **test.login.example.com**. Note também que **\*.example.com** protege apenas os subdomínios de **example.com**, ele não protege o domínio vazio ou apex (**example.com**). Para proteger ambos, consulte a próxima etapa.

**Note**

Em conformidade com o [RFC 5280](#), o tamanho do nome de domínio (tecnicamente, o Nome Comum) inserido nesta etapa não pode exceder 64 octetos (caracteres), incluindo pontos. Cada Subject Alternative Name (SAN - Nome alternativo de unidade) subsequente que você fornecer, como na próxima etapa, pode ter até 253 octetos.

Para adicionar outro nome, escolha Add another name to this certificate (Adicionar outro nome a este certificado) e digite o nome na caixa de texto. Isso é útil para proteger tanto o domínio vazio ou apex (como **example.com**) e seus subdomínios (**\*.example.com**).

3. Na seção Validation method (Método de validação), escolha DNS validation - recommended (Validação por DNS - recomendado) ou Email validation (Validação por e-mail), dependendo das suas necessidades.

**Note**

Se você puder editar sua configuração de DNS, recomendamos usar a validação de domínio de DNS, em vez da validação de e-mail. A validação de DNS tem vários benefícios em relação à validação de e-mail. Consulte [Validação por DNS](#).

Para que o ACM emita um certificado, ele valida se você possui ou controla os nomes de domínio em sua solicitação de certificado. Você pode usar a validação de e-mail ou a validação de DNS.

Se você escolher a validação por e-mail, o ACM enviará um e-mail de validação para três endereços de contato registrados no banco de dados WHOIS e para até cinco endereços comuns de administração do sistema para cada nome de domínio. Você ou um representante autorizado deve responder a uma dessas mensagens de e-mail. Para ter mais informações, consulte [Validação de e-mail](#).

Se você usa a validação por DNS, basta adicionar um registro CNAME fornecido pelo ACM em sua configuração de DNS. Para obter mais informações sobre a validação de DNS, consulte [Validação por DNS](#).

4. Na seção Algoritmo chave, escolha um dos três algoritmos disponíveis:

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

Para obter informações para ajudá-lo a escolher um algoritmo, consulte [Algoritmos-chave](#) a postagem do AWS blog [Como avaliar e usar certificados ECDSA em](#). AWS Certificate Manager

5. Na página Tags (Etiquetas), é possível marcar seu certificado. As tags são pares de valores-chave que servem como metadados para identificar e organizar recursos. AWS Para obter uma lista de parâmetros de tag do ACM e instruções sobre como adicionar tags a certificados após a criação, consulte [Marcação de certificados do AWS Certificate Manager](#).

Ao terminar de adicionar etiquetas, escolha Request (Solicitar).

6. Depois que a solicitação for processada, o console retornará à sua lista de certificados, onde informações sobre o novo certificado serão exibidas.

Um certificado entra no status Pending validation (Validação pendente) mediante solicitação, a menos que falhe por qualquer um dos motivos indicados no tópico de solução de problemas [Falha na solicitação do certificado](#). O ACM faz repetidas tentativas de validar um certificado por 72 horas até atingir o tempo limite. Se um certificado mostrar o status Failed (Com falha) ou Validation timed out (Tempo limite da validação excedido), exclua a solicitação, corrija o problema com [DNS validation](#) (Validação por DNS) ou [Email validation](#) (Validação por e-mail) e tente novamente. Se a validação for bem-sucedida, o certificado entrará no status Issued (Emitido).

#### Note

Dependendo de como tiver ordenado a lista, talvez o certificado procurado não esteja imediatamente visível. Você pode clicar no triângulo preto à direita para alterar a ordem. Também é possível navegar por várias páginas de certificados usando os números de página no canto superior direito.

## Solicitar um certificado público usando a CLI

Use o comando [request-certificate](#) para solicitar um novo certificado público do ACM na linha de comando. Os valores opcionais para o método de validação são DNS e EMAIL. Os valores

opcionais para o algoritmo de chave são RSA\_2048 (o padrão se o parâmetro não for fornecido explicitamente), EC\_prime256v1 e EC\_secp384r1.

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

Esse comando gera o nome de recurso da Amazon (ARN) do seu novo certificado público.

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

## Como solicitar um certificado de PKI privado

Se você tiver acesso a uma CA privada existente criada por CA privada da AWS, o ACM poderá solicitar um certificado adequado para uso em sua PKI privada. A CA pode residir em sua conta ou ser compartilhada com você por uma outra conta. Para obter informações sobre como criar uma CA privada, consulte [Criar uma Autoridade de certificação privada](#).

Os certificados assinados por uma CA privada não são confiáveis por padrão, e o ACM não oferece suporte a nenhuma forma de validação para eles. Conseqüentemente, um administrador deve tomar medidas para instalá-los nos armazenamentos de confiança de clientes de sua organização.

Os certificados privados do ACM seguem o padrão X.509 e estão sujeitos às seguintes restrições:

- Nomes: você deve usar nomes de assunto compatíveis com DNS. Para ter mais informações, consulte [Nomes de domínio](#).
- Algoritmo: Para criptografia, o algoritmo de chave privada do certificado deve ser RSA de 2.048 bits, ECDSA de 256 bits ou ECDSA de 384 bits.

### Note

A família especificada de algoritmos de assinatura (RSA ou ECDSA) deve corresponder à família de algoritmos da chave secreta da CA.

- **Expiração:** cada certificado é válido por 13 meses (395 dias). A data de término do certificado CA de assinatura deve exceder a data de término do certificado solicitado, caso contrário, a solicitação de certificado falhará.
- **Renovação:** o ACM tenta renovar um certificado privado automaticamente após 11 meses.

A CA privada usada para assinar os certificados da entidade final está sujeita às suas próprias restrições:

- A CA deve ter o status de ativo.
- O algoritmo de chave privada dela deve ser RSA 2048 ou RSA 4096.

#### Note

Ao contrário de certificados publicamente confiáveis, certificados assinados por uma CA privada não requerem validação.

## Tópicos

- [Configuração de acesso a uma CA privada](#)
- [Solicitar um certificado de PKI privado usando o console do ACM](#)
- [Solicitar um certificado de PKI privado usando a CLI](#)

## Configuração de acesso a uma CA privada

Você pode usar CA privada da AWS para assinar seus certificados ACM em um dos dois casos:

- **Conta única:** a CA de assinatura e o certificado ACM emitido residem na mesma AWS conta.

Para ativar a emissão e as renovações de uma única conta, o administrador da CA privada da AWS deve conceder permissão à entidade principal do serviço do ACM para criar, recuperar e listar certificados. Isso é feito usando a ação da CA privada da AWS API [CreatePermission](#) ou o AWS CLI comando [create-permission](#). O proprietário da conta atribui essas permissões a um usuário, grupo ou perfil do IAM responsável pela emissão dos certificados.

- **Conta cruzada:** a CA de assinatura e o certificado ACM emitido residem em AWS contas diferentes, e o acesso à CA foi concedido à conta em que o certificado reside.

[Para permitir a emissão e renovações entre contas, o CA privada da AWS administrador deve anexar uma política baseada em recursos à CA usando a ação PutPolicy da CA privada da AWS API ou o comando put-policy. AWS CLI](#) A política especifica as entidades primárias em outras contas que têm permissão de acesso limitado à CA. Para obter mais informações, consulte [Uso de uma política baseada em recursos com o ACM Private CA.](#)

O cenário intercontas também exige que o ACM configure uma função vinculada ao serviço (SLR) para interagir com a política de PCA como entidade primária. O ACM cria a SLR automaticamente ao emitir o primeiro certificado.

O ACM pode alertar você de que não é possível determinar se existe uma SLR na sua conta. Se a necessária permissão do `iam:GetRole` já foi concedida à SLR do ACM para sua conta, o alerta não será repetido depois que a SLR for criada. Se ocorrer novamente, você ou o administrador da conta podem precisar conceder a permissão do `iam:GetRole` ao ACM ou associar sua conta à política gerenciada pelo ACM `AWSCertificateManagerFullAccess`.

Para obter mais informações, consulte [usando uma função vinculada ao serviço com o ACM.](#)

#### Important

Seu certificado ACM deve estar ativamente associado a um AWS serviço suportado antes de ser renovado automaticamente. Para obter informações sobre os recursos que o ACM suporta, consulte [Serviços integrados com AWS Certificate Manager.](#)


## Solicitar um certificado de PKI privado usando o console do ACM

1. Faça login no AWS Management Console e abra o console do ACM em <https://console.aws.amazon.com/acm/home>.  
Selecione Request a certificate.
2. Na página Request certificate (Solicitar certificado), escolha Request a private certificate (Solicitar um certificado privado) e Next (Próximo) para continuar.
3. Na seção Certificate authority details (Detalhes da autoridade de certificação), clique no menu Certificate authority (Autoridade de certificação) e escolha uma das CAs privadas disponíveis. Se a CA for compartilhada de outra conta, o ARN será precedido de informações de propriedade.



Os seguintes detalhes sobre a CA são exibidos para ajudar você a verificar se escolheu a CA correta:

- Proprietário
  - Tipo
  - Nome comum (CN)
  - Organização (O)
  - Unidade organizacional (OU)
  - Nome do país (C)
  - Estado ou província
  - Nome da localidade
4. Na seção Domain names (Nomes de domínio), digite seu nome de domínio. É possível usar um nome de domínio totalmente qualificado (FQDN), como **www.example.com** ou um nome de domínio vazio ou apex, como **example.com**. Você também pode usar um asterisco (\*) como um caractere curinga na posição mais à esquerda para proteger vários nomes de site no mesmo domínio. Por exemplo, **\*.example.com** protege **corp.example.com** e **images.example.com**. O nome-curinga será exibido no campo Subject (Assunto) e na extensão Subject Alternative Name (Nome alternativo do assunto) do certificado do ACM.

 Note

Quando você solicita um certificado-curinga, o asterisco (\*) deve estar na posição mais à esquerda do nome do domínio e só pode proteger um nível de subdomínio. Por exemplo, o **\*.example.com** pode proteger **login.example.com** e **test.example.com** mas não consegue proteger **test.login.example.com**. Note também que **\*.example.com** protege apenas os subdomínios de **example.com**, ele não protege o domínio vazio ou apex (**example.com**). Para proteger ambos, consulte a próxima etapa

Opcionalmente, escolha Add another name to this certificate (Adicionar outro nome a este certificado) e digite o nome na caixa de texto. Isso é útil para autenticar tanto um domínio vazio ou apex (como **example.com**) e seus subdomínios (como **\*.example.com**).

5. Na seção Algoritmo chave, escolha um dos três algoritmos disponíveis:

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

Para obter informações que ajudem você a escolher um algoritmo, consulte [Algoritmos-chave](#).

6. Na seção Tags (Etiquetas), é possível marcar seu certificado opcionalmente. As tags são pares de valores-chave que servem como metadados para identificar e organizar recursos. AWS Para obter uma lista de parâmetros de tag do ACM e instruções sobre como adicionar tags a certificados após a criação, consulte [Marcação de certificados do AWS Certificate Manager](#).
7. Na seção Certificate renewal permissions (Permissões de renovação de certificado), confirme o aviso sobre permissões de renovação de certificado. Essas permissões permitem a renovação automática de certificados de PKI privados que você assina com a CA selecionada. Para obter mais informações, consulte [usando uma função vinculada ao serviço com o ACM](#).
8. Após fornecer todas as informações necessárias, clique em Request (Solicitar). O console retorna para a lista de certificados, na qual você pode visualizar seu novo certificado.

#### Note

Dependendo de como tiver ordenado a lista, talvez o certificado procurado não esteja imediatamente visível. Você pode clicar no triângulo preto à direita para alterar a ordem. Também é possível navegar por várias páginas de certificados usando os números de página no canto superior direito.

## Solicitar um certificado de PKI privado usando a CLI

Use o comando [request-certificate](#) para solicitar um certificado privado no ACM.

#### Note

Quando você solicita um certificado PKI privado assinado por uma CA AWS Private CA, a família de algoritmos de assinatura especificada (RSA ou ECDSA) deve corresponder à família de algoritmos da chave secreta da CA.

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

Esse comando gera o nome de recurso da Amazon (ARN) do seu novo certificado privado.

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

Na maioria dos casos, o ACM anexa automaticamente uma função vinculada ao serviço (SLR) à sua conta na primeira vez que você usa uma CA compartilhada. O SLR permite a renovação automática de certificados de entidade final que você emite. Para verificar se o SLR está presente, você pode consultar o IAM com o seguinte comando:

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

Se o SLR estiver presente, a saída do comando deve ser semelhante à seguinte:

```
{  
  "Role":{  
    "Path":"/aws-service-role/acm.amazonaws.com/",  
    "RoleName":"AWSServiceRoleForCertificateManager",  
    "RoleId":"AAAAAAAA00000000BBBBBBBB",  
    "Arn":"arn:aws:iam::{account_no}:role/aws-service-role/acm.amazonaws.com/  
AWSServiceRoleForCertificateManager",  
    "CreateDate":"2020-08-01T23:10:41Z",  
    "AssumeRolePolicyDocument":{  
      "Version":"2012-10-17",  
      "Statement":[  
        {  
          "Effect":"Allow",  
          "Principal":{  
            "Service":"acm.amazonaws.com"  
          },  
          "Action":"sts:AssumeRole"  
        }  
      ]  
    },  
  },  
}
```

```
"Description": "SLR for ACM Service for accessing cross-account Private CA",
"MaxSessionDuration": 3600,
"RoleLastUsed": {
  "LastUsedDate": "2020-08-01T23:11:04Z",
  "Region": "ap-southeast-1"
}
}
```

Se a SLR estiver ausente, consulte [Uso de uma função vinculada ao serviço com o ACM](#).

## Validação da propriedade de domínios

Antes que a autoridade de certificação (CA) da Amazon possa emitir um certificado para seu site, o AWS Certificate Manager (ACM) deve comprovar que você possui ou controla todos os nomes de domínio especificados na sua solicitação. Você pode optar por provar sua propriedade com a validação por Sistema de Nomes de Domínio (DNS) ou com validação por e-mail no momento em que solicitar um certificado.

### Note

A validação aplica-se apenas a certificados publicamente confiáveis emitidos pelo ACM. O ACM não valida a propriedade do domínio para [certificados importados](#) nem para certificados assinados por uma CA privada. O ACM não pode validar recursos em uma [zona hospedada privada](#) do Amazon VPC em ou qualquer outro domínio privado. Para ter mais informações, consulte [Solução de problemas de validação de certificado](#).

Em geral, recomendamos o uso da validação por DNS em vez da validação por e-mail pelos seguintes motivos:

- Se você usa o Amazon Route 53 para gerenciar seus registros de DNS públicos, poderá atualizar seus registros diretamente por meio do ACM.
- O ACM renova seu certificado validado por DNS automaticamente, desde que o certificado esteja em uso e o registro do DNS esteja em vigor.
- Para serem renovados, os certificados validados por e-mail exigem uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação 45 dias antes do prazo de validade. Esses avisos vão para os endereços de caixa de correio WHOIS do domínio e para até cinco endereços

comuns de administrador. As notificações contêm um link no qual o proprietário do domínio pode clicar para facilitar a renovação. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

Se não tiver autorização para editar o banco de dados de DNS do seu domínio, você deve usar a [validação por e-mail](#) em seu lugar.

#### Note

Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS.

### Tópicos

- [Validação por DNS](#)
- [Validação de e-mail](#)

## Validação por DNS

O Sistema de Nomes de Domínio (DNS) é um serviço de directory service para recursos conectados a uma rede. Seu provedor de DNS mantém um banco de dados contendo registros que definem seu domínio. Quando você escolhe a validação por DNS, o ACM fornece um ou mais registros CNAME que devem ser adicionados a esse banco de dados. Esses registros contêm um par de chave-valor exclusivo que serve como prova de que você controla o domínio.

#### Note

Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS.

Por exemplo, se você solicitar um certificado para o domínio `example.com` com `www.example.com` como um nome adicional, o ACM criará dois registros CNAME para você. Cada registro criado especificamente para seu domínio e sua conta contém um nome e um valor. O valor é um alias que aponta para um AWS domínio que o ACM usa para renovar automaticamente seu certificado. Você adiciona os registros CNAME a seu banco de dados de DNS somente uma vez.


O ACM renova seu certificado automaticamente, desde que o certificado esteja em uso e o registro CNAME permaneça em vigor.

 Important

Se você não usa o Amazon Route 53 para gerenciar seus registros públicos de DNS, entre em contato com seu provedor do DNS para saber como adicionar registros. Se não tiver autoridade para editar o banco de dados de DNS do seu domínio, você deve usar a [validação por e-mail](#) em seu lugar.


Sem a necessidade de repetir a validação, você pode solicitar certificados adicionais do ACM para seu nome de domínio totalmente qualificado (FQDN) enquanto o registro CNAME permanecer em vigor. Ou seja, você pode criar certificados de substituição com o mesmo nome de domínio ou certificados que cobrem subdomínios diferentes. Como o token de validação CNAME funciona para qualquer AWS região, você pode recriar o mesmo certificado em várias regiões. Você também pode substituir um certificado excluído.

Você pode interromper a renovação automática removendo o certificado do serviço da AWS ao qual ele está associado ou excluindo o registro CNAME. Se o Route 53 não for seu provedor de DNS, entre em contato com o provedor para saber como excluir um registro. Se o Route 53 for seu provedor, consulte [Exclusão de conjuntos de registros de recursos](#) no Guia do desenvolvedor do Route 53. Para obter mais informações sobre a renovação de certificados gerenciados, consulte [Renovação gerenciada para certificados do ACM](#).

 Note

A resolução de CNAME não funcionará se mais de cinco CNAMEs estiverem encadeados em sua configuração do DNS. Se você precisar de um encadeamento mais longo, recomendamos usar a [validação por e-mail](#).

## Como funcionam os registros CNAME para o ACM

 Note

Esta seção é para clientes que não usam o Route 53 como provedor de DNS.

Se você não estiver usando o Route 53 como seu provedor DNS, precisará inserir manualmente os registros CNAME fornecidos pelo ACM no banco de dados do seu provedor, geralmente por meio de um site. Os registros CNAME são usados para vários fins, inclusive como mecanismos de redirecionamento e como contêineres para metadados específicos do provedor. Para o ACM, esses registros permitem a validação inicial da propriedade do domínio e a renovação automática contínua de certificados.

A tabela a seguir mostra exemplos de registros CNAME para seis nomes de domínio. O par nome de registro-valor do Registro de cada registro serve para autenticar a propriedade do nome do domínio.

Na tabela, note que os dois primeiros pares nome de registro-valor do registro são iguais. Isso ilustra que, para um domínio-curinga, como `*.example.com`, as strings criadas pelo ACM são as mesmas que as criadas para seu domínio base, `example.com`. Caso contrário, o par nome de registro e valor do registro é diferente para cada nome de domínio.

### Exemplo de registros CNAME

Nome de domínio	Nome de registro	Valor do registro	Comentário
<code>*.exemplo.com</code>	<code>_<u>x1</u>.exemplo.com.</code>	<code>_<u>x2</u>.acm-validações.aws.</code>	Idêntico
<code>exemplo.com</code>	<code>_<u>x1</u>.exemplo.com.</code>	<code>_<u>x2</u>.acm-validações.aws.</code>	
<code>www.exemplo.com</code>	<code>_<u>x3</u>.www.exemplo.com.</code>	<code>_<u>x4</u>.acm-validações.aws.</code>	Exclusivo
<code>host.exemplo.com</code>	<code>_<u>x5</u>.host.exemplo.com.</code>	<code>_<u>x6</u>.acm-validações.aws.</code>	Exclusivo
<code>subdomínio.exemplo.com</code>	<code>_<u>x7</u>.subdomínio.exemplo.com.</code>	<code>_<u>x8</u>.acm-validações.aws.</code>	Exclusivo
<code>host.subdomínio.exemplo.com</code>	<code>_<u>x9</u>.host.subdomínio.exemplo.com.</code>	<code>_<u>x10</u>.acm-validações.aws.</code>	Exclusivo

Os valores de `xN` após o sublinhado (`_`) são longas strings geradas pelo ACM. Por exemplo,

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

representa um nome de registro gerado. O valor do registro associado pode ser

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

para o mesmo registro de DNS.

### Note

Se o provedor de DNS não suportar os valores de CNAME que comecem com sublinha, consulte [Solucionar problemas de validação por DNS](#).

Quando você solicita um certificado e especifica a validação por DNS, o ACM fornece as informações de CNAME no seguinte formato:

Nome do domínio	Nome de registro	Tipo de registro	Valor do registro
exemplo.com	<code>_a79865eb4cd1a6ab990a45779b4e0b96.exemplo.com.</code>	CNAME	<code>_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.</code>

O nome do domínio é o FQDN associado ao certificado. O nome de registro identifica o registro de forma exclusiva, servindo como a chave do par chave-valor. O valor do registro serve como o valor do par chave-valor.

Todos esses três valores (Nome de domínio, Nome do registro e Valor do registro) devem ser inseridos nos campos apropriados da interface da Web do provedor de DNS para adicionar os registros de DNS. Os provedores são inconsistentes em termos de como tratam o campo de nome do registro (ou apenas "nome"). Em alguns casos, espera-se que você forneça toda a sequência como mostrado acima. Outros provedores adicionam automaticamente o nome de domínio a qualquer sequência que você inserir, o que significa (nesse exemplo) que você deve inserir somente

```
_a79865eb4cd1a6ab990a45779b4e0b96
```



no campo de nome. Se você fizer uma suposição errada e inserir um nome de registro que contenha um nome de domínio (como `.example.com`), o resultado final pode ser o seguinte:

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

A validação não funcionará nesse caso. Conseqüentemente, você deve tentar determinar antecipadamente que tipo de entrada seu provedor espera.

## Configuração da validação por DNS

Esta seção descreve como configurar um certificado público para usar a validação por DNS.

Para configurar a validação por DNS no console

### Note

Esse procedimento pressupõe que você já tenha criado pelo menos um certificado e que esteja trabalhando na AWS região em que o criou. Se você tentar abrir o console e ver a tela de primeiro uso, ou conseguir abrir o console e não ver seu certificado na lista, confirme que você especificou a região correta.

1. Abra o console do ACM em <https://console.aws.amazon.com/acm/>.
2. Na lista de certificados, escolha o Certificate ID (ID do certificado) de um certificado com status Pending validation (Validação pendente) que você deseja configurar. Isso abre uma página de detalhes para o certificado.
3. Na seção Domains (Domínios), realize um dos dois procedimentos a seguir:
  - a. (Opcional) Validar com o Route 53.

Um botão Create record in Route 53 (Criar registro no Route 53) ativo será exibido se as seguintes condições forem verdadeiras:

- Você usa o Route 53 como seu provedor de DNS.
- Você tem permissão para gravar na zona hospedada pelo Route 53.
- Seu FQDN ainda não foi validado.

**Note**

Se você estiver usando o Route 53, mas o botão Criar registros no Route 53 não aparecer ou estiver desabilitado, consulte [Console do ACM não exibe o botão “Criar registros no Route 53”](#).

Selecione o botão Create record in Route 53 (Criar registro no Route 53) e, em seguida, escolha Create records (Criar registros). A página Certificate status (Status do certificado) deve abrir com um banner de status informando Successfully created DNS records (Registros de DNS criados com êxito).

Seu novo certificado pode continuar a exibir um status de Validação pendente por até 30 minutos.

**Tip**

Não é possível solicitar de forma programática que o ACM crie automaticamente seu registro no Route 53. No entanto, você pode fazer uma chamada AWS CLI ou de API para o Route 53 para criar o registro no banco de dados DNS do Route 53. Para obter mais informações sobre conjuntos de registros do Route 53, consulte [Trabalho com conjuntos de registros de recursos](#).

- b. (Opcional) Se não estiver usando o Route 53 como seu provedor de DNS, você deve recuperar as informações de CNAME e adicioná-las a seu banco de dados de DNS. Na página de detalhes do novo certificado, é possível fazer isso de duas formas:
- Copie os componentes do CNAME exibidos na seção Domains (Domínios). As informações precisam ser adicionadas manualmente ao banco de dados de DNS.
  - Outra alternativa é escolher Export to CSV (Exportar para CSV). É necessário adicionar as informações do arquivo resultante manualmente ao seu banco de dados de DNS.

**Important**

Para evitar problemas de validação, revise [Como funcionam os registros CNAME para o ACM](#) antes de adicionar informações ao banco de dados do seu provedor de

DNS. Se você tiver problemas, consulte [Solucionar os problemas de validação por DNS](#).

Se o ACM não puder validar o nome do domínio em até 72 horas a partir do momento em que gera um valor de CNAME para você, o ACM altera o status do certificado para Prazo de validação esgotado. O motivo mais provável para este resultado é você não ter atualizado sua configuração de DNS com o valor gerado pelo ACM. Para corrigir esse problema, você deve solicitar um novo certificado após revisar as instruções de CNAME.

## Validação de e-mail

Antes que a autoridade de certificação (CA) da Amazon possa emitir um certificado para seu site, AWS Certificate Manager (ACM) deve verificar se você possui ou controla todos os domínios que você especificou em sua solicitação. Você pode executar uma verificação usando o e-mail ou o DNS. Este tópico discute a validação de e-mail. Para obter informações sobre a validação de DNS, consulte [Validação por DNS](#).

