Manual do usuário

AWS Certificate Manager

Versão 1.0

AWS Certificate Manager: Manual do usuário

Table of Contents

O que AWS Certificate Manageré

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 AWS 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 independente em uma EC2 instância da Amazon, o tutorial a seguir tem instruções: Configurar no SSL/TLS Amazon Linux 2023.

Tópicos

Regiões do compatíveis

O ACM oferece suporte IPv4 e IPv6 em endpoints públicos. Acesse Regiões e endpoints da AWS em Referência geral da AWS ou a Tabela de regiões da AWS para visualizar a disponibilidade regional do ACM.

Os certificados no ACM são recursos regionais. Para usar um certificado com o ELB 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.

Preços para AWS Certificate Manager

Você não está sujeito a uma cobrança adicional pelos SSL/TLS certificados com os quais você gerencia 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.

AWS Certificate Manager conceitos

Esta seção fornece definições dos conceitos usados por AWS Certificate Manager.

Tópicos

- Certificado do ACM
- Raiz do ACM CAs
- 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)
- Hypertext Transfer Protocol (HTTP)
- Infraestrutura de chave pública (PKI)
- 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).

> **Important**
>
> A partir de 11 de junho de 2025, AWS Certificate Manager não emite mais certificados com o uso estendido de chave (EKU) da “Autenticação de Cliente Web TLS” (ClientAuth) para se alinhar aos novos requisitos de navegador para certificados de sites.

- 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
            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
```

Raiz do ACM CAs

Os certificados públicos de entidade final emitidos pelo ACM derivam sua confiança da seguinte raiz da Amazon: CAs

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 ACM são certificados X.509 que vinculam a identidade do seu site e os detalhes da sua organização à chave pública contida no SSL/TLS certificado. O ACM usa sua AWS KMS key para criptografar a chave privada. Para obter 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 SSL/TLS certificados emitidos por engano ou por uma CA comprometida, alguns navegadores exigem que os certificados públicos emitidos para seu domínio sejam registrados em um registro 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 a Amazon CA emitir um SSL/TLS certificado publicamente confiável para seu domínio, ela envia o certificado para pelo menos três servidores de registro 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 obter mais informações, consulte Validação de DNS do AWS Certificate Manager.

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 de apex é `example.com`. Em `www.example.co.uk`, o nome de domínio de 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, $[subdomain_1].[subdomain_2]...[subdomain_n].[apex\ domain].[top\text{-}level\ domain]$ 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.

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.

Hypertext Transfer Protocol (HTTP)

O Hypertext Transfer Protocol (HTTP) é fundamental para comunicação de dados na World Wide Web. Ele é um protocolo da camada da aplicação que habilita a troca de vários tipos de conteúdo. O HTTP opera no modelo cliente-servidor, por meio do qual os navegadores da Web geralmente atuam como clientes que solicitam recursos de servidores da Web. Por ser um protocolo sem estado, o HTTP trata cada solicitação de forma independente, sem reter informações de solicitações anteriores.

No contexto do ACM, o HTTP pode ser usado para validação de domínio ao emitir certificados. SSL/TLS Esse processo envolve o envio de solicitações HTTP específicas por parte do ACM para fins de verificação de propriedade do domínio. A capacidade do servidor de responder corretamente a essas solicitações demonstra o controle sobre o domínio.

Diferentemente dos certificados validados por e-mail ou por DNS, os clientes do ACM não podem emitir certificados validados por HTTP diretamente do ACM. Em vez disso, esses certificados são emitidos e gerenciados automaticamente como parte do processo de CloudFront provisionamento.

Os clientes podem usar o ACM para visualizar, monitorar e gerenciar esses certificados, mas a emissão inicial é feita pela integração entre o ACM e. CloudFront

Embora o HTTP seja amplamente usado, cabe salientar que ele transmite dados em texto simples. Para comunicação segura, é usado HTTPS (HTTP Secure), que criptografa os dados usando SSL/TLS protocolos. Para obter mais informações sobre comunicações seguras, consulte HTTPS seguro.

Infraestrutura de chave pública (PKI)

A infraestrutura de chave pública (PKI) é um sistema de processos, tecnologias e políticas que permite a comunicação segura em redes públicas. No contexto do ACM, a PKI desempenha um papel fundamental na emissão, no gerenciamento e na validação de certificados digitais. A PKI usa um par de chaves criptográficas: uma chave pública, distribuída gratuitamente, e uma chave privada, mantida em segredo pelo proprietário. Esse sistema permite a transmissão segura de dados, as assinaturas digitais e autenticação de entidades digitais.

O ACM implementa vários componentes principais da PKI. Ele atua como uma autoridade de certificação (CA), um terceiro confiável que emite certificados digitais vinculando chaves públicas a entidades como domínios ou organizações. O ACM emite os certificados X.509, os quais contêm informações sobre a entidade, a chave pública correspondente e o período de validade do certificado. Ele também lida com o ciclo de vida completo dos certificados, inclusive a emissão, a renovação e a revogação. Para assegurar a legitimidade das solicitações de certificados, o ACM oferece suporte a vários métodos para validar a propriedade do domínio, como a validação por DNS e a validação por HTTP.

Ao aproveitar a PKI, o ACM permite conexões HTTPS seguras, assinaturas digitais e comunicação criptografada para AWS recursos e aplicativos. Essa infraestrutura é essencial para manter a confidencialidade, a integridade e a autenticidade dos dados transmitidos pela internet. Para obter mais informações sobre como o ACM implementa a PKI, consulte Começando com AWS Certificate Manager certificados.

Certificado raiz

Uma autoridade de certificação (CA) normalmente existe dentro de uma estrutura hierárquica que contém várias outras CAs com relações pai-filho claramente definidas entre elas. A criança ou o subordinado CAs são certificados pelos pais CAs, 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 SSL/TLS certificado é assinado por uma autoridade de certificação (CA) e contém o nome do servidor, o período de validade, a chave pública, o algoritmo de assinatura e muito 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.

Qual é o serviço de AWS certificação certo para minhas necessidades?

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: este serviço destina-se a clientes corporativos que criam uma infraestrutura de chave pública (PKI) dentro da nuvem da AWS e destina-se a uso privado dentro de 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 obter mais informações, consulte o Guia do usuário do CA privada da AWS.

Começando com AWS Certificate Manager certificados

O ACM gerencia certificados públicos, privados e importados. Os certificados são 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**
>
> Os certificados públicos do ACM podem ser instalados em EC2 instâncias da Amazon conectadas a um Nitro Enclave. Você também pode exportar um certificado público para usar em qualquer EC2 instância da Amazon. Para obter informações sobre como configurar um servidor web autônomo em uma EC2 instância da Amazon 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 console AWS de gerenciamento e abra o console do ACM em casahttps://console.aws.amazon.com/acm/. Se a página introdutória for exibida, escolha Get Started (Iniciar). Caso contrário, escolha Certificate Manager ou Private CAs no painel de navegação esquerdo.

Tópicos

- Configurado para usar AWS Certificate Manager

Configurado para usar AWS Certificate Manager

Com o AWS Certificate Manager (ACM), você pode provisionar e gerenciar SSL/TLS certificados para seus sites e aplicativos AWS baseados. Você usa o ACM para criar ou importar e, em seguida, gerenciar um certificado. Você deve usar outros AWS serviços para implantar o certificado em seu site ou aplicativo. Para obter mais informações sobre os serviços integrados com o ACM, consulte Serviços integrados ao ACM. Os tópicos a seguir discutem as etapas que você precisa desempenhar antes de usar o ACM.

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a 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. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Registrar um nome de domínio para o ACM

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 registro de nomes de domínio geralmente tem duração determinada, como um ou dois anos antes de precisar ser renovado.

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 um registro de CAA

Um registro CAA especifica quais autoridades de certificação (CAs) estão autorizadas a emitir certificados para um domínio ou subdomínio. Criar um registro CAA para uso com o ACM ajuda a evitar que o erro CAs emita certificados para seus domínios. Um registro CAA não é um substituto para os requisitos de segurança que são especificados por sua autoridade de certificação, como o requisito para validar que você é o proprietário de um domínio.

Após o ACM validar seu domínio durante o processo de solicitação de certificado, ele verifica a presença de registros de CAA para ter certeza de que ele pode emitir um certificado para você. A configuração de um registro CAA é opcional.

Use os seguintes valores ao configurar seu registro CAA:

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. Observe que, se você planeja usar a validação por HTTP, essa configuração não se aplica porque a validação por HTTP não oferece suporte a certificados curingas. Use a validação por DNS ou e-mail para certificados curingas.

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 CAA que especifique uma das quatro Amazon a seguir CAs, o ACM não poderá 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.

> **Important**
>
> Se você planeja usar a validação HTTP com CloudFront, não precisa configurar registros issuewild porque a validação HTTP não oferece suporte a certificados curinga. Use a validação por DNS ou e-mail para certificados curingas.