Observe as considerações a seguir sobre a validação de e-mails.

- Você precisa de um endereço de e-mail de trabalho funcional registrado em seu domínio para usar a validação por e-mail. Os procedimentos para configurar um endereço de e-mail estão fora do escopo deste guia.
- A validação aplica-se apenas a certificados publicamente confiáveis emitidos pelo ACM. O ACM não valida a propriedade do domínio para [certificados importados](#) nem para certificados assinados por uma CA privada. O ACM não pode validar recursos em uma [zona hospedada privada](#) do Amazon VPC em ou qualquer outro domínio privado. Para ter mais informações, consulte [Solução de problemas de validação de certificado](#).
- Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS.

Os certificados do ACM são válidos por 13 meses (395 dias). Para serem renovados, os certificados validados por e-mail exigem uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação 45 dias antes do prazo de validade, usando os endereços da caixa de correio WHOIS do domínio e para cinco endereços comuns de administrador. As notificações contêm um link no qual o proprietário do domínio pode clicar para facilitar a renovação. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

Se você tiver problemas ao usar a validação de e-mail, consulte [Solução de problemas de validação de e-mail](#).

O ACM envia mensagens de e-mail para os três endereços de contato listados no banco de dados WHOIS e para até cinco endereços do sistema para cada domínio especificado. Ou seja, até oito mensagens de e-mail serão enviadas para cada nome de domínio e nome de assunto alternativo que você incluir em sua solicitação. Por exemplo, se especificar apenas um nome de domínio, você receberá até oito mensagens de e-mail. Para validar, você deve agir em uma dessas oito mensagens em até 72 horas. Se especificar três nomes de domínio, você receberá até 24 mensagens. Para validar, você deve agir em pelo menos três desses e-mails, um para cada nome especificado, em 72 horas.

As mensagens de e-mail são enviadas para os seguintes três endereços de contato registrados no WHOIS:

- Domínio registrado
- Contato técnico
- Contato administrativo

#### Note

É altamente recomendável configurar e monitorar os cinco endereços de sistema comuns para o certificado. A recuperação de informações de contato do WHOIS não é confiável. A taxa de sucesso da pesquisa do WHOIS é baixa (menos de 5%), em parte devido à conformidade com as leis globais de privacidade.

#### Important

A partir de junho de 2024, o ACM não oferecerá suporte à nova validação de e-mail por meio de endereços de contato do WHOIS. Para certificados existentes, a partir de outubro de 2024, o ACM não enviará avisos de renovação para os endereços de contato do WHOIS do domínio. O ACM continuará enviando e-mails de validação para os cinco endereços de sistema comuns do domínio solicitado. Para obter mais detalhes, consulte [AWS Certificate Manager interromperá a pesquisa no WHOIS para certificados validados por e-mail](#)

Se você usar o console para solicitar um certificado, o ACM executará uma consulta de MX para determinar quais servidores aceitam e-mail para seu domínio e enviará e-mails para os cinco endereços de sistema comuns para o primeiro domínio encontrado. Se você usar a [RequestCertificate](#) API ou o AWS CLI comando [request-certificate](#), o ACM não executará uma pesquisa MX. Em vez disso, ele enviará e-mails para o nome de domínio especificado no parâmetro `DomainName` ou no parâmetro opcional `ValidationDomain`. Para ter mais informações, consulte [MX record \(Registro MX\)](#).

- `administrator@your_domain_name`
- `hostmaster@your_domain_name`
- `postmaster@your_domain_name`
- `webmaster@your_domain_name`
- `admin@your_domain_name`

Para obter mais informações sobre como o ACM determina os endereços de e-mail para seus domínios, consulte [\(Opcional\) Configurar e-mail para seu domínio](#).

Exceção a este processo

Se você solicitar um certificado do ACM para um nome de domínio que comece com `www` ou um asterisco de curinga (`*`), o ACM removerá o `www` ou o asterisco inicial e enviará e-mails para os endereços administrativos. Esses endereços são formados por `admin@`, `administrator@`, `hostmaster@`, `postmaster@` e `webmaster@` pré-pendentes na parte restante do nome de domínio. Por exemplo, se você solicitar um certificado do ACM para `www.exemplo.com`, o e-mail será enviado para `admin@exemplo.com` em vez de ser enviado para `admin@www.exemplo.com`. Da mesma forma, se você solicitar um certificado do ACM para `*.teste.exemplo.com`, o e-mail será enviado para `admin@teste.exemplo.com`. Os demais endereços administrativos comuns são formados de maneira similar.

#### Note

Certifique-se de que o e-mail seja enviado para os endereços administrativos de um domínio apex, como `example.com`, em vez de para os endereços administrativos de um subdomínio, como `test.example.com`. Para fazer isso, especifique a `ValidationDomain` opção na [RequestCertificate](#) API ou no comando [request-certificate](#) AWS CLI. Esse recurso não é compatível atualmente ao usar o console para solicitar um certificado.

Mesmo quando todas as mensagens são enviadas para um único endereço de e-mail, você deve responder a uma mensagem para cada domínio ou subdomínio para validá-lo e gerar o certificado.

## Data de expiração da validade e de renovação do certificado

Os certificados do ACM são válidos por 13 meses (395 dias). Para serem renovados, os certificados validados por e-mail exigem uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação 45 dias antes do prazo de validade, usando os endereços da caixa de correio WHOIS do domínio e para cinco endereços comuns de administrador. As notificações contêm um link no qual o proprietário do domínio pode clicar para facilitar a renovação. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

Consulte [Validação de e-mail](#) acima para obter mais informações.

### (opcional) Reenvio do e-mail de validação

Cada e-mail de validação contém um token que você pode usar para aprovar uma solicitação de certificado. No entanto, como o e-mail de validação necessário para o processo de aprovação pode ser bloqueado por filtros de spam ou pode ser perdido em trânsito, o token expira automaticamente após 72 horas. Se não receber o e-mail original ou se o token estiver expirado, você poderá solicitar que o e-mail seja reenviado.

Em caso de problemas persistentes com a validação de e-mail, consulte a seção [Solução de problemas de validação de e-mail](#) em [Solução de problemas](#).

#### Note

As informações a seguir aplicam-se apenas a certificados fornecidos pelo e apenas a certificados que usam validação por e-mail. O e-mail de validação não é necessário para certificados de PKI privados ou para [certificados que você importou para o ACM](#). Para obter informações sobre a validação de domínio de DNS, consulte [Validação por DNS](#).

Para reenviar o e-mail de validação usando o console

1. Faça login no AWS Management Console e abra o console do ACM em <https://console.aws.amazon.com/acm/home>.

2. Na lista de certificados, escolha o Certificate ID (ID do certificado) do certificado que deseja validar. Essa ação abre uma página de detalhes.

 Note


Dependendo de como tiver ordenado a lista, talvez o certificado procurado não esteja imediatamente visível. Você pode clicar no triângulo preto à direita para alterar a ordem. Também é possível navegar por várias páginas de certificados usando os números de página no canto superior direito.

3. Na seção Domains (Domínios), escolha Resend validation email (Reenviar e-mail de validação), selecione cada um dos domínios que precisam de validação e escolha Resend (Reenviar). Um banner com a mensagem Successfully resent validation emails (E-mails de validação reenviados com êxito) deverá aparecer.

Para reenviar o e-mail de validação usando a AWS CLI

Você pode usar o [resend-validation-email](#) comando para reenviar e-mails.

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

 Note

O [resend-validation-email](#) comando se aplica somente aos certificados ACM para os quais você está usando a validação de e-mail. A validação não é necessária para certificados que você importou para o ACM nem para os certificados privados que você gerencia usando o ACM.

## Lista dos certificados gerenciados pelo ACM

Você pode usar o console do ACM ou AWS CLI listar os certificados gerenciados pelo ACM. O console pode listar até 500 certificados em uma página e a CLI até 1.000.

## Para listar certificados usando o console


1. Abra o console do ACM em <https://console.aws.amazon.com/acm/>.
2. Revise as informações na lista de certificados. É possível navegar por várias páginas de certificados usando os números de página no canto superior direito. Cada certificado ocupa uma linha com as seguintes colunas exibidas por padrão para cada certificado:
  - Domain name (Nome do domínio) – O nome de domínio totalmente qualificado (FQDN) para o certificado.
  - Tipo – O tipo de certificado. Os valores possíveis são: Amazon issued (Emitido pela Amazon) | Private (Privado) | Imported (Importado)
  - Status – Status do certificado. Os valores possíveis são: Pending validation (Validação pendente) | Issued (Emitido) | Inactive (Inativo) | Expired (Expirado) | Revoked (Revogado) | Failed (Com falha) | Validation timed out (Tempo limite da validação esgotado)
  - Em uso? — Se o certificado ACM está ativamente associado a um AWS serviço como o Elastic Load CloudFront Balancing ou. O valor pode ser Não ou Sim.
  - Renewal eligibility (Elegibilidade para renovação): indica se o certificado poderá ser renovado automaticamente pelo ACM quando ele estiver prestes a expirar. Os valores possíveis são: Eligible (Elegível) | Ineligible (Inelegível). Para visualizar as regras de qualificação, consulte [Renovação gerenciada para certificados do ACM](#).

Ao escolher o ícone de configurações no canto superior direito do console, você pode personalizar o número de certificados exibidos em uma página, especificar o comportamento de quebra de linha do conteúdo da célula e exibir campos de informações adicionais. Os seguintes campos opcionais estão disponíveis:

- Additional domain names (Nomes de domínio adicionais): um ou mais nomes de domínio (nomes alternativos de assunto) incluídos no certificado.
- Requested at (Solicitado em): o momento em que o ACM solicitou o certificado.
- Issued at (Emitido em): a hora em que o certificado foi emitido. Essas informações estão disponíveis somente para certificados emitidos pela Amazon, e não para importações.
- Not before (Não antes de): a hora antes da qual o certificado não é válido.
- Not after (Não depois de): a hora depois da qual o certificado não é válido.
- Revoked at (Revogado em): para certificados revogados, a hora da revogação.



- **Name tag (Etiqueta de nome):** o valor de uma etiqueta neste certificado chamada Name (Nome), se essa tag existir.
- **Renewal status (Status da renovação):** o status da renovação solicitada para um certificado. Este campo é exibido e tem valor somente se a renovação foi solicitada. Os valores possíveis são: Pending automatic renewal (Renovação automática pendente) | Pending validation (Validação pendente) | Success (Com êxito) | Failure (Com falha).

 Note

Pode levar várias horas para que as alterações no status do certificado se tornem disponíveis. Se for encontrado um problema, uma solicitação de certificado expira após 72 horas e o processo de emissão ou renovação deve ser repetido desde o início.

A preferência de tamanho da página especifica o número de certificados retornados em cada página do console.

Para mais informações sobre os detalhes de certificado disponíveis, consulte [Descrição dos certificados do ACM](#).

Para listar seus certificados usando o AWS CLI

Usar o comando [list-certificate](#) para listar os certificados gerenciados pela ACM, como mostrado no exemplo a seguir:

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

O comando retorna informações semelhantes às seguintes:

```
{
  "CertificateSummaryList": [
    {
      "CertificateArn":
"arn:aws:acm:Region:444455556666:certificate/certificate_ID",
      "DomainName": "example.com"
      "SubjectAlternativeNameSummaries": [
        "example.com",
        "other.example.com"
      ],
      "HasAdditionalSubjectAlternativeNames": false,
    }
  ]
}
```

```
    "Status": "ISSUED",
    "Type": "IMPORTED",
    "KeyAlgorithm": "RSA-2048",
    "KeyUsages": [
      "DIGITAL_SIGNATURE",
      "KEY_ENCIPHERMENT"
    ],
    "ExtendedKeyUsages": [
      "NONE"
    ],
    "InUse": false,
    "RenewalEligibility": "INELIGIBLE",
    "NotBefore": "2022-06-14T23:42:49+00:00",
    "NotAfter": "2032-06-11T23:42:49+00:00",
    "CreatedAt": "2022-08-25T19:28:05.531000+00:00",
    "ImportedAt": "2022-08-25T19:28:05.544000+00:00"
  },...
]
}
```

Por padrão, apenas certificados com keyTypes RSA\_1024 ou RSA\_2048 e pelo menos um domínio especificado são retornados. Para ver outros certificados controlados por você, como certificados sem domínio ou certificados com algoritmo ou tamanho em bits diferente, forneça o parâmetro `--includes` conforme mostrado no exemplo a seguir. O parâmetro permite especificar um membro da estrutura de [Filtros](#).

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

## Descrição dos certificados do ACM


Você pode usar o console do ACM ou o AWS CLI para listar metadados detalhados sobre seus certificados.

Para visualizar detalhes do certificado no console

1. Abra o console do ACM em <https://console.aws.amazon.com/acm/> para exibir seus certificados. É possível navegar por várias páginas de certificados usando os números de página no canto superior direito.
2. Para mostrar metadados detalhados para um certificado listado, escolha a ID do certificado. Uma página é aberta exibindo as seguintes informações:

- Status do certificado
  - Identificador – Identificador exclusivo hexadecimal de 32 bytes do certificado
  - ARN – Um nome do recurso da Amazon (ARN) no formulário `arn:aws:acm:Region:444455556666:certificate/certificate_ID`
  - Type (Tipo) – Identifica a categoria de gerenciamento de um certificado do ACM. Os valores possíveis são: Amazon Issued (Emitido pela Amazon)|Private (Privado)|Imported (Importado). Para obter mais informações, consulte [Solicitação de um certificado público](#), [Como solicitar um certificado de PKI privado](#) ou [Importando certificados para AWS Certificate Manager](#).
  - Status – o status do certificado. Os valores possíveis são: Pending validation (Validação pendente) | Issued (Emitido) | Inactive (Inativo) | Expired (Expirado) | Revoked (Revogado) | Failed (Com falha) | Validation timed out (Tempo limite da validação esgotado)
  - Status detalhado – Data e hora em que o certificado foi emitido ou importado
- Domínios
  - Domínio – O nome de domínio totalmente qualificado (FQDN) para o certificado.
  - Status – O status de validação do domínio. Os valores possíveis são: Pending validation (Validação pendente) | Revoked (Revogado) | Failed (Com falha) | Validation timed out (Tempo limite da validação esgotado) | Success (Êxito)
- Detalhes
  - Em uso? – Se o certificado estiver associado a um [serviço integrado da AWS](#), os valores possíveis são: Yes (Sim)|No (Não)
  - Nome do domínio – O primeiro nome de domínio totalmente qualificado (FQDN) para o certificado.
  - Número de nomes adicionais — Número de nomes de domínio para os quais o certificado é válido
  - Número de série – Um número de série hexadecimal de 16 bytes do certificado
  - Informações da chave pública – O algoritmo criptográfico usado para gerar o par de chaves
  - Signature algorithm (Algoritmo de assinatura) – O algoritmo criptográfico usado para criar a assinatura do certificado.
  - Can be used with (Pode ser usado com): uma lista de [serviços integrados](#) ao ACM que são compatíveis com um certificado com esses parâmetros.
  - Solicitado em – Data e hora da solicitação de emissão

- Emitido em – Se aplicável, a data e a hora da emissão
- Importado em – Se aplicável, a data e a hora da importação
- Não antes – O início do período de validade do certificado
- Não após – A data e a hora do fim da validade do certificado
- Renewal eligibility (Qualificação para renovação): os valores possíveis são: Eligible (Qualificado) | Ineligible (Não qualificado). Para visualizar as regras de qualificação, consulte [Renovação gerenciada para certificados do ACM](#).
- Renewal status (Status da renovação): o status da renovação solicitada para um certificado. Este campo é exibido e tem valor somente se a renovação foi solicitada. Os valores possíveis são: Pending automatic renewal (Renovação automática pendente) | Pending validation (Validação pendente) | Success (Com êxito) | Failure (Com falha).

 Note

Pode levar várias horas para que as alterações no status do certificado se tornem disponíveis. Se for encontrado um problema, uma solicitação de certificado expira após 72 horas e o processo de emissão ou renovação deve ser repetido desde o início.

- CA – O ARN da CA que assinou
- Tags
  - Chave
  - Valor
- Validation state (Estado de validação) – Se aplicável, os valores possíveis são:
  - Pending (Pendente) – A validação foi solicitada e não foi concluída.
  - Validation timed out (Prazo de validação expirado) – Uma validação solicitada expirou, mas você pode repetir a solicitação.
  - None (Nenhum) – O certificado é para uma PKI privada ou é autoassinado e não precisa de validação.

Para visualizar os detalhes do certificado usando o AWS CLI

Use o [describe-certificate](#) no AWS CLI para exibir os detalhes do certificado, conforme mostrado no comando a seguir:

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

O comando retorna informações semelhantes às seguintes:

```
{
  "Certificate": {
    "CertificateArn": "arn:aws:acm:Region:444455556666:certificate/certificate_ID",
    "Status": "EXPIRED",
    "Options": {
      "CertificateTransparencyLoggingPreference": "ENABLED"
    },
    "SubjectAlternativeNames": [
      "example.com",
      "www.example.com"
    ],
    "DomainName": "gregpe.com",
    "NotBefore": 1450137600.0,
    "RenewalEligibility": "INELIGIBLE",
    "NotAfter": 1484481600.0,
    "KeyAlgorithm": "RSA-2048",
    "InUseBy": [
      "arn:aws:cloudfront::account:distribution/E12KXPQHVL5YVC"
    ],
    "SignatureAlgorithm": "SHA256WITHRSA",
    "CreatedAt": 1450212224.0,
    "IssuedAt": 1450212292.0,
    "KeyUsages": [
      {
        "Name": "DIGITAL_SIGNATURE"
      },
      {
        "Name": "KEY_ENCIPHERMENT"
      }
    ],
    "Serial": "07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b",
    "Issuer": "Amazon",
    "Type": "AMAZON_ISSUED",
    "ExtendedKeyUsages": [
      {
        "OID": "1.3.6.1.5.5.7.3.1",
        "Name": "TLS_WEB_SERVER_AUTHENTICATION"
      }
    ],
  }
}
```

```
{
  "OID": "1.3.6.1.5.5.7.3.2",
  "Name": "TLS_WEB_CLIENT_AUTHENTICATION"
},
"DomainValidationOptions": [
  {
    "ValidationEmails": [
      "hostmaster@example.com",
      "admin@example.com",
      "postmaster@example.com",
      "webmaster@example.com",
      "administrator@example.com"
    ],
    "ValidationDomain": "example.com",
    "DomainName": "example.com"
  },
  {
    "ValidationEmails": [
      "hostmaster@example.com",
      "admin@example.com",
      "postmaster@example.com",
      "webmaster@example.com",
      "administrator@example.com"
    ],
    "ValidationDomain": "www.example.com",
    "DomainName": "www.example.com"
  }
],
"Subject": "CN=example.com"
}
```

## Exclusão dos certificados gerenciados pelo ACM

Você pode usar o console do ACM ou o AWS CLI para excluir um certificado.

### Important

- Você não pode excluir um certificado do ACM que esteja sendo usado por outro serviço da AWS. Para excluir um certificado que esteja em uso, você deve primeiro remover a associação do certificado. Isso é feito usando o console ou a CLI para o serviço associado.

- A exclusão de um certificado emitido por uma autoridade de certificação (CA) privada não afeta a CA. Você continuará a ser cobrado pela CA até que ela seja excluída. Para obter mais informações, consulte [Exclusão da sua CA privada](#) no Guia do usuário da AWS Private Certificate Authority .

Para excluir um certificado usando o console

1. Abra o console do ACM em <https://console.aws.amazon.com/acm/>.
2. Na lista de certificados, marque a caixa de seleção do certificado do ACM e selecione Delete (Excluir).

#### Note

Dependendo de como tiver ordenado a lista, talvez o certificado procurado não esteja imediatamente visível. Você pode clicar no triângulo preto à direita para alterar a ordem. Também é possível navegar por várias páginas de certificados usando os números de página no canto superior direito.

Para excluir um certificado usando o AWS CLI

Usar o comando [delete-certificate](#) para excluir um certificado, como mostrado no comando a seguir:

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

## Instalando certificados do ACM;

Você não pode usar o ACM para instalar um certificado público diretamente em seu site ou aplicativo AWS baseado. Você deve usar um dos serviços integrados ao ACM. Para ter mais informações, consulte [Serviços integrados com AWS Certificate Manager](#).

Os certificados ACM assinados por uma CA CA privada da AWS e destinados à sua PKI privada podem ser [exportados](#) e instalados manualmente em qualquer sistema em que você tenha acesso administrativo. Esses certificados não são confiáveis na internet pública.

# Renovação gerenciada para certificados do ACM

O ACM fornece renovação gerenciada para seus certificados SSL/TLS emitidos pela Amazon. Isso significa que o ACM renovará seus certificados automaticamente (se você estiver usando a validação por DNS) ou enviará avisos por e-mail quando a expiração da validade estiver se aproximando. Esses serviços são fornecidos para certificados públicos e privados do ACM.

Um certificado é elegível para renovação automática sujeito às seguintes considerações:

- ELEGÍVEL se associado a outro AWS serviço, como Elastic Load Balancing ou CloudFront
- ELEGÍVEL se exportado desde a sua emissão ou da última renovação.
- ELEGÍVEL se for um certificado privado emitido chamando a [RequestCertificateAPI](#) do ACM e depois exportado ou associado a outro AWS serviço.
- ELEGÍVEL se for um certificado privado emitido por meio do [console de gerenciamento](#) e depois exportado ou associado a outro serviço da AWS .
- NÃO ELEGÍVEL se for um certificado privado emitido pela chamada da CA privada da AWS [IssueCertificateAPI](#).
- NÃO ELEGÍVEL se [importado](#).
- NÃO ELEGÍVEL se já tiver expirado.

Além disso, é necessário satisfazer os seguintes requisitos de [Punycode](#) relacionados a [Internationalized Domain Names](#) (Nomes de domínio internacionalizados):

1. Nomes de domínio que comecem com o padrão “<character><character>--” devem corresponder a “xn--”.
2. Nomes de domínio que comecem com “xn--” também devem ser nomes de domínio internacionalizado válidos.



## Exemplos de Punycode

Nome do domínio	Satisfaz o n.º 1	Satisfaz o n.º 2	Permit	Observação
exemplo.com	n/a	n/a	✓	Não começa com “<character><character>--”
a--examp le.com	n/a	n/a	✓	Não começa com “<character><character>--”
abc--exam ple.com	n/a	n/a	✓	Não começa com “<character><character>--”
xn--xyz.com	Sim	Sim	✓	Nome de domínio internacionalizado válido (é resolvido para 簡.com)
xn--exam le.com	Sim	Não	✗	Não é um nome de domínio internacionalizado válido
ab--exam le.com	Não	Não	✗	Deve começar com “xn--”

Quando o ACM renova um certificado, o nome de recurso da Amazon (ARN) do certificado continua o mesmo. Além disso, os certificados do ACM são [recursos regionais](#). Se você tiver certificados para o mesmo nome de domínio em várias AWS regiões, cada um desses certificados deverá ser renovado de forma independente.

### Tópicos

- [Renovação de certificados confiáveis publicamente](#)
- [Renovação de certificados em uma PKI privada](#)
- [Verificar o status de renovação de um certificado](#)

# Renovação de certificados confiáveis publicamente

Ao emitir um certificado gerenciado e publicamente confiável, é AWS Certificate Manager necessário provar que você é o proprietário do domínio. Isso acontece por meio de uma [validação de DNS](#) ou [validação por e-mail](#). Quando um certificado aparece para renovação, o ACM usa o mesmo método que você escolheu anteriormente para revalidar sua propriedade. Os tópicos a seguir descrevem como o processo de renovação funciona em cada caso.

## Tópicos

- [Renovação de domínios validados pelo DNS](#)
- [Renovação de domínios validados por e-mail](#)

## Renovação de domínios validados pelo DNS

A renovação gerenciada é totalmente automatizada para certificados do ACM que foram originalmente emitidos usando a [validação por DNS](#).

Sessenta dias antes da expiração da validade, o ACM verifica os seguintes critérios de renovação:

- O certificado está sendo usado atualmente por um AWS serviço.
- Todos os registros CNAME de DNS necessários fornecidos pelo ACM (um para cada nome exclusivo alternativo de assunto) estão presentes e acessíveis por meio de DNS público.

Se esses critérios forem atendidos, o ACM considerará os nomes de domínio validados e renovará o certificado.

O ACM envia AWS Health eventos e EventBridge eventos da Amazon quando não consegue validar automaticamente um domínio durante a renovação (por exemplo, devido à presença do registro CAA). Esses eventos são enviados 45 dias, 30 dias, 15 dias, 7 dias, 3 dias e 1 dia antes da expiração da validade. Para ter mais informações, consulte [EventBridge Suporte da Amazon para ACM](#).

## Renovação de domínios validados por e-mail

Os certificados do ACM são válidos por 13 meses (395 dias). Para serem renovados, os certificados validados por e-mail exigem uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação 45 dias antes do prazo de validade, usando os endereços da caixa de correio WHOIS do

domínio e para cinco endereços comuns de administrador. As notificações contêm um link no qual o proprietário do domínio pode clicar para facilitar a renovação. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

Para obter mais informações sobre mensagens de validação por e-mail, consulte [Validação de e-mail](#)

Para saber como é possível responder de forma programática ao e-mail de validação, consulte [Automatizando a validação por e-mail](#).

## Solicitar uma mensagem de e-mail de validação de domínio

Após configurar os endereços de e-mail de contato para seu domínio (consulte [\(Opcional\) Configurar e-mail para seu domínio](#)), você pode usar o console do AWS Certificate Manager ou a API do ACM para solicitar que o ACM envie um e-mail de validação de domínio para a renovação do certificado. Você deve fazer isso nas seguintes circunstâncias:

- Você usou a validação por e-mail quando solicitou seu certificado do ACM inicialmente.
- O status da renovação do certificado é pending validation (validação pendente). Para obter informações sobre como determinar o status de renovação do certificado, consulte [Verificar o status de renovação de um certificado](#).
- Você não recebeu ou não pode encontrar o e-mail de validação de domínio original que o ACM enviou para a renovação do certificado.

Para solicitar que o ACM reenvie o e-mail de validação de domínio (console)

1. Abra o AWS Certificate Manager console em <https://console.aws.amazon.com/acm/home>.
2. Selecione o ID do certificado do certificado que requer validação.
3. Selecione Resend validation email (reenviar o e-mail de validação).

Para solicitar que o ACM reenvie o e-mail de validação de domínio (API do ACM)

Use a [ResendValidationEmail](#) operação na API do ACM. Ao fazer isso, passe o nome de região da Amazon (ARN) do certificado, o domínio que requer validação manual e o domínio no qual você deseja receber os e-mails de validação do domínio. O exemplo a seguir mostra como fazer isso com a AWS CLI. Este exemplo contém quebras de linha para facilitar a leitura.

```
$ aws acm resend-validation-email \  
  --certificate-arn arn:aws:acm:region:account:certificate/certificate_ID \  
  --domain-name domain-name
```

```
--domain subdomain.example.com \  
--validation-domain example.com
```

## Renovação de certificados em uma PKI privada

Os certificados ACM que foram assinados por uma CA privada de CA privada da AWS são elegíveis para renovação gerenciada. Ao contrário dos certificados do ACM publicamente confiáveis, um certificado para uma PKI privada não requer validação. A confiança é estabelecida quando um administrador instala o certificado CA-raiz apropriado nos armazenamentos de confiança do cliente.

### Note

Somente certificados obtidos usando o console do ACM ou a [RequestCertificate](#) da API do ACM são elegíveis para renovação gerenciada. Os certificados emitidos diretamente pelo CA privada da AWS uso da [IssueCertificate](#) da CA privada da AWS API não são gerenciados pelo ACM.

Quando prazo de validade de um certificado gerenciado expira em 60 dias, o ACM tenta renová-lo automaticamente. Isso inclui certificados que foram exportados e instalados manualmente (por exemplo, em um datacenter on-premises). Os clientes também podem forçar a renovação a qualquer momento usando a [RenewCertificate](#) da API do ACM. Para obter um exemplo de implementação Java de renovação forçada, consulte [Renovação de um certificado](#).

Após a renovação, a implantação de um certificado em serviço ocorre de uma das seguintes maneiras:

- Se o certificado é associado a um [serviço integrado](#) do ACM, o novo certificado substitui o antigo sem ação adicional do cliente.
- Se o certificado não é associado a um [serviço integrado](#) do ACM, a ação do cliente é necessária para exportar e instalar o certificado renovado. Você pode realizar essas ações manualmente ou com a ajuda da [AWS HealthAmazon EventBridge](#) e da [AWS Lambda](#) seguinte forma. Para obter mais informações, consulte [Automatização da exportação de certificados renovados](#)

## Automatização da exportação de certificados renovados

O procedimento a seguir fornece um exemplo de solução para automatizar a exportação de seus certificados PKI privados quando o ACM os renova. Este exemplo apenas exporta um certificado e

sua chave privada para fora do ACM. Após a exportação, o certificado ainda deve ser instalado em seu dispositivo de destino.

Como exportar um certificado privado usando o console

1. Seguindo os procedimentos do AWS Lambda Developer Guide, crie e configure uma função Lambda que chame a API de exportação do ACM.
  - a. [Crie uma função do Lambda](#).
  - b. [Crie uma função de execução do Lambda](#) para sua função e adicione a política de confiança a seguir a ela. A política concede permissão ao código em sua função para recuperar o certificado renovado e a chave privada chamando a [ExportCertificate](#) da API do ACM.

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

2. [Crie uma regra na Amazon EventBridge](#) para ouvir eventos de saúde do ACM e chamar sua função Lambda quando ela detectar um. O ACM grava em um AWS Health evento toda vez que tenta renovar um certificado. Para mais informações sobre esses avisos, consulte [Verificar o status usando o Personal Health Dashboard \(PHD\)](#).

Configure a regra adicionando o padrão de evento a seguir.

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
```

```
    "service": [
      "ACM"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_ACM_RENEWAL_STATE_CHANGE"
    ]
  },
  "resources": [
    "arn:aws:acm:region:account:certificate/certificate_ID"
  ]
}
```

3. Conclua o processo de renovação instalando manualmente o certificado no sistema de destino.

## Teste da renovação gerenciada de seus certificados de PKI privada

Você pode usar a API do ACM ou testar manualmente AWS CLI a configuração do seu fluxo de trabalho de renovação gerenciada pelo ACM. Fazendo isso, você pode confirmar que os certificados serão renovados automaticamente pelo ACM antes da expiração da validade.

### Note

Você só pode testar a renovação de certificados emitidos e exportados pela CA privada da AWS.

Quando você usa as ações de API ou os comandos da CLI descritos abaixo, o ACM tenta renovar o certificado. Se a renovação for bem-sucedida, o ACM atualizará os metadados do certificado exibidos no console de gerenciamento ou na saída da API. Se o certificado estiver associado a um [serviço integrado](#) do ACM, o novo certificado será implantado e um evento de renovação será gerado no Amazon CloudWatch Events. Se a renovação falhar, o ACM retorna um erro e sugere uma ação corretiva. (Você pode visualizar essas informações usando o comando [describe-certificate](#).) Se o certificado não é implantado por meio de um serviço integrado, você ainda precisa exportá-lo e instalá-lo manualmente em seu recurso.

**⚠ Important**

Para renovar seus CA privada da AWS certificados com o ACM, você deve primeiro conceder ao principal serviço do ACM permissões para fazer isso. Para obter mais informações, consulte [Atribuindo permissões de renovação de certificado ao ACM](#).

Para testar manualmente a renovação de certificado (AWS CLI)

1. Use o comando [renew-certificate](#) para renovar um certificado privado exportado.

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

2. Depois, use o comando [describe-certificate](#) para confirmar que os detalhes da renovação do certificado foram atualizados.

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

Para testar manualmente a renovação de certificados (API do ACM)

- Envie uma [RenewCertificate](#) solicitação especificando o ARN do certificado privado a ser renovado. Em seguida, use a [DescribeCertificate](#) operação para confirmar que os detalhes de renovação do certificado foram atualizados.

## Verificar o status de renovação de um certificado

Quando você tenta renovar um certificado, o ACM fornece um campo de informações Renewal status (Status da renovação) nos detalhes do certificado. Você pode usar o AWS Certificate Manager console, a API do ACM AWS CLI, o ou o AWS Health Dashboard para verificar o status de renovação de um certificado do ACM. Se você usa o console ou a API do ACM, o status de renovação pode ter um dos quatro valores de status possíveis listados abaixo. AWS CLI Valores semelhantes serão exibidos se você usar o AWS Health Dashboard.

## Renovação automática pendente

O ACM está tentando validar automaticamente os nomes de domínio no certificado. Para ter mais informações, consulte [Renovação de domínios validados pelo DNS](#). Nenhuma outra ação é necessária.

## Validação pendente

ACM não foi capaz de validar automaticamente um ou mais nomes de domínio no certificado. Você deve tomar ação para validar esses nomes de domínio ou o certificado não será renovado. Se, originalmente, você usou a validação por e-mail para o certificado, procure um e-mail do ACM e depois siga o link no e-mail para executar a validação. Se você tiver usado a validação de DNS, verifique se o registro DNS existe e se o certificado permanece em uso.

## Bem-sucedida

Todos os nomes de domínio no certificado foram validados, e o ACM renovou o certificado. Nenhuma outra ação é necessária.

## Com falha

Um ou mais nomes de domínio não foram validados antes que a validade do certificado expirasse, e o ACM não renovou o certificado. Você pode [solicitar um novo certificado](#).

Um certificado é elegível para renovação se estiver associado a outro AWS serviço, como o Elastic Load Balancing ou CloudFront, ou se tiver sido exportado desde a emissão ou a última renovação.

### Note

Pode demorar várias horas para que as alterações no status da renovação se tornem disponíveis. Se um problema for encontrado, a solicitação de renovação expirará após 72 horas e o processo de renovação deverá ser repetido desde o início. Para obter ajuda sobre a solução de problemas, consulte [Solução de problemas de solicitações de certificado](#).

## Tópicos

- [Verificar o status \(console\)](#)
- [Verificar o status \(API\)](#)
- [Verificar o status \(CLI\)](#)



- [Verificar o status usando o Personal Health Dashboard \(PHD\)](#)

## Verificar o status (console)

O procedimento a seguir discute como usar o console do ACM para verificar o status da renovação de um certificado do ACM.

1. Abra o AWS Certificate Manager console em <https://console.aws.amazon.com/acm/home>.
2. Expanda um certificado para visualizar seus detalhes.
3. Localize o Renewal status (Status da renovação) na seção Details (Detalhes). Se você não vir o status, o ACM não terá iniciado o processo de renovação gerenciada para esse certificado.

## Verificar o status (API)

Para ver um exemplo de Java que mostra como usar a [DescribeCertificate](#) ação para verificar o status, consulte [Descrição de um certificado](#).

## Verificar o status (CLI)

O exemplo a seguir mostra como verificar o status da renovação de seu certificado do ACM com o [AWS Command Line Interface \(AWS CLI\)](#).

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

Na resposta, observe o valor no campo `RenewalStatus`. Se você não vir o campo `RenewalStatus`, o ACM não iniciou o processo de renovação gerenciada para o certificado.

## Verificar o status usando o Personal Health Dashboard (PHD)

O ACM tenta renovar automaticamente seu certificado do ACM 60 dias antes da expiração da validade. Se o ACM não puder renovar automaticamente seu certificado, ele enviará avisos de eventos de renovação do certificado para você AWS Health Dashboard em intervalos de 45 dias, 30 dias, 15 dias, 7 dias, 3 dias e 1 dia a partir da expiração para informá-lo de que você precisa tomar medidas. Isso AWS Health Dashboard faz parte do AWS Health serviço. Ele não requer nenhuma configuração e pode ser visualizado por qualquer usuário autenticado em sua conta. Para obter mais informações, consulte o [Guia do usuário do AWS Health](#).

 Note

O ACM grava avisos de eventos de renovação sucessivos em um único evento em sua linha de tempo do PHD. Cada aviso substitui o anterior até que a renovação seja bem-sucedida.

Para usar o AWS Health Dashboard:

1. Faça login AWS Health Dashboard em <https://phd.aws.amazon.com/phd/home#/>.
2. Escolha Event log.
3. Em Filtrar por tags ou atributos, escolha Service.
4. Escolha Certificate Manager.
5. Escolha Aplicar.
6. Em Event category, escolha Scheduled Change.
7. Escolha Aplicar.

# Automatizando a validação por e-mail

Os certificados ACM validados por e-mail normalmente exigem uma ação manual do proprietário do domínio. Organizações que lidam com um grande número de certificados validados por e-mail podem preferir criar um analisador que possa automatizar as respostas necessárias. Para ajudar os clientes a usar a validação por e-mail, as informações nesta seção descrevem os modelos usados para mensagens de e-mail de validação de domínio e o fluxo de trabalho envolvido na realização do processo de validação.

## Modelos de e-mail de validação

As mensagens de e-mail de validação têm um dos dois formatos a seguir, dependendo se um novo certificado está sendo solicitado ou um certificado existente está sendo renovado. O conteúdo das cadeias destacadas deve ser substituído por valores específicos para o domínio que está sendo validado.

### Validando um novo certificado

Texto do modelo de e-mail:

```
Greetings from Amazon Web Services,  
  
We received a request to issue an SSL/TLS certificate for requested_domain.  
  
Verify that the following domain, AWS account ID, and certificate identifier  
correspond  
to a request from you or someone in your organization.  
  
Domain: fqdn  
AWS account ID: account_id  
AWS Region name: region_name  
Certificate Identifier: certificate_identifier  
  
To approve this request, go to Amazon Certificate Approvals  
(https://region\_name.acm-certificates.amazon.com/approvals?  
code=validation\_code&context=validation\_context)  
and follow the instructions on the page.  
  
This email is intended solely for authorized individuals for fqdn. To express any  
concerns
```

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

Sincerely,  
Amazon Web Services

## Validando um certificado para renovação

Texto do modelo de e-mail:

Greetings from Amazon Web Services,

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

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

Domain: *fqdn*  
AWS account ID: *account\_id*  
AWS Region name: *region\_name*  
Certificate Identifier: *certificate\_identifier*

To approve this request, go to Amazon Certificate Approvals at [https://region\\_name.acm-certificates.amazon.com/approvals?code=\\$validation\\_code&context=\\$validation\\_context](https://region_name.acm-certificates.amazon.com/approvals?code=$validation_code&context=$validation_context) and follow the instructions on the page.

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

Sincerely,  
Amazon Web Services

--

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

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

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

Depois de receber uma nova mensagem de validação da AWS, recomendamos que você a use como o modelo mais atualizado e oficial para seu analisador. Os clientes com analisadores de mensagens criados antes de novembro de 2020 devem observar as seguintes alterações que podem ter sido feitas no modelo:

- A linha de assunto do e-mail agora mostra "Certificate request for *domain name*" em vez de ""Certificate approval for *domain name*".
- O AWS account ID agora é apresentado sem traços ou hífens.
- O Certificate Identifier agora apresenta todo o ARN do certificado em vez de uma forma reduzida, por exemplo, *arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369* em vez de *3b4d78e1-0882-4f51-954a-298ee44ff369*.
- O URL de aprovação do certificado agora contém *acm-certificates.amazon.com* em vez de *certificates.amazon.com*.
- O formulário de aprovação aberto clicando no URL de aprovação do certificado agora contém o botão de aprovação. O nome do botão de aprovação é agora *approve-button* em vez de *approval\_button*.
- As mensagens de validação para certificados recém-solicitados e certificados de renovação têm o mesmo formato de e-mail.

## Fluxo de trabalho de validação

Esta seção fornece informações sobre o fluxo de trabalho de renovação para certificados validados por e-mail.

- Quando o console do ACM processa uma solicitação de certificado de vários domínios, ele envia mensagens de e-mail de validação para o primeiro domínio encontrado que inclua um registro MX. O proprietário do domínio precisa validar uma mensagem de e-mail para cada domínio antes que o

ACM possa emitir o certificado. Para obter mais informações, consulte [Uso do DNS para validar a propriedade do domínio](#).

- A validação por e-mail de solicitações de certificado de vários domínios usando a API ou a CLI do ACM gera uma mensagem de e-mail enviada por padrão para o domínio apex e para cada subdomínio. O proprietário do domínio precisa validar uma mensagem de e-mail para cada um desses domínios antes que o ACM possa emitir o certificado.

 Note

Antes de novembro de 2020, os clientes precisavam validar apenas o domínio apex e o ACM emitia um certificado que também abrangia todos os subdomínios. Os clientes com analisadores de mensagens projetados antes dessa época devem observar a alteração no fluxo de trabalho de validação de e-mail.

- Com a API ou a CLI do ACM, você pode forçar que todas as mensagens de e-mail de validação para uma solicitação de certificado de vários domínios sejam enviadas para o domínio apex. Na API, use o parâmetro `DomainValidationOptions` da ação [RequestCertificate](#) para especificar um valor para `ValidationDomain`, que é um membro do tipo [DomainValidationOption](#). Na CLI, use o parâmetro `--domain-validation-options` do comando [request-certificate](#) para especificar um valor para `ValidationDomain`.

# Importando certificados para AWS Certificate Manager

Além de solicitar certificados SSL/TLS fornecidos pelo AWS Certificate Manager (ACM), você pode importar certificados obtidos fora do. AWS Você pode fazer isso porque já possui um certificado de uma autoridade de certificação (CA) de terceiros, ou porque tem requisitos específicos da aplicação que não são atendidos pelos certificados emitidos pelo ACM.

Você pode usar um certificado importado com qualquer serviço da [AWS integrado ao ACM](#). Os certificados que você importa funcionam da mesma forma que os fornecidos pelo ACM, com uma exceção importante: o ACM não oferece [renovação gerenciada](#) para certificados importados.

Para renovar um certificado importado, você pode obter um novo certificado com o emissor do mesmo e, em seguida, [reimportá-lo](#) para o ACM manualmente. Essa ação preserva a associação do certificado e seu nome do recurso da Amazon (ARN). Você também pode importar um certificado completamente novo. Vários certificados com o mesmo nome de domínio podem ser importados, mas eles devem ser importados um de cada vez.

## Important

Você é responsável por monitorar a data de validade dos seus certificados importados e por renová-los antes que expirem. Você pode simplificar essa tarefa usando o Amazon CloudWatch Events para enviar avisos quando seus certificados importados estiverem prestes a expirar. Para ter mais informações, consulte [Usando a Amazon EventBridge](#).

Todos os certificados no ACM são recursos regionais, incluindo os certificados que você importar. Para usar o mesmo certificado com balanceadores de carga do Elastic Load Balancing em diferentes AWS regiões, você deve importar o certificado para cada região em que deseja usá-lo. Para usar um certificado com a Amazon CloudFront, você deve importá-lo para a região Leste dos EUA (Norte da Virgínia). Para ter mais informações, consulte [Regiões compatíveis](#).

Para obter mais informações sobre como importar certificados para o ACM, consulte os tópicos a seguir. Se você tiver problemas ao importar um certificado, consulte [Problemas de importação do certificado](#).

## Tópicos

- [Pré-requisitos para importação de certificados](#)

- [Formato de chaves e certificados para importação](#)
- [Importação de um certificado](#)
- [Reimportação de um certificado](#)

## Pré-requisitos para importação de certificados

Para importar um certificado SSL/TLS autoassinado para o ACM, você deve fornecer o certificado e sua chave privada. Para importar um certificado assinado por uma autoridade AWS não certificadora (CA), você também deve incluir as chaves pública e privada do certificado. Seu certificado deve atender a todos os critérios descritos neste tópico.

Para todos os certificados importados, você deverá especificar um algoritmo de criptografia e um tamanho de chave. O ACM suporta os seguintes algoritmos (nome da API entre parênteses):

- RSA de 1024 bits (RSA\_1024)
- RSA de 2048 bits (RSA\_2048)
- RSA de 3072 bits (RSA\_3072)
- RSA de 4096 bits (RSA\_4096)
- ECDSA de 256 bits (EC\_prime256v1)
- ECDSA de 384 bits (EC\_secp384r1)
- ECDSA de 521 bits (EC\_secp521r1)

Observe também os seguintes requisitos adicionais:

- Os [serviços integrados](#) do ACM só permitem que sejam associados aos recursos os algoritmos e os tamanhos de chaves que eles suportam. Por exemplo, suporta CloudFront somente chaves RSA de 1024 bits, RSA de 2048 bits, RSA de 3072 bits e Elliptic Prime Curve de 256 bits, enquanto o Application Load Balancer oferece suporte a todos os algoritmos disponíveis no ACM. Para obter mais informações, consulte a documentação do serviços que você está usando.
- O certificado deve ser um certificado SSL/TLS X.509 versão 3. Ele deve conter uma chave pública, o nome de domínio totalmente qualificado (FQDN) ou o endereço IP para o seu site e informações sobre o emissor.
- Um certificado pode ser autoassinado por uma chave privada de sua propriedade ou assinado pela chave privada de uma CA emissora. Você deve fornecer a chave privada, que não pode ter mais de 5 KB (5.120 bytes) e não deve ser criptografada.



- Se o certificado for assinado por uma CA e você optar por fornecer a cadeia de certificados, a cadeia deverá ser codificada por PEM.
- O certificado deve estar válido no momento da importação. Você não pode importar um certificado antes de seu período de validade começar nem depois de ele expirar. O campo `NotBefore` do certificado contém a data de início da validade e o campo `NotAfter` contém a data de término.
- Todos os materiais necessários para o certificado (o certificado, a chave privada e a cadeia de certificação) devem ser codificados em PEM. O upload de materiais codificados por DER gerará um erro. Para ter mais informações e exemplos, consulte [Formato de chaves e certificados para importação](#).
- Quando você renovar (reimportar) um certificado, não é possível adicionar uma extensão `KeyUsage` ou `ExtendedKeyUsage` se a extensão não estiver presente no certificado importado anteriormente.
- AWS CloudFormation não suporta a importação de certificados para o ACM.

## Formato de chaves e certificados para importação

O ACM exige que você importe separadamente o certificado, a cadeia de certificados e a chave privada (se houver) e codifique cada componente no formato PEM. PEM significa Privacy Enhanced Mail (E-mails reforçados para privacidade). O formato PEM é frequentemente usado para representar certificados, solicitações de certificado, cadeias de certificados e chaves. A extensão típica para um arquivo formatado como PEM é `.pem`, mas não precisa ser.

### Note

AWS não fornece utilitários para manipular arquivos PEM ou outros formatos de certificado. Os exemplos a seguir dependem de um editor de texto genérico para operações simples. Se você precisar executar tarefas mais complexas (como converter formatos de arquivo ou extrair chaves), ferramentas gratuitas e de código aberto, como o [OpenSSL](#) estão prontamente disponíveis.

Os exemplos a seguir ilustram o formato dos arquivos a serem importados. Se os componentes vierem em um único arquivo, use um editor de texto (cuidadosamente) para separá-los em três arquivos. Observe que se você editar qualquer um dos caracteres de forma incorreta em um arquivo PEM, ou se adicionar um ou mais espaços no final de qualquer linha, o certificado, a cadeia de certificados ou a chave privada serão invalidados.

## Example 1. O certificado codificado em PEM

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

## Example 2. A cadeia de certificados codificada em PEM

Uma cadeia de certificados contém um ou mais certificados. Você pode usar um editor de texto, o comando copy no Windows ou o comando cat do Linux para concatenar os arquivos de certificado em uma cadeia. Os certificados devem ser concatenados em ordem para que cada um certifique diretamente o certificado anterior. Se estiver importando um certificado privado, copie o certificado raiz por último. O exemplo a seguir contém três certificados, mas sua cadeia de certificados pode conter mais ou menos.

### Important

Não copie o seu certificado para a cadeia de certificados.

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

## Example 3. As chaves privadas codificadas em PEM

Os certificados X.509 versão 3 utilizam algoritmos de chave pública. Quando você cria um certificado ou solicitação de certificado X.509, especifica o algoritmo e o tamanho em bits da chave, que devem ser usados para criar o par de chaves privada-pública. A chave pública é colocada no certificado ou na solicitação. Você deve manter a chave privada associada em segredo. Especifique a chave privada quando você importar o certificado. A chave não deve estar criptografada. O exemplo a seguir mostra uma chave privada RSA.