```
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.

AWS Certificate Manager certificados públicos

Após solicitar um certificado público, você deverá validar a propriedade do domínio, conforme descrito em Valide a propriedade do domínio para certificados públicos do AWS Certificate Manager.

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 obter 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 público automaticamente após 11 meses.

> **Note**
>
> Os certificados públicos do ACM podem ser instalados em EC2 instâncias da Amazon conectadas a um Nitro Enclave. Você também pode exportar um certificado público para usar em qualquer EC2 instância da Amazon. Para obter informações sobre como configurar um servidor web autônomo em uma EC2 instância da Amazon 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 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. Se você tiver problemas ao solicitar um certificado, consulte Solucionar problemas de solicitações de certificado.

Para solicitar um certificado para usar uma PKI privada CA privada da AWS, consulteSolicitar um certificado privado no AWS Certificate Manager.

Tópicos

- AWS Certificate Manager características e limitações do certificado público
- Solicitar um certificado público no AWS Certificate Manager

- AWS Certificate Manager certificados públicos exportáveis
- Valide a propriedade do domínio para certificados públicos do AWS Certificate Manager

AWS Certificate Manager características e limitações do certificado público

Os certificados públicos fornecidos pelo ACM têm as características e limitações a seguir. Essas características se aplicam apenas aos certificados fornecidos pelo ACM. Elas podem não se aplicar a certificados importados.

Confiança em navegadores e aplicativos

Os certificados do ACM são da confiança de todos os principais navegadores, incluindo Google Chrome, Microsoft Edge, Mozilla Firefox e Apple Safari. Os navegadores exibem um ícone de cadeado quando conectados por TLS a sites que usam certificados do ACM. Java também confia nos certificados do ACM.

Autoridade e hierarquia de certificação

Os certificados públicos que você solicitou por meio do ACM são obtidos da Amazon Trust Services, uma autoridade de certificação (CA) pública gerenciada pela Amazon. O Amazon Root CAs 1 a 4 tem assinatura cruzada pela Starfield G2 Root Certificate Authority — G2. A raiz Starfield é confiável no Android (versões mais novas do Gingerbread) e iOS (versão 4.1+). As raízes da Amazon são confiáveis no iOS 11+. Navegadores, aplicativos, OSes incluindo raízes da Amazon ou Starfield, confiarão nos certificados públicos do ACM.

O ACM emite certificados preliminares ou de entidade final aos clientes por meio de certificados intermediários CAs, atribuídos aleatoriamente com base no tipo de certificado (RSA ou ECDSA). O ACM não fornece informações intermediárias de CA devido a essa seleção aleatória.