```
-----BEGIN RSA PRIVATE KEY-----
```

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

O próximo exemplo mostra uma chave privada de curva elíptica codificada em PEM. Dependendo de como você cria a chave, os blocos de parâmetros podem não ser incluídos. Se o bloco de parâmetros estiver incluído, o ACM o removerá antes de usar a chave durante o processo de importação.

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

## Importação de um certificado

Você pode importar um certificado obtido externamente (ou seja, um fornecido por um provedor terceirizado de serviços confiáveis) para o ACM usando a API AWS Management Console AWS CLI, a ou a ACM. Os tópicos a seguir mostram como usar o AWS Management Console e AWS CLI. Os procedimentos para obter um certificado de um nãoAWS emissor estão fora do escopo deste guia.

### Important

O algoritmo de assinatura selecionado deve atender aos [Pré-requisitos para importação de certificados](#).

### Tópicos

- [Importar \(console\)](#)
- [Importar \(AWS CLI\)](#)

## Importar (console)

O exemplo a seguir mostra como importar um certificado usando o AWS Management Console.

1. Abra o console do ACM em <https://console.aws.amazon.com/acm/home>. Se esta for a primeira vez que você usa o ACM, procure o cabeçalho do AWS Certificate Manager e escolha o botão Comece a usar abaixo dele.
2. Selecione Importar um certificado.
3. Faça o seguinte:
  - a. Para Corpo do certificado, cole o certificado codificado PEM a importar. Deve começar com -----BEGIN CERTIFICATE----- e terminar com -----END CERTIFICATE-----.
  - b. Para chave privada do certificado, cole a chave privada descryptografada codificada em PEM do certificado. Deve começar com -----BEGIN PRIVATE KEY----- e terminar com -----END PRIVATE KEY-----.
  - c. (Opcional) Para Corpo do certificado, cole a cadeia do certificado codificado PEM.
4. Selecione Revisar e importar.
5. Na página Review and import (Revisar e importar), verifique os metadados exibidos sobre seu certificado para garantir que ele é o que você queria. Estes campos incluem:
  - Domains (Domínios) – Uma lista de nomes de domínio totalmente qualificados (FQDN) autenticados pelo certificado
  - Expires in (Expira em) – O número de dias até que o certificado expire
  - Public key info (Informações da chave pública) – O algoritmo criptográfico usado para gerar o par de chaves
  - Signature algorithm (Algoritmo de assinatura) – O algoritmo criptográfico usado para criar a assinatura do certificado
  - Can be used with (Pode ser usado com) – Uma lista dos [serviços integrados](#) do ACM que suportam o tipo de certificado que você está importando

Se tudo estiver correto, escolha Import( Importar).

## Importar (AWS CLI)

O exemplo a seguir mostra como importar um certificado usando o [AWS Command Line Interface \(AWS CLI\)](#). O exemplo supõe o seguinte:

- O certificado codificado PEM está armazenado em um arquivo chamado `Certificate.pem`.

- A cadeia do certificado codificado PEM está armazenada em um arquivo chamado `CertificateChain.pem`.
- A chave privada não criptografada codificada PEM está armazenada em um arquivo chamado `PrivateKey.pem`.

Para usar o exemplo a seguir, substitua os nomes de arquivos com os nomes dos seus e digite o comando em uma única linha contínua. O exemplo a seguir inclui quebras de linha e espaços extras para facilitar a leitura.

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

Se o comando `import-certificate` for bem-sucedido, ele retorna o [Amazon Resource Name \(ARN\)](#) do certificado importado.

## Reimportação de um certificado

Se você importou um certificado e o associou a outros AWS serviços, poderá reimportar esse certificado antes que ele expire, preservando as associações de AWS serviço do certificado original. Para obter mais informações sobre AWS serviços integrados ao ACM, consulte [Serviços integrados com AWS Certificate Manager](#).

As seguintes condições se aplicam ao reimportar um certificado:

- Você pode adicionar ou remover nomes de domínio.
- Você não pode remover todos os nomes de domínio de um certificado.
- Se as extensões Key Usage estiverem presentes no certificado originalmente importado, você poderá adicionar novos valores de extensão, mas não é possível remover os valores existentes.
- Se as extensões Extended Key Usage estiverem presentes no certificado originalmente importado, você poderá adicionar novos valores de extensão, mas não é possível remover os valores existentes.
- O tipo e o tamanho de chaves não podem ser alterados.
- Não é possível aplicar tags de recurso ao reimportar um certificado.

### Tópicos

- [Reimportar \(console\)](#)
- [Reimportar \(AWS CLI\)](#)

## Reimportar (console)

O exemplo a seguir mostra como reimportar um certificado usando o AWS Management Console.


1. Abra o console do ACM em <https://console.aws.amazon.com/acm/home>.
2. Selecione ou expanda o certificado para reimportação.
3. Abra o painel de detalhes do certificado e escolha o botão Reimportar certificado. Se você selecionou o certificado marcando a caixa de seleção ao lado do nome dele, escolha Reimportar certificado no menu Ações.
4. Para Corpo do certificado, cole o certificado da entidade final codificado em PEM.
5. Para a Chave privada do certificado, cole a chave privada não criptografada e codificada PEM associada à chave pública do certificado.
6. (Opcional) Para Corpo do certificado, cole a cadeia do certificado codificado PEM. A cadeia de certificados inclui um ou mais certificados para todas as autoridades emissoras de certificação intermediárias e o certificado raiz. Se o certificado a ser importado é autoatribuído, nenhuma cadeia de certificados é necessária.
7. Selecione Revisar e importar.
8. Revise as informações sobre seu certificado. Se não houver erros, escolha Reimportar.

## Reimportar (AWS CLI)

O exemplo a seguir mostra como reimportar um certificado usando o [AWS Command Line Interface \(AWS CLI\)](#). O exemplo supõe o seguinte:

- O certificado codificado PEM está armazenado em um arquivo chamado `Certificate.pem`.
- A cadeia do certificado codificado PEM está armazenada em um arquivo chamado `CertificateChain.pem`.
- (Somente certificados privados) A chave privada não criptografada codificada em PEM é armazenada em um arquivo chamado `PrivateKey.pem`.
- Você tem o ARN do certificado que deseja reimportar.

Para usar o exemplo a seguir, substitua os nomes de arquivos e o ARN pelos nomes dos seus e digite o comando em uma única linha contínua. O exemplo a seguir inclui quebras de linha e espaços extras para facilitar a leitura.

 Note

Para reimportar um certificado, você deve especificar o ARN do certificado.

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

Se o comando `import-certificate` for bem-sucedido, ele retorna o [Nome de recurso da Amazon \(ARN\)](#) do certificado.

# Exportação de um certificado privado

Você pode exportar um certificado emitido pela CA privada da AWS para uso em qualquer lugar em seu ambiente privado de PKI. O arquivo exportado contém o certificado, a cadeia de certificados e a chave privada criptografada. Esse arquivo deve ser armazenado com segurança. Para obter mais informações sobre CA privada da AWS, consulte o [Guia AWS Private Certificate Authority do usuário](#).

## Note

Você não pode exportar um certificado publicamente confiável ou sua chave privada, independentemente de ele ter sido emitido pelo ACM ou importado.

## Tópicos

- [Exportação de um certificado privado \(console\)](#)
- [Exportar um certificado privado \(CLI\)](#)

## Exportação de um certificado privado (console)

1. Faça login no AWS Management Console e abra o console do ACM em <https://console.aws.amazon.com/acm/home>.
2. Escolha Certificate Manager
3. Selecione o link do certificado que deseja exportar.
4. Escolha Exportar.
5. Insira e confirme uma frase secreta para a chave privada.

## Note

Ao criar sua senha, você pode usar qualquer caractere ASCII, exceto #, \$ ou %.

6. Escolha Generate PEM Encoding (Gerar codificação PEM).
7. É possível copiar o certificado, a cadeia de certificados e a chave criptografada na memória ou escolher Export to a file (Exportar para um arquivo) para cada um deles.
8. Selecione Done (Concluído).



## Exportar um certificado privado (CLI)

Use o comando [export-certificate](#) para exportar um certificado e uma chave privados. É necessário atribuir uma senha quando você executa o comando. Para maior segurança, use um editor de arquivos para armazenar sua senha em um arquivo e, depois, forneça a senha fornecendo o arquivo. Isso evita que a frase secreta seja armazenada no histórico de comandos e impede que outras pessoas a vejam enquanto você a digita.

### Note

O arquivo que contém a senha não deve terminar em um terminador de linha. Você pode verificar seu arquivo de senha assim:

```
$ file -k passphrase.txt
passphrase.txt: ASCII text, with no line terminators
```

O exemplo a seguir redireciona a saída do comando para jq a fim de aplicar a formatação PEM.

[Linux]

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

[Windows]

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

Isso gera um certificado no formato PEM e codificado em Base64, que também contém a cadeia de certificados e a chave privada criptografada, como no exemplo abreviado a seguir.

```
-----BEGIN CERTIFICATE-----
MIIDTCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMjkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwW0dL0kxpwkkKWtcEkQuHE1v5Vn6HpbFfMxkdPEasoDhthH
```

```

FFWIf4/+V01bDLgju4HgtmV4IJDtqM9rG0Z42eFYmmc3eQ00GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmnnS8j6YxmtPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAduGAWIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMtkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQKDAh0cm9sb2xvbDCCASIwDQYJKoZIhvcNAQEBBQADggEP
...
j2PA0viqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPd1+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBGkqhkiG9w0BBQ0wSDANBgkqhkiG9w0BBQwwGgQUmrZb7kZJ8nTZg7aB
1zmaQh4vwloCAGgAMB0GCWCGSAF1AwQBKqGQDViROIHStQgN0jR6nTUuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTpskNCdCAHqdh0SqBwt65qUTZe3gBt
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrXuHTWjF1
wEuqyd8X/ApkQsYFX/nhep0EIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxf0C1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs90V/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----

```

Para gerar tudo em um arquivo, acrescente o redirecionador > ao exemplo anterior, resultando no seguinte.

```

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

```

# Marcação de certificados do AWS Certificate Manager

Uma tag é um rótulo que você pode atribuir a um certificado do ACM. Cada tag consiste em uma chave e um valor. Você pode usar o console do AWS Certificate Manager, a AWS Command Line Interface (AWS CLI) ou a API do ACM para adicionar, exibir ou remover tags para certificados do ACM. Você pode escolher as tags a serem exibidas no console do ACM.

Você pode criar tags personalizadas que atendam às suas necessidades. Por exemplo, você pode atribuir tags a vários certificados do ACM com uma tag `Environment = Prod` ou `Environment = Beta` para identificar o ambiente a que se destina cada certificado do ACM. A lista a seguir inclui alguns exemplos adicionais de outras tags personalizadas:

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

Outros recursos da AWS também dão suporte à marcação. Você pode, portanto, atribuir a mesma tag a diferentes recursos para indicar se esses recursos estão relacionados. Por exemplo, você pode atribuir uma tag como `Website = example.com` ao certificado do ACM, ao balanceador de carga e a outros recursos usados para o seu site `exemplo.com`.

## Tópicos

- [Restrições de tags](#)
- [Gerenciar tags](#)

## Restrições de tags

As seguintes restrições básicas se aplicam a tags de certificados do ACM:

- O número máximo de tags por certificado do ACM é 50.
- O tamanho máximo de uma chave de tag é 127 caracteres.
- O tamanho máximo de um valor de tag é 255 caracteres.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.

- O prefixo `aws :` é reservado para uso da AWS, não é possível adicionar, editar nem excluir tags cujas chaves comecem com `aws :`. As tags que começam com `aws :` não são consideradas para a cota de tags por recurso.
- Se você planeja usar o esquema de tags em vários serviços e recursos, lembre-se de que outros serviços podem ter outras restrições para caracteres permitidos. Consulte a documentação desse serviço.
- As tags de certificados do ACM não estão disponíveis para uso nos [Resource Groups e no editor de tags do AWS Management Console](#).

Para obter informações gerais sobre convenções de marcação da AWS, consulte [Marcação de recursos da AWS](#).

## Gerenciar tags

Você pode adicionar, editar e excluir as tags usando o Console de gerenciamento do AWS, o AWS Command Line Interface ou a API AWS Certificate Manager.

### Gerenciamento de tags (console)

Você pode usar o AWS Management Console para adicionar, excluir ou editar tags. Você também pode exibir tags em colunas.

#### Adição de uma tag

Use o procedimento a seguir para adicionar tags usando o console do ACM.

Para adicionar uma tag a um certificado (console)

1. Faça login no AWS Management Console e abra o console do AWS Certificate Manager em <https://console.aws.amazon.com/ses/home>.
2. Escolha a seta próxima ao certificado ao qual você deseja adicionar uma tag.
3. No painel de detalhes, role para baixo até Tags.
4. Selecione Editar e Adicionar tag.
5. Digite uma chave e um valor para a tag.
6. Escolha Save (Salvar).

## Exclusão de uma tag

Use o procedimento a seguir para excluir tags usando o console do ACM.

Para excluir uma tag (console)

1. Faça login no AWS Management Console e abra o console do AWS Certificate Manager em <https://console.aws.amazon.com/ses/home>.
2. Escolha a seta ao lado do certificado com uma tag que você deseja excluir.
3. No painel de detalhes, role para baixo até Tags.
4. Escolha Editar.
5. Escolha o X ao lado da tag que você deseja excluir.
6. Escolha Save (Salvar).

## Edição de uma tag

Use o procedimento a seguir para editar tags usando o console do ACM.

Para editar uma tag (console)

1. Faça login no AWS Management Console e abra o console do AWS Certificate Manager em <https://console.aws.amazon.com/ses/home>.
2. Escolha a seta ao lado do certificado que você deseja editar.
3. No painel de detalhes, role para baixo até Tags.
4. Escolha Editar.
5. Modifique a chave ou o valor da tag que você deseja alterar.
6. Escolha Save (Salvar).

## Exibição de tags em colunas

Use o procedimento a seguir para mostrar tags em colunas no console do ACM.

Para exibir tags em colunas (console)

1. Faça login no AWS Management Console e abra o console do AWS Certificate Manager em <https://console.aws.amazon.com/ses/home>.

2. Escolha as tags que deseja exibir como colunas selecionando o ícone de engrenagem



no canto superior direito do console.

3. Selecione a caixa de seleção ao lado da tag que você deseja exibir em uma coluna.

## Gerenciamento de tags (CLI)

Consulte os tópicos a seguir para saber como adicionar, listar e excluir tags usando AWS CLI.

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

## Gerenciamento de tags (API do ACM)

Consulte os tópicos a seguir para saber como adicionar, listar e excluir tags usando a API.

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

# Monitoramento e registro AWS Certificate Manager

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Certificate Manager suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra.

Os tópicos a seguir descrevem as ferramentas AWS de monitoramento de nuvem disponíveis para uso com o ACM.

## Tópicos

- [Usando a Amazon EventBridge](#)
- [Usando CloudTrail com AWS Certificate Manager](#)
- [CloudWatch Métricas suportadas](#)

## Usando a Amazon EventBridge

Você pode usar a [Amazon EventBridge](#) (antiga CloudWatch Events) para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Eventos de AWS serviços, incluindo o ACM, são entregues à Amazon quase EventBridge em tempo real. Você pode usar eventos para acionar alvos, incluindo AWS Lambda funções, AWS Batch trabalhos, tópicos do Amazon SNS e muitos outros. Para obter mais informações, consulte [O que é a Amazon EventBridge?](#)

## Tópicos

- [EventBridge Suporte da Amazon para ACM](#)
- [Acionando ações com a Amazon EventBridge no ACM](#)

## EventBridge Suporte da Amazon para ACM

Este tópico lista e descreve os eventos relacionados ao ACM apoiados pela Amazon EventBridge.

## Evento de expiração do certificado ACM se aproximando

O ACM envia eventos diários de expiração para todos os certificados (públicos, privados e importados) começando 45 dias antes da expiração. Esse tempo pode ser alterado usando a [PutAccountConfiguration](#) da API do ACM.

O ACM inicia automaticamente a renovação dos certificados elegíveis emitidos, mas os certificados importados precisam ser reemitidos e reimportados antes da expiração para evitar interrupções. Para obter mais informações, consulte [Reimportar um certificado](#). Você pode usar eventos de expiração para configurar a automação para reimportar certificados para o ACM. Para obter um exemplo de uso de automação AWS Lambda, consulte [Acionando ações com a Amazon EventBridge no ACM](#).

Os eventos ACM Certificate Approaching Expiration (Expiração do certificado ACM se aproximando) têm a seguinte estrutura.

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

## Evento de certificado ACM expirado

### Note

Eventos de certificado expirado não estão disponíveis para [certificados importados](#).

Os clientes podem ouvir esse evento para alertá-los se um certificado público ou privado emitido pelo ACM em sua conta expirar.



Os eventos ACM Certificate Expired (Certificado ACM expirado) têm a seguinte estrutura.

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

## Evento Certificado ACM disponível

Os clientes podem ouvir esse evento para serem notificados quando um certificado público ou privado gerenciado estiver pronto para uso. O evento é publicado sobre emissão, renovação e importação. Para um certificado privado, uma vez disponível, a ação do cliente ainda é necessária para implantá-lo nos hosts.

Os eventos ACM Certificate Available (Certificado ACM disponível) têm a seguinte estrutura.

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

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

## Evento obrigatório de ação de renovação do certificado ACM

### Note

Ação de renovação de certificado Os eventos obrigatórios não estão disponíveis para [certificados importados](#).

Os clientes podem ouvir esse evento para serem alertados quando uma ação do cliente deve ser executada antes que um certificado possa ser renovado. Por exemplo, se um cliente adicionar registros CAA que impeçam o ACM de renovar um certificado, o ACM publicará esse evento quando a renovação automática falhar 45 dias antes da expiração. Se nenhuma ação do cliente for tomada, o ACM fará novas tentativas de renovação em 30 dias, 15 dias, 3 dias e 1 dia, ou até que a ação do cliente seja tomada, o certificado expire ou o certificado não esteja mais qualificado para renovação. Um evento é publicado para cada uma dessas tentativas de renovação.

Os eventos ACM Certificate Renewal Action Required (Ação de renovação do certificado ACM necessária) têm a seguinte estrutura.

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

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

## AWS eventos de saúde

AWS eventos de saúde são gerados para certificados ACM que são elegíveis para renovação. Para obter mais informações sobre elegibilidade para renovação, consulte [Renovação gerenciada para certificados do ACM](#).

Os eventos de integridade são gerados em dois cenários:

- Sobre a renovação bem-sucedida de um certificado público ou privado.
- Quando um cliente precisa atuar para que uma renovação ocorra. Isso pode significar clicar em um link em uma mensagem de e-mail (para certificados validados por e-mail) ou resolver um erro. Um dos seguintes códigos de tipo de evento está incluído em cada evento. Os códigos são expostos como variáveis que você pode usar para filtrar.
  - AWS\_ACM\_RENEWAL\_STATE\_CHANGE (o certificado foi renovado, expirou ou está prestes a expirar)
  - CAA\_CHECK\_FAILURE (falha na verificação de CAA)
  - AWS\_ACM\_RENEWAL\_FAILURE (para certificados assinados por uma CA privada)

Os eventos de integridade têm a seguinte estrutura. Neste exemplo, um evento AWS\_ACM\_RENEWAL\_STATE\_CHANGE foi gerado.

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

## Acionando ações com a Amazon EventBridge no ACM

Você pode criar EventBridge regras da Amazon com base nesses eventos e usar o EventBridge console da Amazon para configurar ações que ocorrem quando os eventos são detectados. Esta seção fornece exemplos de procedimentos para configurar EventBridge as regras da Amazon e as ações resultantes.

### Tópicos

- [Resposta a um evento com o Amazon SNS](#)
- [Resposta a um evento com uma função do Lambda](#)

## Resposta a um evento com o Amazon SNS

Esta seção mostra como configurar o Amazon SNS para enviar uma notificação de texto sempre que o ACM gerar um evento de integridade.

Conclua o procedimento a seguir para configurar uma resposta.

## Para criar uma EventBridge regra da Amazon e acionar uma ação

1. Crie uma EventBridge regra da Amazon. Para obter mais informações, consulte [Criação de EventBridge regras da Amazon que reagem a eventos](#).
  - a. No EventBridge console da Amazon em <https://console.aws.amazon.com/events/>, navegue até a página Eventos > Regras e escolha Criar regra.
  - b. Na página Create rule (Criar regra), selecione Event Pattern (Padrão do evento).
  - c. Para Service Name (Nome do serviço), escolha Health (Integridade) no menu.
  - d. Para Event Type (Tipo de evento), escolha Specific Health events (Eventos de integridade específicos).
  - e. Selecione Specific service(s) (Serviço(s) específico(s)) e escolha ACM no menu.
  - f. Selecione Specific event type category(s) (Categoria(s) de tipo de evento específico) e escolha AccountNotification.
  - g. Selecione Any event type code (código de tipo qualquer evento).
  - h. Escolha Any resource (Qualquer recurso).
  - i. No editor Event pattern preview (Previsualização do padrão do evento, cole o padrão JSON emitido pelo evento. Este exemplo usa o padrão da seção [AWS eventos de saúde](#).

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

```
}
```

## 2. Configurar uma ação.

Na seção Targets (Destinos), você pode escolher entre muitos serviços que podem consumir imediatamente seu evento, como o Amazon Simple Notification Service (SNS), ou você pode escolher Lambda function (Função do Lambda) para passar o evento para o código executável personalizado. Para obter um exemplo de implementação do AWS Lambda, consulte [Resposta a um evento com uma função do Lambda](#).

## Resposta a um evento com uma função do Lambda

Esse procedimento demonstra como usar AWS Lambda para escutar na Amazon EventBridge, criar notificações com o Amazon Simple Notification Service (SNS) e publicar descobertas AWS Security Hub, fornecendo visibilidade aos administradores e equipes de segurança.

Para configurar uma função do Lambda e uma função do IAM

1. Primeiro, configure uma função AWS Identity and Access Management (IAM) e defina as permissões necessárias para a função Lambda. Essa prática recomendada de segurança oferece flexibilidade na designação de quem tem autorização para chamar a função e na limitação das permissões concedidas a essa pessoa. Não é recomendável executar a maioria das AWS operações diretamente em uma conta de usuário e, especialmente, em uma conta de administrador.

Abra o console IAM em <https://console.aws.amazon.com/iam/>.

2. Use o editor de políticas JSON para criar a política definida no modelo abaixo. Forneça sua própria região e detalhes AWS da conta. Para obter mais informações, consulte [Criação de políticas na guia JSON](#).

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

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

```
]
}
```

3. Criar uma função do IAM e associar a ela a nova política. Para obter informações sobre como criar uma função do IAM e anexar uma política, consulte [Criação de uma função para um AWS serviço \(console\)](#).
4. Abra o AWS Lambda console em <https://console.aws.amazon.com/lambda/>.
5. Criar a função do Lambda. Para obter mais informações, consulte [Criar uma função do Lambda no console](#). Execute as etapas a seguir:
  - a. Na página Create function (Criar função), selecione Author from scratch (Criar do zero).
  - b. Especifique um nome como "handle-expiring-certificates" no campo Nome da função.
  - c. Na lista Runtime (Tempo de execução), escolha Python 3.8.
  - d. Amplie Change default execution role (Alterar função de execução padrão) e escolha Use an existing role (Usar uma função existente).
  - e. Na lista Existing role (Função existente), escolha a função criada acima.
  - f. Escolha Create function (Criar função).
  - g. Em Function code (Código da função), cole o seguinte código:

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



```
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH
THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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

```
        response = result
    else:
        sns_client = boto3.client('sns')
        response = sns_client.publish(TopicArn=os.environ['SNS_TOPIC_ARN'],
Message=result, Subject='Certificate Expiration Notification')
    return result
def log_finding_to_sh(event, cert_details, context_arn):
    # setup for security hub
    sh_region = get_sh_region(event['region'])
    sh_hub_arn = "arn:aws:securityhub:{0}:{1}:hub/default".format(sh_region,
event['account'])
    sh_product_arn = "arn:aws:securityhub:{0}:{1}:product/{1}/
default".format(sh_region, event['account'])
    # check if security hub is enabled, and if the hub arn exists
    sh_client = boto3.client('securityhub', region_name = sh_region)
    try:
        sh_enabled = sh_client.describe_hub(HubArn = sh_hub_arn)
        # the previous command throws an error indicating the hub doesn't exist or
lambda doesn't have rights to it so we'll stop attempting to use it
    except Exception as error:
        sh_enabled = None
        print ('Default Security Hub product doesn\'t exist')
        response = 'Security Hub disabled'
    # This is used to generate the URL to the cert in the Security Hub Findings
to link directly to it
    cert_id = right(cert_details['Certificate']['CertificateArn'], 36)
    if sh_enabled:
        # set up a new findings list
        new_findings = []
        # add expiring certificate to the new findings list
        new_findings.append({
            "SchemaVersion": "2018-10-08",
            "Id": cert_id,
            "ProductArn": sh_product_arn,
            "GeneratorId": context_arn,
            "AwsAccountId": event['account'],
            "Types": [
                "Software and Configuration Checks/AWS Config Analysis"
            ],
            "CreatedAt": event['time'],
            "UpdatedAt": event['time'],
            "Severity": {
                "Original": '89.0',
                "Label": 'HIGH'
            }
        })
```

```

    },
    "Title": 'Certificate expiration',
    "Description": 'cert expiry',
    'Remediation': {
        'Recommendation': {
            'Text': 'A new certificate for ' +
cert_details['Certificate']['DomainName'] + ' should be imported to replace
the existing imported certificate before expiration',
            'Url': "https://console.aws.amazon.com/acm/home?region=" +
event['region'] + "#/?id=" + cert_id
        }
    },
    'Resources': [
        {
            'Id': event['id'],
            'Type': 'ACM Certificate',
            'Partition': 'aws',
            'Region': event['region']
        }
    ],
    'Compliance': {'Status': 'WARNING'}
}))
# push any new findings to security hub
if new_findings:
    try:
        response =
sh_client.batch_import_findings(Findings=new_findings)
        if response['FailedCount'] > 0:
            print("Failed to import {}
findings".format(response['FailedCount']))
        except Exception as error:
            print("Error: ", error)
            raise
    return json.dumps(response)
# function to setup the sh region
def get_sh_region(event_region):
    # security hub findings may need to go to a different region so set that
    here
    if os.environ.get('SECURITY_HUB_REGION') is None:
        sh_region_local = event_region
    else:
        sh_region_local = os.environ['SECURITY_HUB_REGION']
    return sh_region_local
# quick function to trim off right side of a string

```

```
def right(value, count):  
    # To get right part of string, use negative first index in slice.  
    return value[-count:]
```

h. Em Environment variables (Variáveis de ambiente), escolha Edit (Editar) e, opcionalmente, adicione as seguintes variáveis.

- (Opcional) EXPIRY\_DAY

Especifica quanto tempo antes, em dias, será enviado o aviso de expiração de validade do certificado. O padrão da função é 45 dias, mas você pode especificar valores personalizados.

- (Opcional) SNS\_TOPIC\_ARN

Especifica um ARN para um Amazon SNS. Forneça o ARN completo no formato `arn:aws:sns:<região>:<número-conta>:<nome-tópico>`.

- (Opcional) SECURITY\_HUB\_REGION

Especifica um AWS Security Hub em uma região diferente. Se isso não for especificado, a região da função Lambda em execução será usada. Se a função for executada em várias regiões, é melhor que todas as mensagens de certificado sejam enviadas para o Security Hub em uma única região.

- i. Em Basic settings (Configurações básicas), defina o valor Timeout (Tempo limite) como 30 segundos.
- j. Na parte superior da página, escolha Deploy (Implantar).

Conclua as tarefas do procedimento a seguir para começar a usar essa solução.

Para automatizar um aviso de expiração de validade por e-mail

Neste exemplo, fornecemos um único e-mail para cada certificado expirado no momento em que o evento é gerado pela Amazon EventBridge. Por padrão, o ACM gera um evento por dia para um certificado a 45 dias ou menos da expiração da validade. (Esse período pode ser personalizado usando a [PutAccountConfiguration](#) operação da API do ACM.) Cada um desses eventos dispara a seguinte cascata de ações automatizadas:

```
ACM raises Amazon EventBridge event #  
>>>>>> events
```

```
Event matches Amazon EventBridge rule #
```

```
Rule calls Lambda function #
```

```
Function sends SNS email and logs a Finding in Security
```

```
Hub
```

1. Criar a função do Lambda e configurar permissões. (Já concluído – consulte [Para configurar uma função do Lambda e uma função do IAM](#)).
2. Criar um tópico padrão do SNS para a função do Lambda usar para enviar notificações. Para obter mais informações, consulte [Criação de um tópico do Amazon SNS](#).
3. Inscreva todas as partes interessadas no novo tópico SNS. Para obter mais informações, consulte [Assinatura de um tópico do Amazon SNS](#).
4. Crie uma EventBridge regra da Amazon para acionar a função Lambda. Para obter mais informações, consulte [Criação de EventBridge regras da Amazon que reagem a eventos](#).

No EventBridge console da Amazon em <https://console.aws.amazon.com/events/>, navegue até a página Eventos > Regras e escolha Criar regra. Especifique o nome do serviço, o tipo de evento, e a função do Lambda. No editor Event Pattern preview (Previsualização do padrão de evento), cole o seguinte código:

```
{
  "source": [
    "aws.acm"
  ],
  "detail-type": [
    "ACM Certificate Approaching Expiration"
  ]
}
```

Um evento como o que o Lambda recebe é exibido em Show sample event(s) (Mostrar exemplo de evento (s)):

```
{
  "version": "0",
  "id": "9c95e8e4-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "ACM Certificate Approaching Expiration",
  "source": "aws.acm",
  "account": "123456789012",
```

```
"time": "2020-09-30T06:51:08Z",
"region": "us-east-1",
"resources": [
  "arn:aws:acm:us-east-1:123456789012:certificate/61f50cd4-45b9-4259-b049-
d0a53682fa4b"
],
"detail": {
  "DaysToExpiry": 31,
  "CommonName": "My Awesome Service"
}
}
```

### Para limpar

Quando você não precisar mais do exemplo de configuração, ou de qualquer configuração, é uma prática recomendada remover todos os traços para evitar problemas de segurança e cobranças futuras inesperadas:

- Política e função do IAM
- Função do Lambda
- CloudWatch Regra de eventos
- CloudWatch Registros associados ao Lambda
- Tópico do SNS

## Usando CloudTrail com AWS Certificate Manager

AWS Certificate Manager é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ACM. CloudTrail está ativado por padrão em sua AWS conta. CloudTrail captura chamadas de API para o ACM como eventos, incluindo chamadas do console do ACM e chamadas de código para as operações da API do ACM. Se você configurar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o ACM. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao ACM, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#). Quando uma atividade de evento suportada ocorre no ACM, essa atividade

é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS .

Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros.

Para obter mais informações sobre CloudTrail, consulte a seguinte documentação:

- [AWS CloudTrail Guia do usuário](#).
- [Visão geral da criação de uma trilha](#)
- [CloudTrail Serviços e integrações compatíveis](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [recebendo arquivos de CloudTrail log de várias contas](#)

## Tópicos

- [Ações da API ACM suportadas no registro CloudTrail](#)
- [Registro em log chamadas de API para serviços integrados](#)

## Ações da API ACM suportadas no registro CloudTrail

O ACM suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com as credenciais do usuário Usuário raiz da conta da AWS ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte o elemento [CloudTrailUserIdentity](#).

As seções a seguir fornecem exemplos de logs para as operações de API compatíveis.

- [Adição de tags a um certificado \(AddTagsToCertificate\)](#)

- [Exclusão de um certificado \(DeleteCertificate\)](#)
- [Descrição de um certificado \(DescribeCertificate\)](#)
- [Exportação de um certificado \(ExportCertificate\)](#)
- [Importar um certificado \(ImportCertificate\)](#)
- [Lista de certificados \(ListCertificates\)](#)
- [Lista de tags para um certificado \(ListTagsForCertificate\)](#)
- [Remoção das tags de um certificado \(RemoveTagsFromCertificate\)](#)
- [Solicitação de um certificado \(RequestCertificate\)](#)
- [Reenvio do e-mail de validação \(ResendValidationEmail\)](#)
- [Recuperação de um certificado \(GetCertificate\)](#)

## Adição de tags a um certificado ([AddTagsToCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [AddTagsToCertificate](#) API.

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-04-06T13:53:53Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "AddTagsToCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.10.16",
      "requestParameters": {
        "tags": [
          {
            "value": "Alice",
```



```

        "key": "Admin"
      }
    ],
    "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
  },
  "responseElements": null,
  "requestID": "fedcba98-7654-3210-fedc-ba9876543210",
  "eventID": "fedcba98-7654-3210-fedc-ba9876543210",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
]
}

```

## Exclusão de um certificado ([DeleteCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [DeleteCertificate](#) API.

```

{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:26Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "DeleteCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
      },
      "responseElements": null,
    }
  ]
}

```

```
    "requestID": "01234567-89ab-cdef-0123-456789abcdef",
    "eventID": "01234567-89ab-cdef-0123-456789abcdef",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }
]
```

## Descrição de um certificado ([DescribeCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [DescribeCertificateAPI](#).

### Note

O CloudTrail registro da `DescribeCertificate` operação não exibe informações sobre o certificado ACM que você especifica. Você pode visualizar informações sobre o certificado usando o console AWS Command Line Interface, o ou a [DescribeCertificateAPI](#).

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:42Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "DescribeCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/fedcba98-7654-3210-fedc-ba9876543210"
      },
      "responseElements": null,
    }
  ]
}
```

```
    "requestID":"fedcba98-7654-3210-fedc-ba9876543210",
    "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
  }
]
}
```

## Exportação de um certificado ([ExportCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [ExportCertificate](#) API.

```
{
  "Records":[
    {
      "version":"0",
      "id":"01234567-89ab-cdef-0123-456789abcdef",
      "detail-type":"AWS API Call via CloudTrail",
      "source":"aws.acm",
      "account":"123456789012",
      "time":"2018-05-24T15:28:11Z",
      "region":"us-east-1",
      "resources":[

    ],
    "detail":{
      "eventVersion":"1.04",
      "userIdentity":{
        "type":"Root",
        "principalId":"123456789012",
        "arn":"arn:aws:iam::123456789012:user/Alice",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"Alice"
      },
      "eventTime":"2018-05-24T15:28:11Z",
      "eventSource":"acm.amazonaws.com",
      "eventName":"ExportCertificate",
      "awsRegion":"us-east-1",
      "sourceIPAddress":"192.0.2.0",
      "userAgent":"aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4",
      "requestParameters":{
        "passphrase":{
```

```
        "hb": [
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42
        ],
        "offset": 0,
        "isReadOnly": false,
        "bigEndian": true,
        "nativeByteOrder": false,
        "mark": -1,
        "position": 0,
        "limit": 10,
        "capacity": 10,
        "address": 0
    },
    "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
},
"responseElements": {
    "certificateChain":
        "-----BEGIN CERTIFICATE-----
        base64 certificate
        -----END CERTIFICATE-----
        -----BEGIN CERTIFICATE-----
        base64 certificate
        -----END CERTIFICATE-----",
    "privateKey": "*****",
    "certificate":
        "-----BEGIN CERTIFICATE-----
        base64 certificate
        -----END CERTIFICATE-----"
},
"requestID": "01234567-89ab-cdef-0123-456789abcdef",
"eventID": "fedcba98-7654-3210-fedc-ba9876543210",
"eventType": "AwsApiCall"
}
}
```

```
]
}
```

## Importar um certificado ([ImportCertificate](#))

O exemplo a seguir mostra a entrada de CloudTrail registro que registra uma chamada para a operação da [ImportCertificate](#) API do ACM.

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-10-04T16:01:30Z",
  "eventSource": "acm.amazonaws.com",
  "eventName": "ImportCertificate",
  "awsRegion": "ap-southeast-2",
  "sourceIPAddress": "54.240.193.129",
  "userAgent": "Coral/Netty",
  "requestParameters": {
    "privateKey": {
      "hb": [
        "byte",
        "byte",
        "byte",
        "..."
      ],
      "offset": 0,
      "isReadOnly": false,
      "bigEndian": true,
      "nativeByteOrder": false,
      "mark": -1,
      "position": 0,
      "limit": 1674,
      "capacity": 1674,
      "address": 0
    },
    "certificateChain": {
```

```
    "hb":[
      "byte",
      "byte",
      "byte",
      "...",
    ],
    "offset":0,
    "isReadOnly":false,
    "bigEndian":true,
    "nativeByteOrder":false,
    "mark":-1,
    "position":0,
    "limit":2105,
    "capacity":2105,
    "address":0
  },
  "certificate":{
    "hb":[
      "byte",
      "byte",
      "byte",
      "...",
    ],
    "offset":0,
    "isReadOnly":false,
    "bigEndian":true,
    "nativeByteOrder":false,
    "mark":-1,
    "position":0,
    "limit":2503,
    "capacity":2503,
    "address":0
  }
},
"responseElements":{
  "certificateArn":"arn:aws:acm:ap-
southeast-2:111122223333:certificate/01234567-89ab-cdef-0123-456789abcdef"
},
"requestID":"01234567-89ab-cdef-0123-456789abcdef",
"eventID":"01234567-89ab-cdef-0123-456789abcdef",
"eventType":"AwsApiCall",
"recipientAccountId":"111122223333"
}
```

## Lista de certificados ([ListCertificates](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [ListCertificatesAPI](#).

### Note

O CloudTrail registro da `ListCertificates` operação não exibe seus certificados ACM. Você pode visualizar a lista de certificados usando o console AWS Command Line Interface, o ou a [ListCertificatesAPI](#).

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:43Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "ListCertificates",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "maxItems": 1000,
        "certificateStatuses": [
          "ISSUED"
        ]
      },
      "responseElements": null,
      "requestID": "74c99844-ec9c-11e5-ac34-d1e4dfe1a11b",
      "eventID": "cdfef1051-88aa-4aa3-8c33-a325270bff21",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```

```
}
```

## Lista de tags para um certificado ([ListTagsForCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [ListTagsForCertificate](#) API.

### Note

O CloudTrail registro da `ListTagsForCertificate` operação não exibe suas tags. Você pode ver a lista de tags usando o console AWS Command Line Interface, o ou a [ListTagsForCertificate](#) API.

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



```
]
}
```

## Remoção das tags de um certificado ([RemoveTagsFromCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [RemoveTagsFromCertificate](#) API.

```
{
  "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"
  ]
}
```

```
}
```

## Solicitação de um certificado ([RequestCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [RequestCertificate](#) API.

```
{
  "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"
  }
]
}

```

## Reenvio do e-mail de validação ([ResendValidationEmail](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [ResendValidationEmail](#) API.

```

{
  "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"
  }
]
}

```

## Recuperação de um certificado ([GetCertificate](#))

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a [GetCertificate](#) API.

```

{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:41Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "GetCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
      },
      "responseElements": {
        "certificateChain":
          "-----BEGIN CERTIFICATE-----
          Base64-encoded certificate chain
          -----END CERTIFICATE-----",
        "certificate":
          "-----BEGIN CERTIFICATE-----
          Base64-encoded certificate
          -----END CERTIFICATE-----"
      }
    }
  ]
}

```

```
    },
    "requestID": "744dd891-ec9c-11e5-ac34-d1e4dfe1a11b",
    "eventID": "7aa4f909-00dd-478a-9a00-b2709bcad2bb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }
]
}
```

## Registro em log chamadas de API para serviços integrados

Você pode usar CloudTrail para auditar chamadas de API feitas por serviços integrados ao ACM. Para obter mais informações sobre o uso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#). Os exemplos a seguir mostram os tipos de logs que podem ser gerados de acordo com os recursos da AWS em que você provisiona o certificado do ACM.

### Tópicos

- [Criação de um balanceador de carga](#)

## Criação de um balanceador de carga

Você pode usar CloudTrail para auditar chamadas de API feitas por serviços integrados ao ACM. Para obter mais informações sobre o uso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#). Os exemplos a seguir mostram os tipos de registros que podem ser gerados dependendo dos AWS recursos nos quais você provisiona o certificado ACM.

### Tópicos

- [Como criar um balanceador de carga](#)
- [Registrando uma instância do Amazon EC2 com um balanceador de carga](#)
- [Criptografia de uma chave privada](#)
- [Descriptografia de uma chave privada](#)

## Como criar um balanceador de carga

O exemplo a seguir mostra uma chamada para a função `CreateLoadBalancer` por uma usuária do IAM chamada Alice. O nome do balanceador de carga é `TestLinuxDefault`, e o listener é criado usando um certificado do 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"
}
```

## Registrando uma instância do Amazon EC2 com um balanceador de carga

Quando você provisiona o seu site ou aplicativo em uma instância do Amazon Elastic Compute Cloud (Amazon EC2), o balanceador de carga deve ser informado dessa instância. Isso pode ser feito por meio do console do Elastic Load Balancing ou pelo AWS Command Line Interface. O exemplo a seguir mostra uma chamada `RegisterInstancesWithLoadBalancer` para um balanceador de carga chamado `LinuxTest` na AWS conta `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"
}

```

## Criptografia de uma chave privada

O exemplo a seguir mostra uma Encrypt chamada que criptografa a chave privada associada a um certificado do ACM. A criptografia é realizada na 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"
  }
]
}

```

## Descriptografia de uma chave privada

O exemplo a seguir mostra uma chamada Decrypt que descriptografa a chave privada associada a um certificado do ACM. A decodificação é realizada internamente e a AWS chave descriptografada nunca sai. 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"
}

```

## CloudWatch Métricas suportadas

A Amazon CloudWatch é um serviço de monitoramento de AWS recursos. Você pode usar CloudWatch para coletar e monitorar métricas, definir alarmes e reagir automaticamente às mudanças em seus AWS recursos. O ACM publica métricas uma vez por dia para cada certificado em uma conta até a expiração.

O namespace `AWS/CertificateManager` inclui as métricas a seguir.

Métrica	Descrição	Unidade	Dimensões
<code>DaysToExpiry</code>	Número de dias até que a validade de	Inteiro	<code>CertificateArn</code>

Métrica	Descrição	Unidade	Dimensões
	um certificado expire. O ACM interrompe a publicação dessa métrica depois que um certificado expira.		<ul style="list-style-type: none"><li>Valor: ARN do certificado</li></ul>

Para obter mais informações sobre CloudWatch métricas, consulte os tópicos a seguir:

- [Usando o Amazon CloudWatch Metrics](#)
- [Criação de CloudWatch alarmes da Amazon](#)

## Usar a API (exemplos de Java)

Você pode usar a API AWS Certificate Manager para interagir com o serviço de forma programática, enviando solicitações HTTP. Para obter mais informações, consulte a [Referência da API do AWS Certificate Manager](#).

Além da API da Web (ou API HTTP), você pode usar os SDKs AWS e as ferramentas de linha de comando para interagir com o ACM e outros serviços. Para obter mais informações, consulte [Ferramentas para a Amazon Web Services](#).

Os tópicos a seguir mostram como usar um dos SDKs da AWS, o [AWS SDK for Java](#), para executar algumas das operações disponíveis na API do AWS Certificate Manager.

### Tópicos

- [Adição de tags a um certificado](#)
- [Exclusão de um certificado](#)
- [Descrição de um certificado](#)
- [Exportação de um certificado](#)
- [Recuperar um certificado e uma cadeia de certificados](#)
- [Importação um certificado](#)
- [Lista de certificados](#)
- [Renovação de um certificado](#)
- [Lista de tags de certificados](#)
- [Remoção de tags de um certificado](#)
- [Solicitação de um certificado](#)
- [Reenvio de um e-mail de validação](#)

## Adição de tags a um certificado

O exemplo a seguir mostra como usar a função [AddTagsToCertificate](#).

```
package com.amazonaws.samples;

import java.io.IOException;
import java.nio.ByteBuffer;
```

```
import java.nio.charset.StandardCharsets;
import java.nio.file.Files;
import java.nio.file.Paths;

import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 * Certificate Manager
 * service.
 *
 * Input parameters:
 * Accesskey - AWS access key
 * SecretKey - AWS secret key
 * CertificateArn - Use to reimport a certificate (not included in this example).
 * region - AWS region
 * Certificate - PEM file that contains the certificate to import. Ex: /data/certs/
servercert.pem
 * CertificateChain - The certificate chain, not including the end-entity
certificate.
 * PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 * CertificcateArn - The ARN of the imported certificate.
 *
 */
public class AWSCertificateManagerSample {

    public static void main(String[] args) throws IOException {
        String accessKey = "";
        String secretKey = "";
        String certificateArn = null;
        Regions region = Regions.DEFAULT_REGION;
        String serverCertFilePath = "";
        String privateKeyFilePath = "";
        String caCertFilePath = "";

        ImportCertificateRequest req = new ImportCertificateRequest()
            .withCertificate(getCertContent(serverCertFilePath))
    }
```

```
        .withPrivateKey(getCertContent(privateKeyFilePath))

    .withCertificateChain(getCertContent(caCertFilePath)).withCertificateArn(certificateArn);

    AWSCertificateManager client =
    AWSCertificateManagerClientBuilder.standard().withRegion(region)
        .withCredentials(new AWSStaticCredentialsProvider(new
    BasicAWSCredentials(accessKey, secretKey)))
        .build();
    ImportCertificateResult result = client.importCertificate(req);

    System.out.println(result.getCertificateArn());

    List<Tag> expectedTags =
    ImmutableList.of(Tag.builder().withKey("key").withValue("value").build());

    AddTagsToCertificateRequest addTagsToCertificateRequest =
    AddTagsToCertificateRequest.builder()
        .withCertificateArn(result.getCertificateArn())
        .withTags(tags)
        .build();

    client.addTagsToCertificate(addTagsToCertificateRequest);
}

private static ByteBuffer getCertContent(String filePath) throws IOException {
    String fileContent = new String(Files.readAllBytes(Paths.get(filePath)));
    return StandardCharsets.UTF_8.encode(fileContent);
}
}
```

## Exclusão de um certificado

O exemplo a seguir mostra como usar a função [DeleteCertificate](#). Se bem-sucedida, a função retornará um conjunto vazio {}.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.DeleteCertificateRequest;
import com.amazonaws.services.certificatemanager.model.DeleteCertificateResult;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceInUseException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the DeleteCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameter:
 * CertificateArn - The ARN of the certificate to delete.
 */

public class AWSCertificateManagerExample {

    public static void main(String[] args) throws Exception{

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load the credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.US_EAST_1)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Create a request object and specify the ARN of the certificate to delete.
```

```
DeleteCertificateRequest req = new DeleteCertificateRequest();

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

// Delete the specified certificate.
DeleteCertificateResult result = null;
try {
    result = client.deleteCertificate(req);
}
catch (InvalidArnException ex)
{
    throw ex;
}
catch (ResourceInUseException ex)
{
    throw ex;
}
catch (ResourceNotFoundException ex)
{
    throw ex;
}

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

}
}
```

## Descrição de um certificado

O exemplo a seguir mostra como usar a função [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);  
  
}  
}
```

Se bem-sucedido, o exemplo anterior exibirá informações semelhantes a estas.

```
{  
  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: Fri0ct0608: 17: 39PDT2017,  
  }  
}
```

```
Status: ISSUED,  
NotBefore: ThuOct0510: 14: 32PDT2017,  
NotAfter: SunOct0310: 14: 32PDT2027,  
KeyAlgorithm: RSA-2048,  
SignatureAlgorithm: SHA256WITHRSA,  
InUseBy: [],  
Type: IMPORTED,  
  }  
}
```

## Exportação de um certificado

O exemplo a seguir mostra como usar a função [ExportCertificate](#). Essa função exporta um certificado privado emitido por uma autoridade de certificação (CA) privada no formato PKCS #8. (Não é possível exportar certificados públicos independentemente de serem emitidos pelo ACM ou importados.) Ela também exporta a cadeia de certificados e a chave privada. No exemplo, a frase secreta da chave é armazenada em um arquivo local.

```
package com.amazonaws.samples;  
  
import com.amazonaws.AmazonClientException;  
  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.auth.AWSStaticCredentialsProvider;  
import com.amazonaws.auth.AWSCredentials;  
import com.amazonaws.regions.Regions;  
  
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;  
import com.amazonaws.services.certificatemanager.AWSCertificateManager;  
  
import com.amazonaws.services.certificatemanager.model.ExportCertificateRequest;  
import com.amazonaws.services.certificatemanager.model.ExportCertificateResult;  
  
import com.amazonaws.services.certificatemanager.model.InvalidArnException;  
import com.amazonaws.services.certificatemanager.model.InvalidTagException;  
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;  
  
import java.io.FileNotFoundException;  
import java.io.IOException;  
import java.io.RandomAccessFile;  
import java.nio.ByteBuffer;
```

```
import java.nio.channels.FileChannel;

public class ExportCertificate {

    public static void main(String[] args) throws Exception {

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.your_region)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Initialize a file descriptor for the passphrase file.
        RandomAccessFile file_passphrase = null;

        // Initialize a buffer for the passphrase.
        ByteBuffer buf_passphrase = null;

        // Create a file stream for reading the private key passphrase.
        try {
            file_passphrase = new RandomAccessFile("C:\\Temp\\password.txt", "r");
        }
        catch (IllegalArgumentException ex) {
            throw ex;
        }
        catch (SecurityException ex) {
            throw ex;
        }
        catch (FileNotFoundException ex) {
            throw ex;
        }
    }
}
```

```
// Create a channel to map the file.
FileChannel channel_passphrase = file_passphrase.getChannel();

// Map the file to the buffer.
try {
    buf_passphrase = channel_passphrase.map(FileChannel.MapMode.READ_ONLY, 0,
channel_passphrase.size());

    // Clean up after the file is mapped.
    channel_passphrase.close();
    file_passphrase.close();
}
catch (IOException ex)
{
    throw ex;
}

// Create a request object.
ExportCertificateRequest req = new ExportCertificateRequest();

// Set the certificate ARN.
req.withCertificateArn("arn:aws:acm:region:account:"
    +"certificate/M12345678-1234-1234-1234-123456789012");

// Set the passphrase.
req.withPassphrase(buf_passphrase);

// Export the certificate.
ExportCertificateResult result = null;

try {
    result = client.exportCertificate(req);
}
catch(InvalidArnException ex)
{
    throw ex;
}
catch (InvalidTagException ex)
{
    throw ex;
}
catch (ResourceNotFoundException ex)
{
    throw ex;
}
```

```
    }

    // Clear the buffer.
    buf_passphrase.clear();

    // Display the certificate and certificate chain.
    String certificate = result.getCertificate();
    System.out.println(certificate);

    String certificate_chain = result.getCertificateChain();
    System.out.println(certificate_chain);

    // This example retrieves but does not display the private key.
    String private_key = result.getPrivateKey();
}
}
```

## Recuperar um certificado e uma cadeia de certificados

O exemplo a seguir mostra como usar a função [GetCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.GetCertificateRequest;
import com.amazonaws.services.certificatemanager.model.GetCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.RequestInProgressException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the GetCertificate function in the AWS
 * Certificate
 * Manager service.
 */
```

```
* Input parameter:  
*   CertificateArn - The ARN of the certificate to retrieve.  
*  
* Output parameters:  
*   Certificate - A base64-encoded certificate in PEM format.  
*   CertificateChain - The base64-encoded certificate chain in PEM format.  
*  
*/
```

```
public class AWSCertificateManagerExample {  
  
    public static void main(String[] args) throws Exception{  
  
        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in  
Windows  
        // or the ~/.aws/credentials file in Linux.  
        AWSCredentials credentials = null;  
        try {  
            credentials = new ProfileCredentialsProvider().getCredentials();  
        }  
        catch (Exception ex) {  
            throw new AmazonClientException("Cannot load the credentials from the  
credential profiles file.", ex);  
        }  
  
        // Create a client.  
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()  
            .withRegion(Regions.US_EAST_1)  
            .withCredentials(new AWSStaticCredentialsProvider(credentials))  
            .build();  
  
        // Create a request object and set the ARN of the certificate to be described.  
        GetCertificateRequest req = new GetCertificateRequest();  
  
        req.setCertificateArn("arn:aws:acm:region:account:certificate/  
12345678-1234-1234-1234-123456789012");  
  
        // Retrieve the certificate and certificate chain.  
        // If you recently requested the certificate, loop until it has been created.  
        GetCertificateResult result = null;  
        long totalTimeout = 1200001;  
        long timeSlept = 01;  
        long sleepInterval = 100001;  
        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);
}
}
```