Validação de domínio (DV)

Os certificados do ACM têm validação de domínio, identificando somente um nome de domínio. Ao solicitar um certificado do ACM, você deve provar a propriedade ou o controle de todos os domínios especificados. Você pode validar a propriedade usando e-mail ou DNS. Para obter mais informações, consulte Validação de e-mail do AWS Certificate Manager e Validação de DNS do AWS Certificate Manager.

Validação por HTTP

O ACM oferece suporte à validação HTTP para verificação da propriedade do domínio ao emitir certificados TLS públicos para uso com. CloudFront Esse método usa redirecionamentos HTTP para provar a propriedade do domínio e oferece renovação automática semelhante à validação de DNS. Atualmente, a validação de HTTP só está disponível por meio do recurso CloudFront Distribution Tenants.

Redirecionamento HTTP

Para validação por HTTP, o ACM fornece um URL `RedirectFrom` e um URL `RedirectTo`. Você deve configurar um redirecionamento de `RedirectFrom` para `RedirectTo` para demonstrar controle do domínio. O `RedirectFrom` URL inclui o domínio validado, enquanto `RedirectTo` aponta para um local controlado pelo ACM na CloudFront infraestrutura contendo um token de validação exclusivo.

Gerenciado por

Os certificados no ACM gerenciados por outro serviço mostram a identidade desse serviço no campo `ManagedBy`. Para certificados usando validação HTTP com CloudFront, esse campo exibe “CLOUDFRONT”. Esses certificados só podem ser usados por meio de CloudFront. O `ManagedBy` campo aparece em DescribeCertificate e e ListCertificates APIs nas páginas de detalhes e inventário de certificados no console do ACM.

O campo `ManagedBy` é mutuamente excludente com o atributo “Pode ser usado com”. Para certificados CloudFront gerenciados, você não pode adicionar novos usos por meio de outros AWS serviços. Você só pode usar esses certificados com mais recursos por meio da CloudFront API.

Rotação CA intermediária e raiz

A Amazon pode descontinuar uma CA intermediária sem aviso prévio para manter uma infraestrutura de certificados resiliente. Essas mudanças não afetam os clientes. Para obter mais informações, consulte “Amazon apresenta autoridades de certificação intermediárias dinâmicas”.

Se a Amazon descontinuar uma CA raiz, a alteração ocorrerá tão rapidamente quanto necessário. A Amazon usará todos os métodos disponíveis para notificar AWS os clientes AWS Health Dashboard, incluindo e-mail e contato com gerentes técnicos de contas.

Acesso ao firewall para revogação

Os certificados de entidade final revogados usam OCSP e CRLs para verificar e publicar informações de revogação. Alguns firewalls de clientes podem precisar de regras adicionais para permitir esses mecanismos.

Use esses padrões curingas de URL para identificar o tráfego de revogação:

- OCSP

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

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

- CRL

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

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

Um asterisco (*) representa um ou mais caracteres alfanuméricos, um ponto de interrogação (?) representa um único caractere alfanumérico e um símbolo do jogo da velha (#) representa um número.

Algoritmos-chave

Os certificados devem especificar um algoritmo e um tamanho de chave. O ACM oferece suporte aos seguintes algoritmos de chave pública RSA e ECDSA:

- 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`)

O ACM pode solicitar novos certificados usando os algoritmos marcados com um asterisco (*). Os outros algoritmos são somente para certificados importados.

> **Note**
>
> Para certificados PKI privados assinados por uma CA Privada da AWS CA, a família de algoritmos de assinatura (RSA ou ECDSA) deve corresponder à família de algoritmos de chave secreta da CA.

As chaves ECDSA são menores e mais eficientes computacionalmente do que as chaves RSA de segurança comparável, mas nem todos os clientes de rede oferecem suporte ao ECDSA. Esta tabela, adaptada do NIST, compara os tamanhos das chaves RSA e ECDSA (em bits) para obter força de segurança equivalente:

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	521

A força de segurança, 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 ajuda na escolha de um algoritmo, consulte a postagem do AWS blog Como avaliar e usar certificados ECDSA em. AWS Certificate Manager

> **Important**
>
> Os Serviços integrados só permitem os algoritmos e tamanhos de chave com suporte para seus recursos. O suporte varia dependendo de o certificado ser importado para o IAM ou para o ACM. Para obter detalhes, consulte a documentação de cada serviço:
>
> - Para ELB, consulte HTTPS Listeners for Your Application Load Balancer.
> - Para isso CloudFront, consulte SSL/TLS Protocolos e cifras compatíveis.

Renovação e implantação gerenciadas

O ACM gerencia a renovação e o provisionamento dos certificados correspondentes. A renovação automática ajuda a evitar tempo de inatividade devido a certificados com erros de configuração, revogados ou expirados. Para obter mais informações, consulte Renovação gerenciada do certificado em AWS Certificate Manager.

Vários nomes de domínio

Cada certificado do ACM deve incluir pelo menos um nome de domínio totalmente qualificado (FQDN) e pode incluir mais nomes. Por exemplo, um certificado para `www.example.com` também pode incluir `www.example.net`. Isso também se aplica a domínios simples (ápex da zona ou domínios nus). Você pode solicitar um certificado para www.example.com e incluir example.com. Para obter mais informações, consulte AWS Certificate Manager certificados públicos.

Punycode

Os requisitos de Punycode a seguir para Nomes de domínio internacionalizados devem ser atendidos:

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	Satisfazo n.º 1	Satisfazo n.º 2	Permit	Observação
exemplo.com	n/a	n/a	✓	Não começa com “<character><character>--”
a--example.com	n/a	n/a	✓	Não começa com “<character><character>--”
abc--example.com	n/a	n/a	✓	Não começa com “<character><character>--”

Nome do domínio	Satisfazo n.º 1	Satisfazo n.º 2	Permit	Observação
xn--xyz.com	Sim	Sim	✓	Nome de domínio internacionalizado válido (é resolvido para 简.com)
xn--example.com	Sim	Não	✗	Não é um nome de domínio internacionalizado válido
ab--example.com	Não	Não	✗	Deve começar com “xn--”

Período de validade

Os certificados do ACM são válidos por 13 meses (395 dias).