O exemplo anterior cria um resultado semelhante ao seguinte:

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

## Importação um certificado

O exemplo a seguir mostra como usar a função [ImportCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```



```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 * Certificate Manager
 * service.
 *
 * Input parameters:
 * Certificate - PEM file that contains the certificate to import.
 * CertificateArn - Use to reimport a certificate (not included in this example).
 * CertificateChain - The certificate chain, not including the end-entity
 * certificate.
 * PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 * 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 AWSStaticCredentialsProvider(credentials))
    .build();

// Initialize the file descriptors.
RandomAccessFile file_certificate = null;
RandomAccessFile file_chain = null;
RandomAccessFile file_key = null;

// Initialize the buffers.
ByteBuffer buf_certificate = null;
ByteBuffer buf_chain = null;
ByteBuffer buf_key = null;

// Create the file streams for reading.
try {
    file_certificate = new RandomAccessFile("C:\\Temp\\certificate.pem", "r");
    file_chain = new RandomAccessFile("C:\\Temp\\chain.pem", "r");
    file_key = new RandomAccessFile("C:\\Temp\\private_key.pem", "r");
}
catch (IllegalArgumentException ex) {
    throw ex;
}
catch (SecurityException ex) {
    throw ex;
}
catch (FileNotFoundException ex) {
    throw ex;
}

// Create channels for mapping the files.
FileChannel channel_certificate = file_certificate.getChannel();
FileChannel channel_chain = file_chain.getChannel();
FileChannel channel_key = file_key.getChannel();

// Map the files to buffers.
try {
```

```
        buf_certificate = channel_certificate.map(FileChannel.MapMode.READ_ONLY, 0,
channel_certificate.size());
        buf_chain = channel_chain.map(FileChannel.MapMode.READ_ONLY, 0,
channel_chain.size());
        buf_key = channel_key.map(FileChannel.MapMode.READ_ONLY, 0,
channel_key.size());

        // The files have been mapped, so clean up.
        channel_certificate.close();
        channel_chain.close();
        channel_key.close();
        file_certificate.close();
        file_chain.close();
        file_key.close();
    }
    catch (IOException ex)
    {
        throw ex;
    }

    // Create a request object and set the parameters.
    ImportCertificateRequest req = new ImportCertificateRequest();
    req.setCertificate(buf_certificate);
    req.setCertificateChain(buf_chain);
    req.setPrivateKey(buf_key);

    // Import the certificate.
    ImportCertificateResult result = null;
    try {
        result = client.importCertificate(req);
    }
    catch(LimitExceededException ex)
    {
        throw ex;
    }
    catch (ResourceNotFoundException ex)
    {
        throw ex;
    }

    // Clear the buffers.
    buf_certificate.clear();
    buf_chain.clear();
    buf_key.clear();
```

```
    // Retrieve and display the certificate ARN.
    String arn = result.getCertificateArn();
    System.out.println(arn);
}
}
```

## Lista de certificados

O exemplo a seguir mostra como usar a função [ListCertificates](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListCertificatesRequest;
import com.amazonaws.services.certificatemanager.model.ListCertificatesResult;

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

import com.amazonaws.AmazonClientException;

import java.util.Arrays;
import java.util.List;

/**
 * This sample demonstrates how to use the ListCertificates function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameters:
 * CertificateStatuses - An array of strings that contains the statuses to use for
 * filtering.
 * MaxItems - The maximum number of certificates to return in the response.
 * NextToken - Use when paginating results.
 *
 * Output parameters:
 * CertificateSummaryList - A list of certificates.
 * NextToken - Use to show additional results when paginating a truncated list.
 *
 */
```

```
*/

public class AWSCertificateManagerExample {

    public static void main(String[] args) throws Exception{

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load the credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.US_EAST_1)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Create a request object and set the parameters.
        ListCertificatesRequest req = new ListCertificatesRequest();
        List<String> Statuses = Arrays.asList("ISSUED", "EXPIRED", "PENDING_VALIDATION",
"FAILED");
        req.setCertificateStatuses(Statuses);
        req.setMaxItems(10);

        // Retrieve the list of certificates.
        ListCertificatesResult result = null;
        try {
            result = client.listCertificates(req);
        }
        catch (Exception ex)
        {
            throw ex;
        }

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

```
}
```

O exemplo anterior cria um resultado semelhante ao seguinte:

```
{
  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
  }]
}
```

## Renovação de um certificado

O exemplo a seguir mostra como usar a função [RenewCertificate](#). A função renova um certificado privado emitido por uma autoridade de certificação (CA) privada e exportado com a função [ExportCertificate](#). No momento, somente certificados privados exportados podem ser renovados com essa função. Para renovar os certificados da CA privada da AWS com o ACM, você deve primeiro conceder as permissões de entidade principal do serviço do ACM para fazer isso. Para obter mais informações, consulte [Atribuição de permissões de renovação de certificado ao ACM](#).

```
package com.amazonaws.samples;

import com.amazonaws.AmazonClientException;

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

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
```

```
import com.amazonaws.services.certificatemanager.AWSCertificateManager;

import com.amazonaws.services.certificatemanager.model.RenewCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RenewCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.ValidationException;

import java.io.FileNotFoundException;
import java.io.IOException;
import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

public class RenewCertificate {

    public static void main(String[] args) throws Exception {

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.your_region)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Create a request object and specify the ARN of the certificate to renew.
        RenewCertificateRequest req = new RenewCertificateRequest();
        req.withCertificateArn("arn:aws:acm:region:account:"
            +"certificate/M12345678-1234-1234-1234-123456789012");
    }
}
```

```
// Renew the certificate.
RenewCertificateResult result = null;
try {
    result = client.renewCertificate(req);
}
catch(InvalidArnException ex)
{
    throw ex;
}
catch (ResourceNotFoundException ex)
{
    throw ex;
}
catch (ValidationException ex)
{
    throw ex;
}

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

## Lista de tags de certificados

O exemplo a seguir mostra como usar a função [ListTagsForCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.regions.Regions;
```



```
/**
 * This sample demonstrates how to use the ListTagsForCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameter:
 * CertificateArn - The ARN of the certificate whose tags you want to list.
 */

public class AWSCertificateManagerExample {

    public static void main(String[] args) throws Exception{

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.US_EAST_1)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Create a request object and specify the ARN of the certificate.
        ListTagsForCertificateRequest req = new ListTagsForCertificateRequest();

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

        // Create a result object.
        ListTagsForCertificateResult result = null;
        try {
            result = client.listTagsForCertificate(req);
        }
    }
}
```

```
    }
    catch(InvalidArnException ex) {
        throw ex;
    }
    catch(ResourceNotFoundException ex) {
        throw ex;
    }

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

}
}
```

O exemplo anterior cria um resultado semelhante ao seguinte:

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

## Remoção de tags de um certificado

O exemplo a seguir mostra como usar a função [RemoveTagsFromCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import
    com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateResult;
import com.amazonaws.services.certificatemanager.model.Tag;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.InvalidTagException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

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

import java.util.ArrayList;
```

```
/**
 * This sample demonstrates how to use the RemoveTagsFromCertificate function in the
 * AWS Certificate
 * Manager service.
 *
 * Input parameters:
 * CertificateArn - The ARN of the certificate from which you want to remove one or
 * more tags.
 * Tags - A collection of key-value pairs that specify which tags to remove.
 */

public class AWSCertificateManagerExample {

    public static void main(String[] args) throws Exception {

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
            .withRegion(Regions.US_EAST_1)
            .withCredentials(new AWSStaticCredentialsProvider(credentials))
            .build();

        // Specify the tags to remove.
        Tag tag1 = new Tag();
        tag1.setKey("Short_Name");
        tag1.setValue("My_Cert");

        Tag tag2 = new Tag()
            .withKey("Purpose")
            .withValue("Test");
    }
}
```

```
// Add the tags to a collection.
ArrayList<Tag> tags = new ArrayList<Tag>();
tags.add(tag1);
tags.add(tag2);

// Create a request object.
RemoveTagsFromCertificateRequest req = new RemoveTagsFromCertificateRequest();

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

// Create a result object.
RemoveTagsFromCertificateResult result = null;
try {
    result = client.removeTagsFromCertificate(req);
}
catch(InvalidArnException ex)
{
    throw ex;
}
catch(InvalidTagException ex)
{
    throw ex;
}
catch(ResourceNotFoundException ex)
{
    throw ex;
}

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

## Solicitação de um certificado

O exemplo a seguir mostra como usar a função [RequestCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.services.certificatemanager.model.RequestCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RequestCertificateResult;

import
    com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.AmazonClientException;

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

import java.util.ArrayList;

/**
 * This sample demonstrates how to use the RequestCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameters:
 *  DomainName - FQDN of your site.
 *  DomainValidationOptions - Domain name for email validation.
 *  IdempotencyToken - Distinguishes between calls to RequestCertificate.
 *  SubjectAlternativeNames - Additional FQDNs for the subject alternative names
 * extension.
 *
 * Output parameter:
 *  Certificate ARN - The Amazon Resource Name (ARN) of the certificate you requested.
 */

public class AWSCertificateManagerExample {

    public static void main(String[] args) {

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
```

```
        throw new AmazonClientException("Cannot load your credentials from file.",
ex);
    }

    // Create a client.
    AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
        .withRegion(Regions.US_EAST_1)
        .withCredentials(new AWSStaticCredentialsProvider(credentials))
        .build();

    // Specify a SAN.
    ArrayList<String> san = new ArrayList<String>();
    san.add("www.example.com");

    // Create a request object and set the input parameters.
    RequestCertificateRequest req = new RequestCertificateRequest();
    req.setDomainName("example.com");
    req.setIdempotencyToken("1Aq25pTy");
    req.setSubjectAlternativeNames(san);

    // Create a result object and display the certificate ARN.
    RequestCertificateResult result = null;
    try {
        result = client.requestCertificate(req);
    }
    catch(InvalidDomainValidationOptionsException ex)
    {
        throw ex;
    }
    catch(LimitExceededException ex)
    {
        throw ex;
    }

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

}

}
```

O exemplo anterior cria um resultado semelhante ao seguinte:

```
{CertificateArn:  
  arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

## Reenvio de um e-mail de validação

O exemplo a seguir mostra como usar a função [ResendValidationEmail](#).

```
package com.amazonaws.samples;  
  
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;  
import com.amazonaws.services.certificatemanager.AWSCertificateManager;  
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailRequest;  
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailResult;  
  
import  
  com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;  
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;  
import com.amazonaws.services.certificatemanager.model.InvalidStateException;  
import com.amazonaws.services.certificatemanager.model.InvalidArnException;  
import com.amazonaws.AmazonClientException;  
  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.auth.AWSStaticCredentialsProvider;  
import com.amazonaws.auth.AWSCredentials;  
import com.amazonaws.regions.Regions;  
  
/**  
 * This sample demonstrates how to use the ResendValidationEmail function in the AWS  
 Certificate  
 Manager service.  
 *  
 * Input parameters:  
 * CertificateArn - Amazon Resource Name (ARN) of the certificate request.  
 * Domain - FQDN in the certificate request.  
 * ValidationDomain - The base validation domain that is used to send email.  
 *  
 */  
  
public class AWSCertificateManagerExample {  
  
    public static void main(String[] args) {
```

```
// Retrieve your credentials from the C:\Users\name\.aws\credentials file in
Windows
// or the ~/.aws/credentials file in Linux.
AWSCredentials credentials = null;
try {
    credentials = new ProfileCredentialsProvider().getCredentials();
}
catch (Exception ex) {
    throw new AmazonClientException("Cannot load your credentials from file.",
ex);
}

// Create a client.
AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
    .withRegion(Regions.US_EAST_1)
    .withCredentials(new AWSStaticCredentialsProvider(credentials))
    .build();

// Create a request object and set the input parameters.
ResendValidationEmailRequest req = new ResendValidationEmailRequest();

req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");
req.setDomain("gregpe.io");
req.setValidationDomain("gregpe.io");

// Create a result object.
ResendValidationEmailResult result = null;
try {
    result = client.resendValidationEmail(req);
}
catch(ResourceNotFoundException ex)
{
    throw ex;
}
catch (InvalidStateException ex)
{
    throw ex;
}
catch (InvalidArnException ex)
{
    throw ex;
}
catch (InvalidDomainValidationOptionsException ex)
```



```
    {  
        throw ex;  
    }  
  
    // Display the result.  
    System.out.println(result.toString());  
  
    }  
}
```

O exemplo anterior reenvia o e-mail de validação e exibe um conjunto vazio.

# Solução de problemas

Consulte os tópicos a seguir se você encontrar problemas para usar o AWS Certificate Manager.

## Note

Se você não encontrar seu problema abordado nesta seção, recomendamos acessar o [Central de conhecimento da AWS](#).

## Tópicos

- [Solução de problemas de solicitações de certificado](#)
- [Solução de problemas de validação de certificado](#)
- [Solução de problemas de renovação de certificado gerenciado](#)
- [Solução de outros problemas](#)
- [Tratamento de exceções](#)

## Solução de problemas de solicitações de certificado

Consulte os tópicos a seguir se encontrar problemas ao solicitar um certificado do ACM.

## Tópicos

- [Prazo de solicitação de certificado encerrado](#)
- [Falha na solicitação de certificado](#)

## Prazo de solicitação de certificado encerrado

O prazo para as solicitações de certificados do ACM expira se não forem validadas em 72 horas. Para corrigir essa condição, abra o console, localize o registro do certificado, clique na caixa de seleção correspondente, escolha Actions (Ações) e escolha Delete (Excluir). Em seguida, escolha Actions (Ações) e Request a certificate (Solicitar um certificado) para recomeçar. Para obter mais informações, consulte [Validação por DNS](#) ou [Validação de e-mail](#). Se possível, recomendamos usar a validação de DNS.

## Falha na solicitação de certificado

Se a solicitação causar falha do ACM e você receber uma das mensagens de erro a seguir, execute as etapas sugeridas para corrigir o problema. Não é possível reenviar uma solicitação de certificado com falha; depois de resolver o problema, envie uma nova solicitação.

### Tópicos

- [Mensagem de erro: No Available Contacts \(Não há contatos disponíveis\)](#)
- [Mensagem de erro: Additional Verification Required \(Verificação adicional obrigatória\)](#)
- [Mensagem de erro: Invalid Public Domain \(Domínio público inválido\)](#)
- [Mensagem de erro: outra](#)

### Mensagem de erro: No Available Contacts (Não há contatos disponíveis)

Você escolheu a validação por e-mail ao solicitar um certificado, mas o ACM não pôde encontrar um endereço de e-mail para validar um ou mais nomes de domínio na solicitação. Para corrigir este problema, você pode executar uma das seguintes ações:

- Verifique se você tem um endereço de e-mail registrado no WHOIS e se o endereço está visível ao executar uma pesquisa WHOIS padrão para os nomes de domínio na solicitação de certificado. Normalmente, isso é feito por meio do registrador do domínio.
- Verifique se o domínio está configurado para receber e-mail. O servidor de nomes de domínio deve ter um registro de troca de e-mail (registro MX) para que os servidores de e-mail do ACM saibam para onde enviar o [e-mail de validação de domínio](#).

Executar apenas uma das tarefas anteriores é suficiente para corrigir esse problema; você não precisa fazer ambas. Depois de corrigir o problema, solicite um novo certificado.

Para obter mais informações sobre como garantir que você receba os e-mails de validação de domínio do ACM, consulte [\(Opcional\) Configurar e-mail para seu domínio](#) ou [E-mail de validação não recebido](#). Se você seguir estas etapas e continuar a ver a mensagem Contatos não disponíveis, [relate isso para a AWS](#) para que possamos investigar.

### Mensagem de erro: Additional Verification Required (Verificação adicional obrigatória)

O ACM requer informações adicionais para processar essa solicitação de certificado. Isso acontece como uma medida de proteção contra fraudes se seu domínio se classificar nos [1000 principais](#)

[sites da Alexa](#). Para fornecer as informações necessárias, use a [Central de suporte](#) para entrar em contato com o AWS Support. Se você não tem um plano de suporte, publique um novo thread no [Fórum de discussão do ACM](#).

#### Note

Você não pode solicitar um certificado para nomes de domínio pertencentes à Amazon, como aqueles que terminam em `amazonaws.com`, `cloudfront.net` ou `elasticbeanstalk.com`.

## Mensagem de erro: Invalid Public Domain (Domínio público inválido)

Um ou mais nomes de domínio na solicitação de certificado não são válidos. Normalmente, isso ocorre porque um nome de domínio na solicitação não é um domínio de nível superior válido. Tente solicitar um certificado novamente, corrigindo os erros de ortografia ou digitação que havia na solicitação com falha e garantindo que todos os nomes de domínio na solicitação sejam de domínios de nível superior válidos. Por exemplo, você não pode solicitar um certificado do ACM para `example.invalidpublicdomain` porque "invalidpublicdomain" não é um domínio de nível superior válido. Se continuar a receber esse motivo de falha, entre em contato com a [Central de suporte](#). Se você não tem um plano de suporte, publique um novo thread no [Fórum de discussão do ACM](#).

## Mensagem de erro: outra

Normalmente, essa falha ocorre quando há um erro ortográfico em um ou mais dos nomes de domínio na solicitação de certificado. Tente solicitar um certificado novamente, corrigindo os erros de ortografia ou digitação que havia na solicitação com falha. Se continuar a receber essa mensagem de falha, use a [Central de suporte](#) para entrar em contato com o AWS Support. Se você não tem um plano de suporte, publique um novo thread no [Fórum de discussão do ACM](#).

## Solução de problemas de validação de certificado

Se o status da solicitação de certificado do ACM for Pending validation (Validação pendente), a solicitação estará aguardando por uma ação sua. Se você escolheu a validação de e-mail quando fez a solicitação, você ou um representante autorizado deverá responder às mensagens de e-mail sobre a validação. Essas mensagens foram enviadas aos endereços de contato WHOIS registrados e a outros endereços de e-mail comuns para o domínio solicitado. Para ter mais informações, consulte [Validação de e-mail](#). Se você escolheu a validação por DNS, deve gravar o registro CNAME

criado pelo ACM para você em seu banco de dados do DNS. Para ter mais informações, consulte [Validação por DNS](#).

#### Important

Você deve validar que possui ou controla cada nome de domínio incluído na solicitação de certificado. Se você escolheu a validação de e-mail, receberá mensagens de e-mail sobre a validação para cada domínio. Se você não as receber, consulte [E-mail de validação não recebido](#). Se você escolheu a validação de DNS, deverá criar um registro CNAME para cada domínio.

#### Note

Certificados públicos do ACM podem ser instalados em instâncias do Amazon EC2 conectadas a um [Nitro Enclave](#), mas não a outras instâncias do Amazon EC2. Para obter informações sobre como configurar um servidor Web independente em uma instância do Amazon EC2 não conectada a um Nitro Enclave, consulte [Tutorial: Instalar um servidor Web LAMP no Amazon Linux 2](#) ou [Tutorial: Instalar um servidor Web LAMP com o Amazon Linux AMI](#).

Recomendamos que você use a validação de DNS em vez da validação de e-mail.

Consulte os tópicos a seguir se tiver problemas de validação.

#### Tópicos

- [Solucionar os problemas de validação por DNS](#)
- [Solução de problemas de validação de e-mail](#)

## Solucionar os problemas de validação por DNS

Consulte as orientações a seguir se tiver problemas ao validar um certificado com o DNS.

A primeira etapa na solução de problemas de DNS é verificar o status atual do seu domínio com ferramentas como as seguintes:

- dig – [Linux](#), [Windows](#)

- nslookup – [Linux](#), [Windows](#)
- whois – [Linux](#), [Windows](#)

## Tópicos

- [Sublinhas proibidos pelo provedor de DNS](#)
- [Ponto final padrão adicionado pelo provedor DNS](#)
- [Validação de DNS em caso de falha GoDaddy](#)
- [Console do ACM não exibe o botão “Criar registros no Route 53”](#)
- [Falha de validação do Route 53 em domínios privados \(não confiáveis\)](#)
- [A validação foi bem-sucedida, mas a emissão ou renovação falhou](#)
- [Falha de validação para o servidor de DNS em uma VPN](#)

## Sublinhas proibidos pelo provedor de DNS

Se o seu provedor de DNS não permite sublinhas iniciais em valores de CNAME, você pode remover a sublinha do valor fornecido pelo ACM e validar seu domínio sem ela. Por exemplo, o valor de `_x2.acm-validations.aws` pode ser alterado para CNAME `x2.acm-validations.aws` para fins de validação. No entanto, o nome do parâmetro CNAME sempre deve começar com um sublinhado.

Você pode usar qualquer um dos valores no lado direito da tabela abaixo para validar um domínio.

Nome	Tipo	Valor
<code>_&lt;random value&gt;.example.com.</code>	CNAME	<code>_&lt;random value&gt;.acm-validations.aws.</code>
<code>&lt;random value&gt;.example.com.</code>	CNAME	<code>&lt;random value&gt;.acm-validations.aws.</code>

## Ponto final padrão adicionado pelo provedor DNS

Alguns provedores de DNS adicionam por padrão um ponto final ao valor CNAME fornecido. Como resultado, adicionar o ponto você mesmo causa um erro. Por exemplo, "`<random_value>.acm-validations.aws.`" é rejeitado enquanto "`<random_value>.acm-validations.aws`" é aceito.

## Validação de DNS em caso de falha GoDaddy

Pode ocorrer uma falha na validação por DNS para domínios registrados no GoDaddy e outros registros, a menos que você modifique os valores CNAME fornecidos pelo ACM. Considerando-se `example.com` como o nome de domínio, o registro CNAME emitido tem a seguinte forma:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:  
_cjhvou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

Você pode criar um registro CNAME compatível com GoDaddy truncando o domínio apex (incluindo o ponto) no final do campo NAME, da seguinte forma:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:  
_cjhvou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

## Console do ACM não exibe o botão “Criar registros no Route 53”

Se você selecionar o Amazon Route 53 como seu provedor de DNS, AWS Certificate Manager poderá interagir diretamente com ele para validar a propriedade do seu domínio. Em algumas circunstâncias, o botão Criar registros no Route 53 pode não estar disponível quando você espera. Se isso acontecer, verifique as seguintes causas possíveis.

- Você não está usando o Route 53 como provedor de DNS.
- Você está conectado ao ACM e ao Route 53 por contas diferentes.
- Você não tem permissões do IAM para criar registros em uma zona hospedada pelo Route 53.
- Você ou outra pessoa já validou o domínio.
- O domínio não é endereçável publicamente.

## Falha de validação do Route 53 em domínios privados (não confiáveis)

Durante a validação de DNS, o ACM procura um CNAME em uma zona hospedada publicamente. Quando não encontra, ele expira após 72 horas com o status Validation timed out (Validação atingiu o tempo limite). Você não pode usá-lo para hospedar registros de DNS para domínios privados, incluindo recursos em uma [zona hospedada privada](#) do Amazon VPC, domínios não confiáveis em sua PKI privada e certificados autoassinados.

AWS fornece suporte para domínios publicamente não confiáveis por meio do [CA privada da AWS](#) serviço.

## A validação foi bem-sucedida, mas a emissão ou renovação falhou

Se a emissão do certificado falhar com “Validação pendente”, mesmo que o DNS esteja correto, verifique se a emissão não está sendo bloqueada por um registro de Autorização da autoridade de certificação (CAA). Para ter mais informações, consulte [\(Opcional\) Configurar um registro de CAA](#).

## Falha de validação para o servidor de DNS em uma VPN

Se você localizar um servidor de DNS em uma VPN e o ACM não validar um certificado verificado nesse servidor, verifique se o servidor está acessível publicamente. A emissão de certificados públicos usando a validação por DNS do ACM requer que os registros de domínio sejam resolvidos pela Internet pública.

## Solução de problemas de validação de e-mail

Consulte as orientações a seguir se tiver problemas ao validar um certificado por e-mail.

### Tópicos

- [E-mail de validação não recebido](#)
- [E-mail enviado para subdomínio](#)
- [Informações de contato ocultas](#)
- [Renovações de certificado](#)
- [Restrição do WHOIS](#)
- [Carimbo de data/hora inicial persistente para validação de e-mail](#)
- [Solução de problemas com o domínio de nível superior .IO](#)
- [Não consigo mudar para a validação de DNS](#)

## E-mail de validação não recebido

Quando você solicita um certificado do ACM, e escolhe validação por e-mail, o e-mail de validação do domínio é enviado a três endereços de contato especificados no WHOIS e a cinco endereços administrativos comuns. Para ter mais informações, consulte [Validação de e-mail](#). Se você está com problemas de recebimento do e-mail de validação, revise as sugestões a seguir.

### Onde procurar o e-mail

O e-mail de validação é enviado aos endereços de contato relacionados no WHOIS e a endereços administrativos comuns para o domínio. O e-mail não é enviado ao proprietário da



AWS conta, a menos que o proprietário também esteja listado como um contato de domínio no WHOIS. Revise a lista de endereços de e-mail que são exibidos no console do ACM (ou retornados da CLI ou API) para determinar onde você deve procurar o e-mail de validação. Para ver a lista, clique no ícone ao lado do nome de domínio na caixa Validação não concluída.

O e-mail é marcado como spam

Verifique se o e-mail de validação está na pasta de spam.


O Gmail classifica automaticamente seu e-mail

Se você estiver usando o Gmail, o e-mail de validação pode ter sido classificado automaticamente nas guias Atualizações ou Promoções.

O registrador do domínio não exibe informações de contato nem se a proteção de privacidade está ativada

Em alguns casos, os contatos técnicos e administrativos do registrante do domínio no WHOIS podem não estar disponíveis publicamente e, AWS portanto, não podem entrar em contato com esses contatos. A seu critério, você pode optar por configurar seu registrador para relacionar seu endereço de e-mail no WHOIS, embora nem todos os registradores ofereçam suporte a essa opção. Você pode precisar fazer uma alteração diretamente no registro do seu domínio. Em outros casos, as informações de contato do domínio podem estar usando um endereço de privacidade, como aqueles fornecidos por WhoisGuard ou PrivacyGuard.

Para domínios comprados do Route 53, a proteção de privacidade está habilitada por padrão e seu endereço de e-mail é mapeado para um endereço de e-mail `whoisprivacyservice.org`, `contact.gandi.net` ou `identity-protect.org`. Certifique-se de que o endereço de e-mail do registrador cadastrado com o seu registrador do domínio esteja atualizado para que os e-mails enviados para esses endereços de e-mail obscuros possam ser encaminhados para um endereço de e-mail que você controle.

 Note

A proteção de privacidade para alguns domínios que você compra com o Route 53 será habilitada, mesmo se você optar por tornar suas informações de contato públicas. Por exemplo, a proteção de privacidade para o domínio de nível superior `.ca` não pode ser programaticamente desativada pelo Route 53. Você deve entrar em contato com o [AWS Support Center](#) e solicitar que a proteção de privacidade seja desativada.

Se as informações de contato de e-mail para seu domínio não estiverem disponíveis por meio de WHOIS, ou se um e-mail enviado para as informações de contato não chegar ao proprietário do domínio ou a um representante autorizado, recomendamos que você configure seu domínio ou subdomínio para receber e-mails enviados para um ou mais endereços administrativos comuns formados antepondo-se `admin@`, `administrador@`, `hostmaster@`, `webmaster@` e `postmaster@` ao nome de domínio solicitado. Para obter mais informações sobre a configuração de e-mail para seu domínio, consulte a documentação do seu provedor de serviço de e-mail e siga as instruções em [\(Opcional\) Configurar e-mail para seu domínio](#). Se você estiver usando a Amazon WorkMail, consulte [Trabalhando com usuários](#) no Guia do WorkMail administrador da Amazon.

Após tornar disponível pelo menos um dos oito endereços de e-mail para os quais a AWS envia o e-mail de validação e confirmar que você recebe um e-mail para esse endereço, você estará pronto para solicitar um certificado por meio do ACM. Depois de fazer uma solicitação de certificado, certifique-se de que o endereço de e-mail pretendido aparece na lista de endereços de e-mail no AWS Management Console. Embora o certificado esteja no estado de Validação pendente, você pode expandir a lista para visualizá-lo clicando no ícone ao lado do nome de domínio na caixa Validação não concluída. Você também pode visualizar a lista na Step 3: Validate (Etapa 3: Validar) do assistente Request a Certificate (Solicitar um certificado) do ACM. Os endereços de e-mail relacionados são aqueles para os quais o e-mail foi enviado.

### Registros MX ausentes ou configurados incorretamente

Um registro MX é um registro de recurso no banco de dados Domain Name System (DNS) que especifica um ou mais servidores de e-mail para aceitar mensagens de e-mail para o seu domínio. Se o registro MX está ausente ou configurado incorretamente, o e-mail não pode ser enviado para nenhum dos cinco endereços comuns de administração do sistema especificados em [Validação de e-mail](#). Corrija o problema de registro MX ausente ou configurado incorretamente e tente reenviar o e-mail ou solicitar seu certificado novamente.

#### Note

Atualmente, recomendamos que você aguarde pelo menos uma hora antes de tentar reenviar o e-mail ou solicitar seu certificado.

#### Note

Para ignorar a exigência de um registro MX, você pode usar a `ValidationDomain` opção na [RequestCertificate](#) API ou o AWS CLI comando [request-certificate](#) para

especificar o nome de domínio para o qual o ACM envia e-mails de validação. Se você usa a API ou a AWS CLI, AWS não executa uma pesquisa MX.

Entre em contato com a Central de suporte

Se, depois de analisar a orientação anterior, você ainda não recebeu o e-mail de validação de domínio, visite a [Central de AWS Support](#) e abra um caso. Se você não tiver um contrato de suporte, publique uma mensagem no [Fórum de discussão do ACM](#).

## E-mail enviado para subdomínio

Se você estiver usando o console para solicitar um certificado para um nome de subdomínio, como `sub.test.example.com`, o ACM verificará se há um registro MX para `sub.test.example.com`. Se não, o domínio pai `test.example.com` é marcado, e assim por diante, até o domínio de base `example.com`. Se um registro MX for encontrado, a pesquisa é interrompida e um e-mail de validação é enviado para os endereços de administração comuns para o subdomínio. Então, por exemplo, se um registro MX é encontrado para `test.example.com`, um e-mail é enviado para `admin@teste.exemplo.com`, `administrador@teste.exemplo.com` e outros endereços administrativos especificados no [Validação de e-mail](#). Se um registro MX não é encontrado em nenhum dos subdomínios, um e-mail é enviado para o subdomínio para o qual você solicitou originalmente o certificado. Para ver uma discussão detalhada sobre como configurar seu e-mail e como o ACM funciona com o DNS e o banco de dados WHOIS, consulte [\(Opcional\) Configurar e-mail para seu domínio](#).

Em vez de usar o console, você pode usar a `ValidationDomain` opção na [RequestCertificateAPI](#) ou o AWS CLI comando [request-certificate](#) para especificar o nome de domínio para o qual o ACM envia e-mails de validação. Se você usa a API ou a AWS CLI, AWS não executa uma pesquisa MX.

## Informações de contato ocultas

Um problema comum ocorre quando você tenta criar um novo certificado. Alguns registradores permitem que você oculte suas informações de contato na listagem WHOIS. Outros permitem que você substitua o seu endereço de e-mail verdadeiro por um endereço de privacidade (ou proxy). Isso impede que você receba o e-mail de validação nos endereços de contato registrados.

Para receber e-mail, assegure-se de que suas informações de contato sejam públicas no WHOIS, ou se a listagem WHOIS exibir um endereço de e-mail de privacidade, verifique se o endereço de e-mail

enviado para o endereço de e-mail de privacidade é encaminhado para o seu endereço de e-mail real. Após a conclusão da configuração do WHOIS e, desde que o prazo da solicitação de certificado não tenha expirado, você pode optar por reenviar o e-mail de validação. O ACM executa uma nova consulta do WHOIS/MX e envia o e-mail de validação para o seu endereço de contato agora público.

## Renovações de certificado

Se você tornou públicas suas informações do WHOIS quando solicitou um novo certificado e, depois, ocultou suas informações, o ACM não poderá recuperar seus endereços de contato registrados quando você tentar renovar seu certificado. O ACM envia o e-mail de validação para esses endereços de contato e para cinco endereços administrativos comuns formados usando seu registro MX. Para resolver esse problema, torne suas informações WHOIS públicas novamente e reenvie os e-mails de validação. O ACM executa uma nova consulta ao WHOIS/MX e envia o e-mail de validação para seus endereços de contato agora públicos.

## Restrição do WHOIS

Às vezes, o ACM não pode entrar em contato com o servidor do WHOIS mesmo depois de você ter enviado várias solicitações do e-mail de validação. Esse problema é externo AWS a. Ou seja, a AWS não controla os servidores do WHOIS servidores e não pode impedir a limitação do servidor do WHOIS. Se esse problema ocorrer, abra um caso no [AWS Support Center](#) para obter ajuda com uma solução alternativa.

## Carimbo de data/hora inicial persistente para validação de e-mail

O carimbo de data/hora da primeira solicitação de validação por e-mail de um certificado persiste nas solicitações posteriores de renovação de validação. Isso não é evidência de erro em operações do ACM.

## Solução de problemas com o domínio de nível superior .IO

O domínio .IO é atribuído ao Território Britânico no Oceano Índico. No momento, o registro de domínio não exibe suas informações públicas do banco de dados WHOIS. Isso é verdadeiro independentemente de a proteção de privacidade para o domínio estar ativada ou desativada. Os registradores poderão exibir essas informações em suas próprias saídas WHOIS se a proteção de privacidade estiver desativada, mas essa prática varia entre os registradores. O ACM não pode enviar o e-mail de validação para os três endereços de contato registrados a seguir se eles não estiverem disponíveis no registrador do WHOIS.

- Domínio registrado

- Contato técnico
- Contato administrativo

Porém, o ACM envia um e-mail de validação para os seguintes cinco endereços comuns do sistema em que o *seu domínio* é o nome de domínio inserido a primeira vez que você solicitou um certificado e *.io* é o domínio de nível superior.

- `administrador@your_domain.io`
- `hostmaster@your_domain.io`
- `postmaster@your_domain.io`
- `webmaster@your_domain.io`
- `admin@your_domain.io`

Para receber um e-mail de validação para um domínio *.IO*, certifique-se de ter habilitado uma das cinco contas de e-mail anteriores. Caso contrário, você não receberá um e-mail de validação, e um certificado do ACM não será emitido.

#### Note

Recomendamos que você use a validação de DNS em vez da validação de e-mail. Para ter mais informações, consulte [Validação por DNS](#).

## Não consigo mudar para a validação de DNS

Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS.

## Solução de problemas de renovação de certificado gerenciado

O ACM tenta renovar automaticamente seus certificados do ACM antes que a validade expire, de forma que você não precise fazer nenhuma ação. Consulte os tópicos a seguir se tiver problemas com [Renovação gerenciada para certificados do ACM](#).

## Preparação para validação automática de domínio

Para que o ACM possa renovar seus certificados automaticamente, o seguinte deve ser verdadeiro:

- Seu certificado deve estar associado a um AWS serviço integrado ao ACM. Para obter informações sobre os recursos que o ACM suporta, consulte [Serviços integrados com AWS Certificate Manager](#).
- Para certificados validados por e-mail, o ACM deve ser capaz de entrar em contato com você em um endereço de e-mail de administrador para cada domínio listado em seu certificado. Os endereços de e-mail que serão tentados estão listados em [Validação de e-mail](#).
- Para certificados validados por DNS, certifique-se de que sua configuração de DNS contenha os registros CNAME corretos, conforme descrito em [Validação por DNS](#).

## Tratamento de falhas de renovação de certificado gerenciada

À medida que o certificado está prestes a expirar (60 dias para DNS, 45 para EMAIL e 60 dias para Privado), o ACM tenta renovar o certificado se ele atender aos [critérios de elegibilidade](#). Talvez seja necessário tomar medidas para concluir a renovação. Para ter mais informações, consulte [Renovação gerenciada para certificados do ACM](#).

### Renovação de certificado gerenciada para certificados validados por e-mail

Os certificados do ACM são válidos por 13 meses (395 dias). Para serem renovados, os certificados validados por e-mail exigem uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação 45 dias antes do prazo de validade, usando os endereços da caixa de correio WHOIS do domínio e para cinco endereços comuns de administrador. As notificações contêm um link no qual o proprietário do domínio pode clicar para facilitar a renovação. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

Consulte [Validar com e-mail](#) para obter instruções sobre como identificar quais domínios estão no estado PENDING\_VALIDATION e repita o processo de validação para esses domínios

### Renovação de certificado gerenciada para certificados validados por DNS

O ACM não tenta realizar a validação de TLS para certificados validados por DNS. Se o ACM não conseguir renovar um certificado validado com a validação por DNS, provavelmente é devido a registros CNAME ausentes ou imprecisos na configuração do DNS. Se isso ocorrer, o ACM notificará você de que o certificado não pôde ser renovado automaticamente.

### ⚠ Important

Você deverá inserir os registros CNAME corretos em seu banco de dados do DNS. Consulte o registrador de domínio sobre como fazer isso.

É possível encontrar os registros CNAME de seus domínios expandindo seu certificado as entradas de domínio no console do ACM. Consulte as figuras a seguir para obter detalhes. Você também pode recuperar registros CNAME usando a [DescribeCertificate](#) operação na API do ACM ou o [comando describe-certificate](#) na CLI do ACM. Para ter mais informações, consulte [Validação por DNS](#).

« < Viewing 1 to 3 of 3 certificates > »

<input type="checkbox"/>	Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
<input type="checkbox"/>		amzn1.example.biz		Issued	Amazon Issued	No	Ineligible
<input type="checkbox"/>		amzn2.example.biz		Validation timed out	Amazon Issued	No	Ineligible
<input type="checkbox"/>		amzn3.example.biz		Issued	Amazon Issued	No	Ineligible

**Status**

Status Issued  
Detailed status The certificate was issued at 2018-03-22T22:42:12UTC

Domain	Validation status
amzn3.example.biz	Success

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

**Details**

Type	Amazon Issued	Requested at	2018-03-22T22:38:52UTC
In use?	No	Issued at	2018-03-22T22:42:12UTC
Domain name	amzn3.example.biz	Not before	2018-03-22T00:00:00UTC
Number of additional names	0	Not after	2019-04-22T12:00:00UTC
Identifier	1fae4ec1-6db6-4d3d-967a-ee5e53ecd45	Public key info	RSA 2048-bit
Serial number	0e:10:30:f3:1c:b4:1e:b7:54:bb:f3:99:62:5b:7f:fb	Signature algorithm	SHA256WITHRSA
		ARN	arn:aws:acm:us-west-2:140948901414:certificate/1fae4ec1-6db6-4d3d-967a-ee5e53ecd45
		Validation state	None

**Tags**

Edit

Name

« < Viewing 1 to 3 of 3 certificates > »

Selecione o certificado de destino no console.

Domain	Validation status
amzn3.example.biz	Success

Add the following CNAME record to the DNS configuration for your domain. The procedure for adding CNAME records depends on your DNS service Provider. [Learn more.](#)

Name	Type	Value
_dc8d107e33e2a83816b6a2a395a5cf5d.amzn.example.biz.	CNAME	_dadbc0aaa5530cf8b0964967cf1d4ed8.acm-validations.aws.

**Note:** Changing the DNS configuration allows ACM to issue certificates for this domain name for as long as the DNS record exists. You can revoke permission at any time by removing the record. [Learn more.](#)

[Create record in Route 53](#) **Amazon Route 53 DNS Customers** ACM can update your DNS configuration for you. [Learn more.](#)

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

Expanda a janela do certificado para encontrar as informações de CNAME.

Se o problema persistir, entre em contato com o [Support Center](#).

## Prazos de renovação

O [Renovação gerenciada para certificados do ACM](#) é um processo assíncrono. Isso significa que as etapas não ocorrem em sucessão imediata. Após todos os nomes de domínio em um certificado do ACM terem sido validados, pode haver um atraso antes de o ACM obter o novo certificado. Um atraso adicional pode ocorrer entre a hora em que o ACM obtém o certificado renovado e a hora em que esse certificado é implantado nos recursos da AWS que o usam. Portanto, as alterações no status do certificado podem demorar várias horas para aparecer no console.

## Solução de outros problemas

Esta seção inclui orientações para problemas não relacionados à emissão ou à validação de certificados do ACM.



## Tópicos

- [Problemas da autorização da autoridade de certificação \(CAA\)](#)
- [Problemas de importação do certificado](#)
- [Problemas de fixação do certificado](#)
- [Problemas do API Gateway](#)
- [O que fazer quando um certificado de trabalho falha inesperadamente](#)
- [Problemas com a função vinculada ao serviço \(SLR\) do ACM](#)

## Problemas da autorização da autoridade de certificação (CAA)

Você pode usar registros do DNS da CAA para especificar que a autoridade de certificação (CA) da Amazon pode emitir certificados do ACM para seu domínio ou subdomínio. Se você receber um erro durante a emissão do certificado que diz `no more domain names have failed validation due to a Certification Authority Authorization (CAA) error` (Falha de validação em um ou mais nomes de domínio devido a um erro de autenticação da autoridade de certificação (CAA)), verifique os registros DNS da CAA. Se receber esse erro depois que a solicitação de certificado do ACM foi validada com êxito, você deverá atualizar seus registros de CAA e solicitar um certificado novamente. O campo `value` (valor) em seu registro de CAA precisa conter um dos seguintes nomes de domínio:

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

Para obter mais informações sobre a criação de um registro de CAA, consulte [\(Opcional\) Configurar um registro de CAA](#).

### Note

Você pode optar por não configurar um registro de CAA para seu domínio se não quiser habilitar a verificação de CAA.

## Problemas de importação do certificado

Você pode importar certificados de terceiros para o ACM e associá-los aos [serviços integrados](#). Se você encontrar problemas, revise os [pré-requisitos](#) e os tópicos de [formato do certificado](#). Observe principalmente o seguinte:

- Só é possível importar certificados SSL/TLS X.509 versão 3.
- O certificado pode ser autoassinado ou pode ser assinado por uma autoridade de certificação (CA).
- Se o certificado for assinado por uma CA, você deverá incluir uma cadeia de certificados intermediária que forneça um caminho para a raiz da autoridade.
- Se o certificado for autoassinado, você deverá incluir a chave privada como texto sem formatação.
- Cada certificado na cadeia deve certificar diretamente o certificado anterior.
- Não inclua o certificado de entidade final na cadeia de certificados intermediária.
- Seu certificado, a cadeia de certificados e a chave privada (se houver) devem ser codificados em PEM. Em geral, a codificação PEM consiste em blocos de texto ASCII codificado na Base64 que começam e terminam com linhas de cabeçalho e rodapé de texto simples. Você não deve adicionar linhas ou espaços nem fazer quaisquer outras alterações em um arquivo PEM durante a cópia ou o upload do mesmo. Você pode verificar cadeias de certificados usando o [utilitário de verificação OpenSSL](#).
- A chave privada (se houver) não deve estar criptografada. (Dica: se tiver uma senha, ela é criptografada.)
- Os serviços [integrados](#) com o ACM devem usar tamanhos de chave e algoritmos suportados pelo ACM. Consulte o Guia AWS Certificate Manager do usuário e a documentação de cada serviço para garantir que seu certificado funcione.
- O suporte aos certificados dos serviços integrados pode ser diferente dependendo de o certificado ser importado para o IAM ou para o ACM.
- O certificado deve estar válido quando ele é importado.
- As informações detalhadas sobre todos os seus certificados são exibidas no console. Por padrão, no entanto, se você chamar a [ListCertificatesAPI](#) ou o AWS CLI comando [list-certificates](#) sem especificar o keyTypes filtro, somente os RSA\_2048 certificados RSA\_1024 ou certificados serão exibidos.

## Problemas de fixação do certificado

Para renovar um certificado, o ACM gera um novo par de chaves pública/privada. Se seu aplicativo usa [Fixação do certificado](#), às vezes conhecido como fixação SSL, para fixar um certificado ACM, talvez o aplicativo não consiga se conectar ao seu domínio depois de AWS renovar o certificado. Por esse motivo, recomendamos que você não fixe um certificado do ACM. Se o seu aplicativo precisa fazer fixação de um certificado, você pode fazer o seguinte:

- [Importe o seu próprio certificado para o ACM](#) e, em seguida, fixe seu aplicativo no certificado importado. O ACM não fornece renovação gerenciada para certificados importados.
- Se você estiver usando um certificado público, fixe o aplicativo a todos os [certificados raiz da Amazon](#) disponíveis. Se você estiver usando um certificado privado, fixe o aplicativo ao certificado raiz da CA.

## Problemas do API Gateway

Quando você implanta um endpoint de API otimizado para borda, o API Gateway configura uma CloudFront distribuição para você. A CloudFront distribuição é de propriedade do API Gateway, não da sua conta. A distribuição é vinculada ao certificado do ACM que você usou ao implantar a API. Para remover o vínculo e permitir que o ACM exclua o certificado, você deve remover o domínio personalizado do API Gateway que está associado ao certificado.

Ao implantar um endpoint de uma API regional, o API Gateway cria um Application Load Balancer (ALB) em seu nome. O balanceador de carga é de propriedade do API Gateway e não é visível a você. O ALB é vinculado ao certificado do ACM que você usou ao implantar a API. Para remover o vínculo e permitir que o ACM exclua o certificado, você deve remover o domínio personalizado do API Gateway que está associado ao certificado.

## O que fazer quando um certificado de trabalho falha inesperadamente

Se você tiver associado com êxito um certificado do ACM a um serviço integrado, mas o certificado parar de funcionar e o serviço integrado começar a retornar erros, a causa pode ser uma alteração nas permissões de que o serviço precisa para usar um certificado do ACM.

Por exemplo, o Elastic Load Balancing (ELB) exige permissão para descriptografar e AWS KMS key isso, por sua vez, decifra a chave privada do certificado. Essa permissão é concedida por uma política baseada em recursos que o ACM aplica quando você associa um certificado ao ELB. Se o

ELB perder a concessão para essa permissão, ele falhará a próxima vez que tentar descriptografar a chave do certificado.

Para investigar o problema, verifique o status de suas concessões usando o AWS KMS console em <https://console.aws.amazon.com/kms>. Depois faça uma das seguintes ações:

- Se você acredita que as permissões concedidas a um serviço integrado foram revogadas, visite o console do serviço integrado, desassocie o certificado do serviço e associe-o novamente. Isto reaplicará a política baseada nos recursos e criará uma nova concessão.
- Se você acredita que as permissões concedidas ao ACM foram revogadas, entre AWS Support em contato em <https://console.aws.amazon.com/support/home#/>.

## Problemas com a função vinculada ao serviço (SLR) do ACM

Quando você emite um certificado assinado por uma CA privada que foi compartilhada com você por outra conta, o ACM tenta primeiro configurar uma função vinculada ao serviço (SLR) para interagir como principal com uma CA privada da AWS política de acesso baseada em recursos. Se você emitir um certificado privado de uma autoridade de certificação compartilhada e o SLR não estiver em vigor, o ACM não poderá renovar automaticamente esse certificado para você.

O ACM pode alertar você de que não é possível determinar se existe uma SLR na sua conta. Se a necessária permissão do `iam:GetRole` já foi concedida à SLR do ACM para sua conta, o alerta não será repetido depois que a SLR for criada. Se ele ocorrer novamente, você ou o administrador da conta podem precisar conceder a permissão `iam:GetRole` ao ACM ou associar sua conta à política `AWSCertificateManagerFullAccess` gerenciada pelo ACM.

Para mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Tratamento de exceções

Um AWS Certificate Manager comando pode falhar por vários motivos. Para obter informações sobre cada exceção, consulte a tabela abaixo.

## Tratamento de exceções de certificado privado

As exceções a seguir podem ocorrer quando você tenta renovar um certificado PKI privado emitido pela CA privada da AWS

**Note**

CA privada da AWS não é suportado na região da China (Pequim) e na região da China (Ningxia).

Código de falha do ACM	Comentário
PCA_ACCESS_DENIED	<p>A CA privada não concedeu permissões ao ACM. Isso aciona um código de CA privada da AWS <code>AccessDeniedException</code> falha.</p> <p>Para solucionar o problema, conceda as permissões necessárias ao responsável pelo serviço do ACM usando a CA privada da AWS <a href="#">CreatePermission</a> operação.</p>
PCA_INVALID_DURATION	<p>O período de validade do certificado solicitado excede o período de validade da CA privada emissora. Isso aciona um código de CA privada da AWS <code>ValidationException</code> falha.</p> <p>Para solucionar o problema, <a href="#">instale um novo certificado CA</a> com um período de validade apropriado.</p>
PCA_INVALID_STATE	<p>A CA privada que está sendo chamada não está no estado correto para executar a operação do ACM solicitada. Isso aciona um código de CA privada da AWS <code>InvalidStateException</code> falha.</p> <p>Resolva o problema da seguinte forma:</p> <ul style="list-style-type: none"> <li>• Se a CA tiver o status <code>CREATING</code>, aguarde a conclusão da criação e instale o certificado CA.</li> </ul>

Código de falha do ACM	Comentário
	<ul style="list-style-type: none"><li>• Se a CA tiver o status PENDING_CERTIFICATE, instale o certificado CA.</li><li>• Se a CA tiver o status DISABLED, atualize-a para o status ACTIVE.</li><li>• Se a CA tiver o status DELETED, restaure-a.</li><li>• Se a autoridade de certificação tiver o status EXPIRED, instale um novo certificado</li><li>• Se a CA tiver o status FAILED, e você não conseguir resolver o problema, entre em contato com o <a href="#">AWS Support</a>.</li></ul>
PCA_LIMIT_EXCEEDED	<p>A CA privada atingiu uma cota de emissão. Isso aciona um código de CA privada da AWS <code>LimitExceededException</code> falha. Tente repetir a solicitação antes de prosseguir com esta ajuda.</p> <p>Se o erro persistir, entre em contato com o <a href="#">AWS Support</a> para solicitar um aumento de cota.</p>
PCA_REQUEST_FAILED	<p>Ocorreu um erro de rede ou de sistema. Isso aciona um código de CA privada da AWS <code>RequestFailedException</code> falha. Tente repetir a solicitação antes de prosseguir com esta ajuda.</p> <p>Se o erro persistir, entre em contato com o <a href="#">AWS Support</a>.</p>

Código de falha do ACM	Comentário
PCA_RESOURCE_NOT_FOUND	<p>A CA privada foi excluída permanentemente. Isso aciona um código de CA privada da AWS <code>ResourceNotFoundException</code> falha. Verifique se você usou o ARN correto. Se isso falhar, você não poderá usar essa CA.</p> <p>Para solucionar o problema, <a href="#">crie outra CA</a>.</p>
SLR_NOT_FOUND	<p>Para renovar um certificado assinado por uma autoridade de certificação privada que reside em outra conta, o ACM requer uma função vinculada ao serviço (SLR) na conta em que o certificado reside. Se você precisar recriar um SLR excluído, consulte <a href="#">Criação da a SLR para o ACM</a>.</p>

# Conceitos

Esta seção fornece as definições dos conceitos usados pelo AWS Certificate Manager.