Nomes curinga

O ACM permite um asterisco (*) no nome de domínio para criar um certificado curinga para proteger vários sites no mesmo domínio. Por exemplo, `*.example.com` protege `www.example.com` e `images.example.com`.

Em um certificado curinga, o asterisco (*) deve estar na posição mais à esquerda do nome do domínio e só protege um nível de subdomínio. Por exemplo, `*.example.com` protege `login.example.com` e `test.example.com`, mas não `test.login.example.com`. Além disso, `*.example.com` protege apenas os subdomínios, não o domínio vazio ou apex (`example.com`). É possível solicitar um certificado para um domínio vazio e seus subdomínios especificando vários nomes de domínio, como `example.com` e `*.example.com`.

> **Important**
>
> Se você usa CloudFront, observe que a validação HTTP não oferece suporte a certificados curinga. Para certificados curingas, você deve usar a validação por DNS ou a validação por e-mail. É recomendável a validação por DNS porque ela oferece suporte à renovação automática do certificado.

Solicitar um certificado público no AWS Certificate Manager

Você pode solicitar certificados AWS Certificate Manager públicos do console do ACM ou da API. AWS CLI Você pode usar esses certificados integrados Serviços da AWS ou exportá-los para uso fora do Nuvem AWS.

A lista a seguir descreve as diferenças entre certificados públicos e certificados públicos exportáveis.

Certificados públicos

Use certificados públicos do ACM integrados, Serviços da AWS como ELB CloudFront, Amazon e Amazon API Gateway. Para obter mais informações, consulte Serviços integrados ao ACM.

> **Note**
>
> Os certificados públicos do ACM criados antes de 17 de junho de 2025 não podem ser exportados.

Certificados públicos exportáveis

Os certificados públicos exportáveis funcionam de forma integrada Serviços da AWS e também podem ser usados externamente Nuvem AWS. Para obter mais informações, consulte AWS Certificate Manager certificados públicos exportáveis e Serviços integrados ao ACM. Você deve criar um novo certificado público do ACM e habilitar “exportável” para poder exportar o certificado público.

As seções a seguir descrevem como solicitar, exportar e revogar um certificado público do ACM.

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 console AWS de gerenciamento e abra o console do ACM em https://console.aws.amazon.com/acm/casa.

   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 vaziou 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 Assunto e na extensão 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. Se você quiser criar certificados públicos exportáveis do ACM, selecione a opção Habilitar exportação. Você poderá acessar as chaves privadas do certificado e usá-las fora da Nuvem

AWS. Para obter mais informações, consulte AWS Certificate Manager certificados públicos exportáveis.

4. 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 de DNS do AWS Certificate Manager.

   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.

   a. Se você escolher a validação por e-mail, o ACM enviará um e-mail de validação para o domínio especificado no campo do nome do domínio. Se você especificar um domínio de validação, o ACM enviará um e-mail para esse domínio de validação. Para obter mais informações sobre a validação de e-mail, consulte Validação de e-mail do AWS Certificate Manager.

   b. 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 de DNS do AWS Certificate Manager.

5. Na seção Algoritmo-chave, escolha um algoritmo.

6. 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 Marcar recursos do AWS Certificate Manager.

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

7. 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 Com falha ou Tempo limite da validação excedido, exclua a solicitação, corrija o problema com a Validação por DNS ou 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,Export=ENABLED
```

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

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

AWS Certificate Manager certificados públicos exportáveis

AWS Certificate Manager certificados públicos exportáveis permitem provisionar, gerenciar e implantar certificados SSL/TLS em qualquer lugar, incluindo EC2 instâncias, contêineres e hosts locais da Amazon. Esse recurso estende os certificados públicos emitidos pelo ACM além dos integrados Serviços da AWS, oferecendo controle centralizado sobre os certificados em toda a sua infraestrutura.

Benefícios

A seguir, descrevemos os benefícios dos certificados públicos exportáveis do ACM:

- Gerenciamento simplificado de certificados: gerencie centralmente os certificados de todos os seus recursos com o ACM.
- Emissão mais rápida de certificados: acesse e use certificados em menos tempo.
- Renovações automatizadas: o ACM gerencia automaticamente as renovações de certificados e notifica você quando novos certificados estiverem prontos para implantação. Para obter mais informações, consulte EventBridge Suporte da Amazon para ACM.
- Econômico: pague somente pelos certificados públicos exportáveis que você criar.
- Implantação flexível: use certificados com qualquer servidor ou aplicação que suporte certificados SSL/TLS padrão.

Como funcionam os certificados públicos exportáveis do ACM

A seguir, descrevemos como os certificados públicos exportáveis do ACM funcionam:

1. Solicite um certificado exportável por meio do ACM para seu domínio.
2. Confirme a propriedade do domínio usando a validação por DNS ou e-mail.
3. Exporte o certificado, a chave privada e a cadeia de certificados.
4. Implante o certificado em seu servidor ou aplicação.
5. O ACM gerencia as renovações e envia notificações quando novos certificados estão disponíveis.

Considerações sobre segurança

A seguir estão as considerações de segurança ao usar certificados públicos exportáveis do ACM. Para obter mais informações, consulte Proteção de dados em AWS Certificate Manager.

- Proteja as chaves privadas exportadas usando controles de acesso e armazenamento seguro.
- Use o atributo de revogação do ACM se suspeitar de comprometimento da chave.
- Implemente procedimentos adequados de rotação de chaves ao implantar certificados renovados.

Limitações

A seguir estão algumas limitações do certificado do ACM:

- Os certificados têm um período de validade de 13 meses (395 dias).
- O ACM renova os certificados após 11 meses. O ACM renovará os certificados que expirarão 60 dias antes da data de expiração.
- Você deve gerenciar o processo de implantação dos certificados exportados.

Preços

Você está sujeito a uma cobrança adicional pelos SSL/TLS certificados públicos exportáveis que você cria com AWS Certificate Manager. Para obter as informações mais recentes sobre preços do ACM, consulte a página AWS Certificate Manager de preços de serviços no AWS site.

Práticas recomendadas

A seguir, algumas práticas recomendadas ao usar os certificados do ACM:

- Depois que um certificado for renovado, você deve começar a usá-lo imediatamente.
- Teste e implemente processos de implantação automatizados para os certificados renovados.
- Monitore implantações de certificados usando EventBridge métricas e alarmes da Amazon.

Exportar um certificado AWS Certificate Manager público

Os procedimentos a seguir explicam como você pode exportar um certificado público do ACM no console do ACM. Como alternativa, você pode usar a ação `export-certificate` AWS CLI ou ExportCertificateAPI.

> **Note**
>
> Os certificados públicos do ACM criados antes de 17 de junho de 2025 não podem ser exportados.

Exportar um certificado público (console)

1. Faça login no Console de gerenciamento da AWS e abra o console do ACM em https://console.aws.amazon.com/acm/.
2. Escolha Listar certificados e marque a caixa de seleção do certificado que você deseja exportar.
   - Como alternativa, você pode selecionar o certificado. Na página de detalhes do certificado, selecione Exportar.
3. Escolha Mais ações e, em seguida, Exportar.
4. Insira e confirme uma frase secreta para a chave privada.
5. Você pode baixar ou copiar os arquivos do certificado.

> **Note**
>
> No console do ACM, você pode exportar arquivos de certificado .pem. Você pode converter o arquivo .pem em outro formato de arquivo, como .ppk. Para obter mais informações, consulte este artigo do re:Post.

Exportar um certificado público (AWS CLI)

Use o `export-certificate` AWS CLI comando ou a ação ExportCertificateda API para exportar um certificado público e uma chave privada. 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.

```
[Windows/Linux]$ aws acm export-certificate \
    --certificate-arn arn:aws:acm:us-east-1:111122223333: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-----
MIIDTDCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwWOdLOkxpwkkKWtcEkQuHE1v5Vn6HpbfFmxkdPEasoDhthH
FFWIf4/+VOlbDLgjU4HgtmV4IJDtqM9rGOZ42eFYmmc3eQO0GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmannS8j6YxmtpPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQQKDAh0cm9sb2xvbDCCASIwDQYJKoZIhvcNAQEBBQADggEP
...
j2PAOviqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPdl+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCAggAMB0GCWCGSAFlAwQBKgQQDViroIHStQgNOjR6nTUnuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTPskNCdCAHqdhOSqBwt65qUTZe3gBt
```

```
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrrxuHTWjFl
wEuqyd8X/ApkQsYFX/nhepOEIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxfOC1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs9OV/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----
```

Para gerar a saída de tudo para um arquivo, acrescente o redirecionamento > ao exemplo anterior, resultando no seguinte comando:

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:us-east-1:111122223333:certificate/certificate_ID \
     --passphrase fileb://path-to-passphrase-file \
     | jq -r '"\(.Certificate)\(.CertificateChain)\(.PrivateKey)"' \
     > /tmp/export.txt
```

Proteja cargas de trabalho do Kubernetes com certificados ACM

Você pode usar certificados públicos AWS Certificate Manager exportáveis com AWS Controllers for Kubernetes (ACK) para emitir e exportar certificados TLS públicos do ACM para suas cargas de trabalho do Kubernetes. Essa integração permite que você proteja os pods do Amazon Elastic Kubernetes Service (Amazon EKS) e encerre o TLS no seu Kubernetes Ingress. Para começar, consulte o Controlador ACM para Kubernetes ativado. GitHub