## Tópicos

- [Certificado do ACM](#)
- [CAs-raiz do ACM](#)
- [Domínio de apex](#)
- [Criptografia de chave assimétrica](#)
- [Certificate Authority \(Autoridade certificadora\)](#)
- [Registro de transparência de certificados](#)
- [Domain Name System](#)
- [Nomes de domínio](#)
- [Criptografia e descriptografia](#)
- [Nome de domínio totalmente qualificado \(FQDN\)](#)
- [Infraestrutura de chave pública](#)
- [Certificado raiz](#)
- [Secure Sockets Layer \(SSL\)](#)
- [HTTPS seguro](#)
- [Certificados do servidor SSL](#)
- [Criptografia de chave simétrica](#)
- [Transport Layer Security \(TLS\)](#)
- [Confiança](#)

## Certificado do ACM

O ACM gera certificados X.509 versão 3. Cada um deles é válido por 13 meses (395 dias) e contém as extensões a seguir.

- **Basic Constraints (Restrições básicas):** especifica se o requerente do certificado é uma autoridade de certificação (CA).



- **Authority Key Identifier (Identificador de chave da autoridade):** permite a identificação da chave pública correspondente à chave privada usada para assinar o certificado.
- **Subject Key Identifier (Identificador de chave do requerente):** permite a identificação de certificados que contenham uma chave pública específica.
- **Key Usage (Uso da chave):** define a finalidade da chave pública incorporada ao certificado.
- **Extended Key Usage (Uso da chave estendido):** especifica um ou mais finalidades de uso da chave pública além das especificadas pela extensão Key Usage (Uso da chave).
- **CRL Distribution Points (Pontos de distribuição do CRL):** especifica onde informações do CRL podem ser obtidas.

O texto simples de um certificado emitido pelo ACM é semelhante ao seguinte exemplo:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

f2:16:ad:85:d8:42:d1:8a:3f:33:fa:cc:c8:50:a8:9e

Signature Algorithm: sha256WithRSAEncryption

Issuer: O=Example CA

Validity

Not Before: Jan 30 18:46:53 2018 GMT

Not After : Jan 31 19:46:53 2018 GMT

Subject: C=US, ST=VA, L=Herndon, O=Amazon, OU=AWS, CN=example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

```
00:ba:a6:8a:aa:91:0b:63:e8:08:de:ca:e7:59:a4:
69:4c:e9:ea:26:04:d5:31:54:f5:ec:cb:4e:af:27:
e3:94:0f:a6:85:41:6b:8e:a3:c1:c8:c0:3f:1c:ac:
a2:ca:0a:b2:dd:7f:c0:57:53:0b:9f:b4:70:78:d5:
43:20:ef:2c:07:5a:e4:1f:d1:25:24:4a:81:ab:d5:
08:26:73:f8:a6:d7:22:c2:4f:4f:86:72:0e:11:95:
03:96:6d:d5:3f:ff:18:a6:0b:36:c5:4f:78:bc:51:
b5:b6:36:86:7c:36:65:6f:2e:82:73:1f:c7:95:85:
a4:77:96:3f:c0:96:e2:02:94:64:f0:3a:df:e0:76:
05:c4:56:a2:44:72:6f:8a:8a:a1:f3:ee:34:47:14:
bc:32:f7:50:6a:e9:42:f5:f4:1c:9a:7a:74:1d:e5:
68:09:75:19:4b:ac:c6:33:90:97:8c:0d:d1:eb:8a:
02:f3:3e:01:83:8d:16:f6:40:39:21:be:1a:72:d8:
```

```
5a:15:68:75:42:3e:f0:0d:54:16:ed:9a:8f:94:ec:
59:25:e0:37:8e:af:6a:6d:99:0a:8d:7d:78:0f:ea:
40:6d:3a:55:36:8e:60:5b:d6:0d:b4:06:a3:ac:ab:
e2:bf:c9:b7:fe:22:9e:2a:f6:f3:42:bb:94:3e:b7:
08:73
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Authority Key Identifier:

keyid:84:8C:AC:03:A2:38:D9:B6:81:7C:DF:F1:95:C3:28:31:D5:F7:88:42

X509v3 Subject Key Identifier:

97:06:15:F1:EA:EC:07:83:4C:19:A9:2F:AF:BA:BB:FC:B2:3B:55:D8

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 CRL Distribution Points:

Full Name:

URI:http://example.com/crl

Signature Algorithm: sha256WithRSAEncryption

```
69:03:15:0c:fb:a9:39:a3:30:63:b2:d4:fb:cc:8f:48:a3:46:
69:60:a7:33:4a:f4:74:88:c6:b6:b6:b8:ab:32:c2:a0:98:c6:
8d:f0:8f:b5:df:78:a1:5b:02:18:72:65:bb:53:af:2f:3a:43:
76:3c:9d:d4:35:a2:e2:1f:29:11:67:80:29:b9:fe:c9:42:52:
cb:6d:cd:d0:e2:2f:16:26:19:cd:f7:26:c5:dc:81:40:3b:e3:
d1:b0:7e:ba:80:99:9a:5f:dd:92:b0:bb:0c:32:dd:68:69:08:
e9:3c:41:2f:15:a7:53:78:4d:33:45:17:3e:f2:f1:45:6b:e7:
17:d4:80:41:15:75:ed:c3:d4:b5:e3:48:8d:b5:0d:86:d4:7d:
94:27:62:84:d8:98:6f:90:1e:9c:e0:0b:fa:94:cc:9c:ee:3a:
8a:6e:6a:9d:ad:b8:76:7b:9a:5f:d1:a5:4f:d0:b7:07:f8:1c:
03:e5:3a:90:8c:bc:76:c9:96:f0:4a:31:65:60:d8:10:fc:36:
44:8a:c1:fb:9c:33:75:fe:a6:08:d3:89:81:b0:6f:c3:04:0b:
a3:04:a1:d1:1c:46:57:41:08:40:b1:38:f9:57:62:97:10:42:
8e:f3:a7:a8:77:26:71:74:c2:0a:5b:9e:cc:d5:2c:c5:27:c3:
12:b9:35:d5
```

## CAs-raiz do ACM

Os certificados públicos de entidade final emitidos pelo ACM geram sua confiança das seguintes CAs-raiz da Amazon:

Nome distinto	Algoritmo de criptografia
CN=Amazon Root CA 1, O=Amazon, C=US	RSA de 2048 bits (RSA_2048)
CN=Amazon Root CA 2, O=Amazon, C=US	RSA de 4096 bits (RSA_4096)
CN=Amazon Root CA 3, O=Amazon, C=US	Elliptic Prime Curve de 256 bits (EC_prime256v1 )
CN=Amazon Root CA 4, O=Amazon, C=US	Elliptic Prime Curve de 384 bits (EC_secp384r1 )

A raiz padrão de confiança para certificados emitidos pelo ACM é CN=Amazon Root CA 1, O=Amazon, C=US, que oferece segurança RSA de 2048 bits. As outras raízes estão reservadas para uso futuro. Todas as raízes têm assinatura cruzada pelo certificado de autoridade de certificação raiz Starfield Services.

Para obter mais informações, consulte [Amazon Trust Services](#).

## Domínio de apex

Consulte [Nomes de domínio](#).

## Criptografia de chave assimétrica

Ao contrário da [Criptografia de chave simétrica](#), a criptografia assimétrica usa chaves diferentes, mas matematicamente relacionadas, para criptografar e descriptografar o conteúdo. Uma das chaves é pública e, normalmente, é disponibilizada em um certificado X.509 v3. A outra chave é privada e fica armazenada em segurança. O certificado X.509 vincula a identidade de um usuário, computador ou outro recurso (o assunto do certificado) à chave pública.

Os certificados do ACM são certificados X.509 SSL/TLS que vinculam a identidade do seu site e os detalhes da sua organização à chave pública contida no certificado. O ACM usa a AWS KMS

key para criptografar a chave privada. Para ter mais informações, consulte [Segurança para chaves privadas de certificados](#).

## Certificate Authority (Autoridade certificadora)

Uma autoridade certificadora (CA) é uma entidade que emite certificados digitais. Comercialmente, o tipo mais comum de certificado digital é baseado no padrão ISO X.509. A CA emite certificados digitais assinados que afirmam a identidade do certificado específico e vinculam essa identidade à chave pública contida no certificado. Em geral, a CA também gerencia a revogação de certificados.

## Registro de transparência de certificados

Para se proteger contra certificados SSL/TLS emitidos por engano ou por um CA comprometida, alguns navegadores exigem que os certificados públicos emitidos para seu domínio sejam registrados em um log de transparência de certificados. O nome de domínio é registrado. A chave privada, não. Os certificados não registrados normalmente geram um erro no navegador.

É possível monitorar os logs para garantir a emissão de apenas certificados autorizados para seu domínio. É possível usar um serviço como o [Certificate Search](#) para verificar os logs.

Antes de emitir um certificado SSL/TLS publicamente confiável para seu domínio, a CA da Amazon envia-o a pelo menos três servidores de log de transparência de certificados. Esses servidores adicionam o certificado aos bancos de dados públicos e retornam um carimbo de tempo do certificado assinado (SCT) para a CA da Amazon. A CA incorpora o SCT no certificado, assina o certificado e emite-o para você. Os carimbos de tempo são incluídos com outras extensões X.509.

```
X509v3 extensions:
```

```
CT Precertificate SCTs:
```

```
Signed Certificate Timestamp:
```

```
Version    : v1(0)
```

```
Log ID     : BB:D9:DF:...8E:1E:D1:85
```

```
Timestamp : Apr 24 23:43:15.598 2018 GMT
```

```
Extensions: none
```

```
Signature  : ecdsa-with-SHA256
```

```
30:45:02:...18:CB:79:2F
```

```
Signed Certificate Timestamp:
```

```
Version    : v1(0)
```

```
Log ID      : 87:75:BF:...A0:83:0F
Timestamp  : Apr 24 23:43:15.565 2018 GMT
Extensions: none
Signature  : ecdsa-with-SHA256
            30:45:02:...29:8F:6C
```

O registro de transparência de certificados é automático ao solicitar ou renovar um certificado, a menos que você cancele essa opção. Para obter mais informações o cancelamento, consulte [Cancelamento do registro em log de transparência de certificado](#).

## Domain Name System

O Domain Name System (DNS) é um sistema de nomeação distribuído hierárquico para computadores e outros recursos conectados à internet ou a uma rede privada. O DNS é usado principalmente para converter nomes de domínio textuais, como `aws.amazon.com`, em endereços IP (Internet Protocol) numéricos no formato `111.122.133.144`. O banco de dados do DNS de seu domínio, no entanto, contém vários registros que podem ser usados para outros fins. Por exemplo, com o ACM você pode usar um registro CNAME para validar que possui ou controla um domínio ao solicitar um certificado. Para ter mais informações, consulte [Validação por DNS](#).

## Nomes de domínio

Um nome de domínio é uma string de texto, como `www.example.com`, que pode ser convertida pelo Domain Name System (DNS) em um endereço IP. As redes de computadores, incluindo a Internet, usam endereços IP em vez de nomes textuais. Um nome de domínio consiste em diferentes rótulos separados por pontos:

### TLD

O rótulo mais à direita é chamado de domínio de nível superior (TLD). Exemplos comuns incluem `.com`, `.net` e `.edu`. Além disso, o TLD das entidades registradas em alguns países é uma abreviação do nome do país e é chamado de código do país. Alguns exemplos são `.uk` para o Reino Unido, `.ru` para a Rússia e `.fr` para França. Quando os códigos de países são usados, uma hierarquia de segundo nível do TLD é frequentemente apresentada para identificar o tipo da entidade registrada. Por exemplo, o TLD `.co.uk` identifica empresas comerciais no Reino Unido.

### Domínio de apex

O nome de domínio de apex inclui e expande o domínio de nível superior. Para nomes de domínio que incluem um código de país, o domínio de apex inclui o código e os rótulos, se houver algum, que identificam o tipo da entidade registrada. O domínio de apex não inclui subdomínios (consulte o parágrafo a seguir). Em `www.example.com`, o nome de domínio apex é `example.com`. Em `www.example.co.uk`, o nome de domínio apex é `example.co.uk`. Outros nomes frequentemente usados em lugar de apex são base, raiz, apex de raiz ou apex de zona.

## Subdomínio

Os nomes dos subdomínios precedem o nome do domínio de apex e são separados dele, e entre si, por um período. O nome de subdomínio mais comum é `www`, mas qualquer nome é possível. Os nomes de subdomínios podem ter vários níveis. Por exemplo, em `jake.dog.animals.example.com`, os subdomínios são `jake`, `dog` e `animals`, nessa ordem.

## Superdomínio

O domínio ao qual um subdomínio pertence.

## FQDN

Um nome de domínio totalmente qualificado (FQDN) é o nome DNS completo de um computador, site ou outro recurso conectado a uma rede ou à Internet. Por exemplo, `aws.amazon.com` é o FQDN para o Amazon Web Services. Um FQDN inclui todos os domínios até o domínio de nível mais alto. Por exemplo, `[subdomain1].[subdomain2]. . . [subdomainn].[apex domain].[top-level domain]` representa o formato geral de um FQDN.

## PQDN

Um nome de domínio que não é totalmente qualificado é chamado de nome de domínio parcialmente qualificado (PQDN), e é ambíguo. Um nome como `[subdomain1.subdomain2.]` é um PQDN porque o domínio raiz não pode ser determinado.

## Registro

O direito de usar um nome de domínio é delegado pelos registradores de nomes de domínio. Os registradores normalmente são credenciados pela Internet Corporation for Assigned Names and Numbers (ICANN). Além disso, outras organizações chamadas registros mantêm os bancos de dados TLD. Quando você solicita um nome de domínio, o registrador envia suas informações para o registro do TLD apropriado. O registro atribui um nome de domínio, atualiza o banco de dados TLD e publica suas informações no WHOIS. Normalmente, os nomes de domínio devem ser adquiridos.

# Criptografia e descriptografia

A criptografia é o processo de fornecer a confidencialidade dos dados. A descriptografia reverte o processo e recupera os dados originais. Os dados não criptografados normalmente são chamados de texto simples sejam ou não texto. Os dados criptografados geralmente são chamados de texto cifrado. A criptografia HTTPS de mensagens entre clientes e servidores usa algoritmos e chaves. Os algoritmos definem o step-by-step procedimento pelo qual os dados de texto simples são convertidos em texto cifrado (criptografia) e o texto cifrado é convertido novamente no texto sem formatação original (decodificação). As chaves são usadas pelos algoritmos durante o processo de criptografia ou descriptografia. As chaves podem ser privadas ou públicas.

## Nome de domínio totalmente qualificado (FQDN)

Consulte [Nomes de domínio](#).

## Infraestrutura de chave pública

Uma infraestrutura de chave pública (PKI) consiste em hardware, software, pessoas, políticas, documentos e procedimentos necessários para criar, emitir, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A PKI facilita a transferência segura de informações em redes de computadores.

## Certificado raiz

Uma autoridade certificadora (CA) normalmente existe em uma estrutura hierárquica que contém várias outras CAs com relacionamentos pai-filho claramente definidos entre eles. CAs subordinadas (ou filhas) são certificadas pelas CAs de seus pais, criando uma cadeia de certificados. A CA no alto da hierarquia é chamada de CA raiz, e seu certificado é chamado de certificado raiz. Este certificado é geralmente autoassinado.

## Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) são protocolos de criptografia que fornecem segurança na comunicação em uma rede de computadores. TLS é o sucessor do SSL. Ambos usam certificados X.509 para autenticar o servidor. Os dois protocolos negociam uma chave simétrica entre o cliente e o servidor, que é usada para criptografar os dados entre as duas entidades.

## HTTPS seguro

HTTPS significa HTTP sobre SSL/TLS, uma forma de HTTP seguro que é compatível com todos os principais navegadores e servidores. Todas as solicitações e respostas HTTP são criptografadas antes de serem enviadas pela rede. HTTPS combina o protocolo HTTP com técnicas de criptografia simétricas, assimétricas e baseadas em certificado X.509. HTTPS funciona inserindo uma camada de segurança de criptografia abaixo da camada de aplicativos HTTP e acima da camada de transporte TCP no modelo Open Systems Interconnection (OSI). A camada de segurança usa o protocolo Secure Sockets Layer (SSL) ou o protocolo de Transport Layer Security (TLS).

## Certificados do servidor SSL

As transações HTTPS exigem certificados de servidor para autenticar um servidor. Um certificado de servidor é uma estrutura de dados X.509 v3 que vincula a chave pública no certificado ao assunto do certificado. Um certificado SSL/TLS é assinado por uma autoridade certificadora (CA) e contém o nome do servidor, o período de validade, a chave pública, o algoritmo de assinatura e mais.

## Criptografia de chave simétrica

A criptografia de chave simétrica usa a mesma chave para criptografar e descriptografar dados digitais. Consulte também [Criptografia de chave assimétrica](#).

## Transport Layer Security (TLS)

Consulte [Secure Sockets Layer \(SSL\)](#).

## Confiança

Para que um navegador da web confie na identidade de um site, o navegador deve ser capaz de verificar o certificado do site. Os navegadores, no entanto, confiam em apenas um pequeno número de certificados conhecidos como certificados CA raiz. Um terceiro confiável, conhecido como uma autoridade certificadora (CA), valida a identidade do site e emite um certificado digital assinado para o operador do site. O navegador pode, então, verificar a assinatura digital para validar a identidade do site. Se a validação for bem-sucedida, o navegador exibe um ícone de cadeado na barra de endereços.



## Histórico do documento

A tabela a seguir descreve o histórico de versões da documentação do AWS Certificate Manager a partir de 2018.

Alteração	Descrição	Data
<a href="#">Próxima descontinuação da verificação de e-mail do WHOIS</a>	Foi adicionada uma observação sobre a suspensão da verificação de e-mail do WHOIS a partir de junho de 2024.	5 de fevereiro de 2024
<a href="#">Adição de suporte a chave de condição</a>	Foi adicionado suporte a chaves de condição do IAM na solicitação de certificados do ACM. Para ver a lista de condições compatíveis, consulte <a href="https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported">https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported</a> .	24 de agosto de 2023
<a href="#">Suporte ECDSA adicionado</a>	Adicionado suporte para Elliptic Curve Digital Signature Algorithm (ECDSA) ao solicitar um certificado ACM público. Para ver uma lista dos algoritmos de chave suportados, consulte <a href="https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms">https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms</a> .	8 de novembro de 2022
<a href="#">Novos CloudWatch eventos</a>	Adicionados eventos ACM Certificate Expired, ACM	27 de outubro de 2022

Certificate Available e ACM Certificate Renewal Action Required. Para obter uma lista de CloudWatch eventos compatíveis, consulte <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html>.

[Atualização dos tipos de algoritmo de chave para importação](#)

Os certificados importados para o ACM agora podem ter chaves com algoritmos RSA e curva elíptica adicionais. Para ver uma lista dos algoritmos de chave suportados no momento, consulte <https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html>.

14 de julho de 2021

[Promoção de "Monitoramento e registro em log" a um capítulo separado.](#)

Movida a documentação de monitoramento e registro em log para seu próprio capítulo. Essa alteração abrange CloudWatch métricas, CloudWatch eventos/ EventBridge e CloudTrail. Para ter mais informações, consulte <https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html>.

23 de março de 2021

[Suporte adicionado a CloudWatch métricas e eventos](#)

Foram adicionadas DaysToExpiry métricas, eventos e APIs de suporte. Para obter mais informações, consulte <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html> e <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html>.

3 de março de 2021

[Adicionado suporte abrangendo todas as contas](#)

Adição de suporte entre contas para o uso de CAs privadas da CA privada da AWS. Para ter mais informações, consulte <https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html>.

17 de agosto de 2020

[Adição de suporte à região](#)

Adição de suporte regional para as regiões da AWS China (Pequim e Ningxia). Para obter uma lista completa das regiões compatíveis, consulte [https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca\\_region](https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region).

4 de março de 2020

<a href="#">Adicionados testes de fluxo de trabalho de renovação</a>	Agora, os clientes podem testar manualmente a configuração do seu fluxo de trabalho de renovação gerenciada do ACM. Para obter mais informações, consulte <a href="#">Testar a configuração de renovação gerenciada do ACM</a> .	14 de março de 2019
<a href="#">O registro em log da transparência dos certificados agora é padrão</a>	Adicionada a capacidade de publicar certificados públicos do ACM em logs de transparência de certificados por padrão.	24 de abril de 2018
<a href="#">Lançamento da CA privada da AWS</a>	Lançado o Private Certificate Manager (CM) do ACM, uma extensão do AWS Certificate Manager que permite que os usuários estabeleçam uma infraestrutura gerenciada e segura para emissão e revogação de certificados digitais e privados. Para obter mais informações, consulte <a href="#">AWS Private Certificate Authority</a> .	4 de abril de 2018
<a href="#">Registro em log da transparência dos certificados</a>	Adicionado o registro em log de transparência de certificados às melhores práticas.	27 de março de 2018

A tabela a seguir descreve o histórico de versões da documentação do AWS Certificate Manager antes de 2018.

Alteração	Descrição	Data de lançamento
Novo conteúdo	Validação de DNS adicionada a <a href="#">Validação por DNS</a> .	21 de novembro de 2017
Novo conteúdo	Adição de novos exemplos de código Java a <a href="#">Usar a API (exemplos de Java)</a> .	12 de outubro de 2017
Novo conteúdo	Adição de informações sobre registros de CAA a <a href="#">(Opcional) Configurar um registro de CAA</a> .	21 de setembro de 2017
Novo conteúdo	Informações adicionadas sobre domínios .IO a <a href="#">Solução de problemas</a> .	07 de julho de 2017
Novo conteúdo	Informações adicionadas sobre reimportação de um certificado a <a href="#">Reimportação de um certificado</a> .	07 de julho de 2017
Novo conteúdo	Informações adicionadas sobre fixação de certificado a <a href="#">Práticas recomendadas</a> e a <a href="#">Solução de problemas</a> .	07 de julho de 2017
Novo conteúdo	adicionado a .AWS CloudFormation <a href="#">Serviços integrados com AWS Certificate Manager</a>	27 de maio de 2017
Atualizar	Mais informações adicionadas a <a href="#">Cotas</a> .	27 de maio de 2017
Novo conteúdo	Documentação adicionada sobre <a href="#">Identity and Access</a>	28 de abril de 2017

Alteração	Descrição	Data de lançamento
	<a href="#">Management para o AWS Certificate Manager.</a>	
Atualizar	Gráfico adicionado para mostrar para onde o e-mail de validação é enviado. Consulte <a href="#">Validação de e-mail.</a>	21 de abril de 2017
Atualizar	Informações adicionadas sobre a configuração de e-mail para o seu domínio. Consulte <a href="#">(Opcional) Configurar e-mail para seu domínio.</a>	6 de abril de 2017
Atualizar	Informações adicionadas sobre a verificação de status da renovação do certificado no console. Consulte <a href="#">Verificar o status de renovação de um certificado.</a>	28 de março de 2017
Atualizar	Atualização da documentação para usar o Elastic Load Balancing.	21 de março de 2017
Novo conteúdo	Adicionado suporte para AWS Elastic Beanstalk e Amazon API Gateway. Consulte <a href="#">Serviços integrados com AWS Certificate Manager.</a>	21 de março de 2017
Atualizar	Documentação sobre <a href="#">Renovação gerenciada</a> atualizada.	20 de fevereiro de 2017
Novo conteúdo	Documentação adicionada sobre <a href="#">Importar certificados.</a>	13 de outubro de 2016

Alteração	Descrição	Data de lançamento
Novo conteúdo	Adicionado suporte do AWS CloudTrail para as ações do ACM. Consulte <a href="#">Usando CloudTrail com AWS Certificate Manager</a> .	25 de março de 2016
Novo guia	Essa versão apresenta o AWS Certificate Manager.	21 de janeiro de 2016

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.