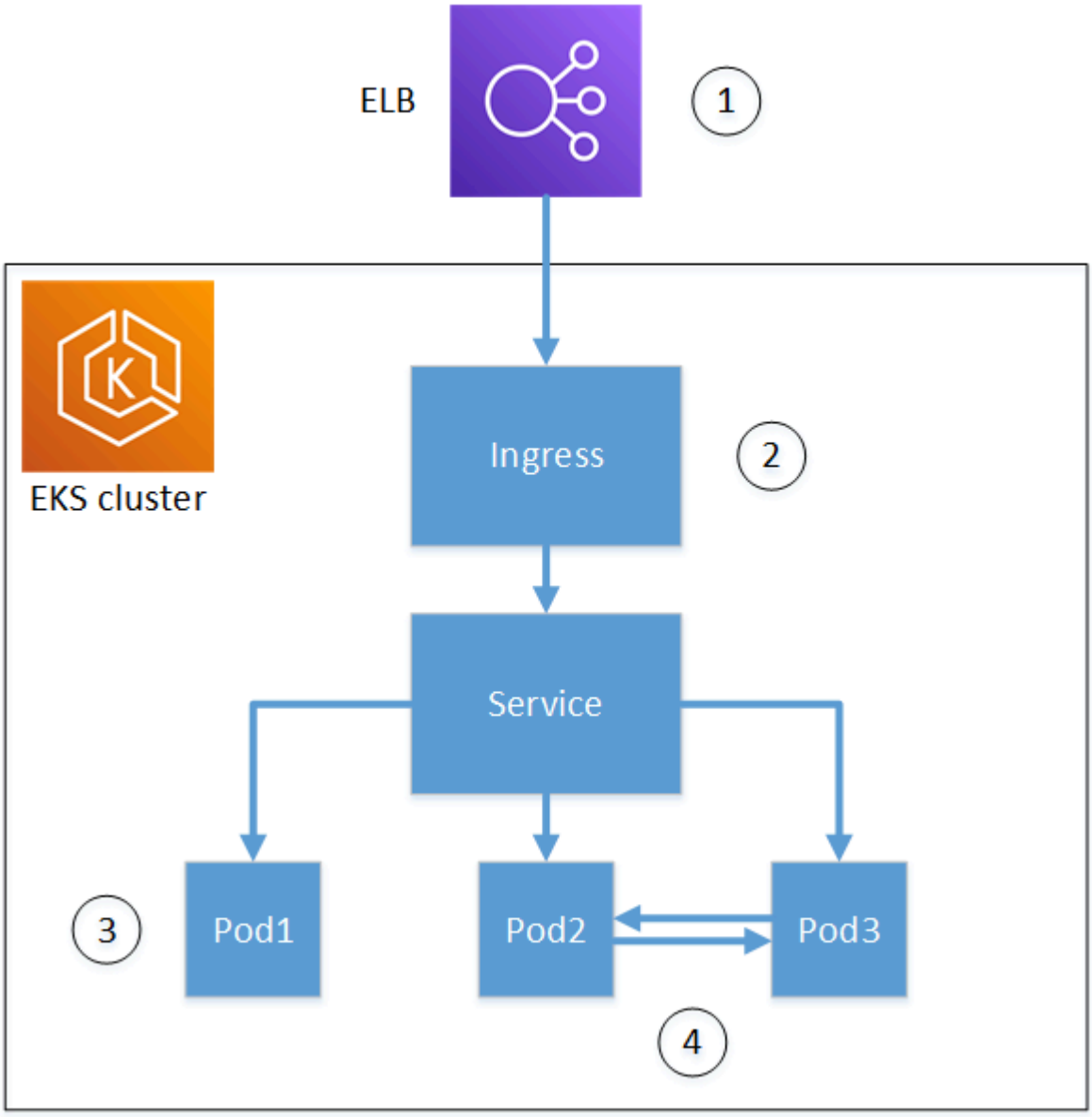
AWS Os controladores para Kubernetes (ACK) estendem a API Kubernetes para gerenciar recursos usando manifestos nativos do Kubernetes. AWS O controlador de serviço ACK para ACM fornece gerenciamento automatizado do ciclo de vida do certificado em seu fluxo de trabalho do Kubernetes. Quando você cria um recurso de certificado ACM no Kubernetes, o controlador ACK executa as seguintes ações:

1. Solicita um certificado do ACM, que gera a solicitação de assinatura de certificado (CSR).
2. Aguarda a conclusão da validação do domínio e a emissão do certificado pelo ACM.
3. Se o `exportTo` campo for especificado, exporta o certificado emitido e a chave privada e os armazena no segredo do Kubernetes especificado.
4. Se o `exportTo` campo for especificado e o certificado estiver qualificado para renovação, atualize o segredo do Kubernetes com certificados renovados antes da expiração.

Os certificados emitidos publicamente exigem a validação do domínio antes que o ACM possa emiti-los. Você pode usar o controlador de serviço ACK para o Amazon Route 53 para criar automaticamente os registros CNAME de validação de DNS necessários na sua zona hospedada.

Opções de uso do certificado

Você pode usar certificados ACM com o Kubernetes de algumas maneiras:



1. Encerramento do balanceador de carga (sem exportação): emita certificados por meio do ACK e use-os para encerrar o TLS em um AWS balanceador de carga. O certificado permanece no ACM e é descoberto automaticamente pelo Load AWS Balancer Controller. Essa abordagem não exige a exportação do certificado.

2. Encerramento de entrada (com exportação): exporte certificados do ACM e armazene-os no Kubernetes Secrets para terminação de TLS no nível de entrada. Isso permite que você use certificados diretamente em suas cargas de trabalho do Kubernetes.

> **Note**
>
> Para casos de uso que exigem certificados privados, consulte AWS Private CA Connector for Kubernetes, um plug-in cert-manager.

Pré-requisitos

Antes de instalar o controlador de serviço ACK para ACM, verifique se você tem o seguinte:

- Um cluster Kubernetes.
- Capacete instalado.
- O `kubectl` configurado para se comunicar com o cluster.
- `eksctl`instalado para configurar associações de identidade de pod no EKS.

Instale o controlador de serviço ACK para ACM

Use o Helm para instalar o controlador de serviço ACK para ACM em seu cluster Amazon EKS.

1. Crie um namespace para o controlador ACK.

```
$ kubectl create namespace ack-system --dry-run=client -o yaml | kubectl apply -f -
```

2. Crie uma associação de identidade de pod para o controlador ACK. *CLUSTER_NAME*Substitua pelo nome do seu cluster e *REGION* pela sua AWS região.

```
$ eksctl create podidentityassociation --cluster CLUSTER_NAME --region REGION \
    --namespace ack-system \
    --create-service-account \
    --service-account-name ack-acm-controller \
    --permission-policy-arns arn:aws:iam::aws:policy/
AWSCertificateManagerFullAccess
```

3. Faça login no registro público do Amazon ECR.

```
$ aws ecr-public get-login-password --region us-east-1 | helm registry login --
username AWS --password-stdin public.ecr.aws
```

4. Instale o controlador de serviço ACK para ACM. *REGION*Substitua pela sua AWS região.

```
$ helm install -n ack-system ack-acm-controller oci://public.ecr.aws/
aws-controllers-k8s/acm-chart --set serviceAccount.create=false --set
 serviceAccount.name=ack-acm-controller --set aws.region=REGION
```

5. Verifique se o controlador está em execução.

```
$ kubectl get pods -n ack-system
```

Para obter mais informações sobre associações de identidade de pod, consulte EKS Pod Identity no Guia do usuário do Amazon EKS.

Exemplo: Encerrar o TLS no Ingress

O exemplo a seguir demonstra como exportar um certificado ACM e usá-lo para encerrar o TLS no nível do Kubernetes Ingress. Essa configuração cria um certificado ACM, o exporta para um segredo do Kubernetes e configura um recurso de entrada para usar o certificado para terminação de TLS.

Neste exemplo:

- O segredo é criado para armazenar o certificado exportado () `exported-cert-secret`
- O recurso ACK Certificate solicita um certificado do ACM para seu domínio e o exporta para o `exported-cert-secret` Secret.
- O recurso Ingress faz referência `exported-cert-secret` ao para encerrar o TLS para tráfego de entrada.

`${HOSTNAME}`Substitua pelo seu nome de domínio.

```
apiVersion: v1
kind: Secret
type: kubernetes.io/tls
metadata:
  name: exported-cert-secret
  namespace: demo-app
```

```
data:
  tls.crt: ""
  tls.key: ""
---
apiVersion: acm.services.k8s.aws/v1alpha1
kind: Certificate
metadata:
  name: exportable-public-cert
  namespace: demo-app
spec:
  domainName: ${HOSTNAME}
  options:
    certificateTransparencyLoggingPreference: ENABLED
  exportTo:
    namespace: demo-app
    name: exported-cert-secret
    key: tls.crt
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress-traefik
  namespace: demo-app
spec:
  tls:
  - hosts:
    - ${HOSTNAME}
    secretName: exported-cert-secret
  ingressClassName: traefik
  rules:
  - host: ${HOSTNAME}
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: whoami
            port:
              number: 80
```

Depois de implantado, o controlador de serviço ACK para ACM gerencia automaticamente o ciclo de vida do certificado, incluindo renovações. Quando o ACM renova o certificado, o controlador atualiza

o `exported-cert-secret` segredo com o novo certificado, garantindo que seu Ingress continue usando certificados válidos sem intervenção manual.

Revogar um certificado AWS Certificate Manager público

Você pode revogar um certificado público AWS Certificate Manager exportável usando o console do ACM ou a ação da AWS CLI API.

> **Warning**
>
> Depois que um certificado for revogado, você não poderá reutilizá-lo. A revogação de um certificado é permanente.

Talvez seja necessário revogar um certificado para estar em conformidade com as políticas da sua organização ou mitigar o comprometimento da chave. É necessário um motivo para revogar um certificado. Os seguintes motivos podem ser usados:

- Não especificado
- Afiliação alterada
- Substituído
- Cessação da operação

Para saber mais, consulte o Acordo de assinante do certificado do Amazon Trust Services e o Amazon Trust Service.

AWS fornece dois serviços para verificar revogações de certificados: Online Certificate Status Protocol (OCSP) e lista de revogação de certificados. Com o OCSP, o cliente consulta um banco de dados de revogação autoritativo que retorna um status em tempo real. O OCSP depende das informações de validação incorporadas nos certificados.

Considerações

Veja a seguir algumas considerações antes de revogar um certificado:

- Você só pode revogar certificados que foram exportados anteriormente.
- Você não pode revogar certificados públicos não exportáveis. Se não precisar mais desses certificados, você deve excluí-los.

- Se não precisar mais dos certificados, você deve excluir os certificados, em vez de revogá-los.
- O processo de revogação do certificado é global. Todos os certificados válidos que você decidir revogar serão revogados junto com os associados. ARNs
- A revogação do certificado é permanente. Você não pode recuperar os certificados revogados para reutilização.
- Pode levar até 24 horas para que a revogação do certificado entre em vigor.

Revogar um certificado (console)

Os procedimentos a seguir explicam como você pode revogar um certificado público ou privado do ACM.

1. Faça login no Console de gerenciamento da AWS e abra o console do ACM em https://console.aws.amazon.com/acm/.
2. Escolha Listar certificados e marque a caixa de seleção do certificado que você deseja revogar.
   - Como alternativa, você pode selecionar o certificado. Na página de detalhes do certificado, selecione Revogar.
3. Escolha Mais ações e, em seguida, Revogar.
4. É exibida uma caixa de diálogo na qual você deve fornecer um motivo para a revogação, inserir **`revoke`** e escolher Revogar.

Revogar um certificado (AWS CLI)

Use o `revoke-certificate` AWS CLI comando ou a ação `RevokeCertificate`da API para revogar um certificado público ou privado do ACM. É possível recuperar o ARN do certificado chamando o comando `list-certificates`.

```
$ aws acm revoke-certificate \
    --certificate-arn arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234 \
    --revocation-reason "UNSPECIFIED"
```

> **Warning**
>
> Depois que um certificado for revogado, você não poderá reutilizá-lo. A revogação de um certificado é permanente.

A saída do comando `revoke-certificate` seria como mostrado a seguir.

```
arn:aws:acm:us-east-1:111122223333:certificate/12345678-1234-1234-1234
```

Configurar eventos de renovação automática

Com certificados públicos AWS Certificate Manager exportáveis e a Amazon EventBridge, você pode configurar eventos de renovação automática de certificados.

1. Configure um EventBridge evento da Amazon para monitorar as renovações de certificados. Para obter mais informações, consulte o EventBridge suporte da Amazon para o ACM.
2. Crie automação para lidar com a implantação de certificados quando ocorrerem renovações. Para obter mais informações, consulte Iniciando ações com a Amazon EventBridge no ACM.
3. Configure EventBridge eventos para alertá-lo sobre qualquer falha de renovação ou implantação.

Forçar renovação de certificado

Você pode renovar seus certificados públicos e privados do ACM com o console do ACM, o certificado de renovação ou a ação da API AWS CLI. `RenewCertificate` Você só pode renovar os certificados que foram exportados anteriormente.

> **Important**
>
> Quando você renova um certificado público exportável do ACM, é cobrada uma taxa adicional. Para obter as informações mais recentes sobre preços do ACM, consulte a página AWS Certificate Manager de preços de serviços no AWS site.

Renovar um certificado (console)

O procedimento a seguir explica como você pode forçar a renovação de um certificado público ou privado do ACM.

1. Faça login no Console de gerenciamento da AWS e abra o console do ACM em https://console.aws.amazon.com/acm/.
2. Escolha Listar certificados e marque a caixa de seleção do certificado que você deseja renovar.
   - Como alternativa, você pode selecionar o certificado. Na página de detalhes do certificado, selecione Renovar.
3. Escolha Mais ações e, em seguida, Renovar.
4. É exibida uma caixa de diálogo na qual você deve inserir **`renew`** e escolher Renovar.

Renovar um certificado (AWS CLI)

Use o `renew-certificate` AWS CLI comando ou a ação `RenewCertificate`da API para renovar um certificado público ou privado do ACM. É possível recuperar o ARN do certificado chamando o comando `list-certificates`. O comando `renew-certificate` não retorna uma resposta.

```
$ aws acm renew-certificate \
    --certificate-arn arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012
```

Valide a propriedade do domínio para certificados públicos do AWS Certificate Manager

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), validação por e-mail ou validação por HTTP quando 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 obter mais informações, consulte Solucionar problemas de validação de certificados.

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 um ou mais dos cinco endereços de administrador comuns do domínio. 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 puder editar o banco de dados de DNS do seu domínio, você deve usar a validação por e-mail em seu lugar.

A validação HTTP está disponível para certificados usados com o CloudFront. Esse método usa redirecionamentos HTTP para provar a propriedade do domínio e oferece renovação automática semelhante à validação de DNS.

> **Note**
>
> Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS. Para usar a validação de DNS, exclua o certificado e crie um novo que use a validação de DNS.

Tópicos

Validação de DNS do AWS Certificate Manager

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. Para usar a validação de DNS, exclua o certificado e crie um novo que use a validação de 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 domínio da AWS que o ACM usa para renovar seu certificado automaticamente. 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 região da AWS, 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 do certificado em AWS Certificate Manager.

> **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
*.exemplo.com	*_x1*.exemplo.com.	*_x2*.acm-validações.aws.	Idêntico
exemplo.com	*_x1*.exemplo.com.	*_x2*.acm-validações.aws.	
www.exemplo.com	*_x3*.www.exemplo.com.	*_x4*.acm-validações.aws.	Exclusivo
host.exemplo.com	*_x5*.host.exemplo.com.	*_x6*.acm-validações.aws.	Exclusivo
subdomínio.exemplo.com	*_x7*.subdomínio.exemplo.com.	*_x8*.acm-validações.aws.	Exclusivo
host.subdomínio.exemplo.com	*_x9*.host.subdomínio.exemplo.com.	*_x10*.acm-validações.aws.	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	_a79865eb4cd1a6ab990a45779b4e0b96.exemplo.com.	CNAME	_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.

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. Consequentemente, 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**
>
> Este procedimento pressupõe que você já tenha criado pelo menos um certificado e que esteja trabalhando na região da AWS onde o criou. Se tentar abrir o console e visualizar a tela de primeiro uso, ou se conseguir abrir o console e não vir seu certificado na lista, verifique se 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 Criar registros no Route 53 não aparecer ou estiver desabilitado, consulte Console do ACM não exibe o botão “Criar registros no Route 53”.

Selecione Criar registros no Route 53 e, em seguida, escolha 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. Você pode, contudo, fazer uma chamada de AWS CLI ou de API para que o Route 53 crie o registro no banco de dados de 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 do AWS Certificate Manager

Para que a autoridade de certificação (CA) da Amazon possa emitir um certificado para seu site, o AWS Certificate Manager (ACM) deve verificar que você possui ou controla todos os domínios especificados na sua solicitação. Você pode executar uma verificação usando o e-mail ou o DNS. Este tópico discute a validação de e-mail.

Se você tiver problemas ao usar a validação de e-mail, consulte Solução de problemas de validação de e-mail.

Como a validação por e-mail funciona

O ACM envia mensagens de e-mail de validação para os cinco e-mails do sistema comuns a seguir para cada domínio. Como alternativa, você pode especificar um superdomínio como domínio de validação se quiser receber esses e-mails nesse domínio. Qualquer subdomínio até o endereço mínimo do site é válido e é usado como domínio para o endereço de e-mail como o sufixo após @. Por exemplo, você poderá receber um e-mail para admin@example.com se especificar exemplo.com como o domínio de validação para subdomínio.exemplo.com.

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

Para comprovar que o domínio é seu, você deverá selecionar o link de validação incluído nesses e-mails. O ACM também envia e-mails de validação para esses mesmos endereços para renovar o certificado quando o certificado estiver a 45 dias de expirar.

A validação por e-mail de solicitações de certificado de vários domínios usando a API ou a CLI do ACM faz com que uma mensagem de e-mail seja enviada por cada domínio solicitado, mesmo se a solicitação incluir subdomínios de outros domínios na solicitação. O proprietário do domínio precisa validar uma mensagem de e-mail para cada um desses domínios antes que o ACM possa emitir o certificado.

Exceção a este processo

Se você solicitar um certificado do ACM para um nome de domínio que comece com **www** ou um asterisco como curinga (*), o ACM removerá o **www** ou o asterisco inicial e enviará e-mails para os endereços administrativos. Esses endereços são formados, antepondo admin@, administrador@, hostmaster@, postmaster@ e webmaster@ ao 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.

> **Important**
>
> O ACM não oferece mais suporte à validação por e-mail do WHOIS no caso de novos certificados ou de renovações. Os endereços comuns do sistema permanecem com suporte. Para obter detalhes, consulte a publicação do blog.

Considerações

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 obter mais informações, consulte Solucionar problemas de validação de certificados.
- Depois de criar um certificado com validação de e-mail, você não pode alternar para validá-lo com DNS. Para usar a validação de DNS, exclua o certificado e crie um novo que use a validação de DNS.

Data de expiração da validade e de renovação do certificado

Os certificados do ACM são válidos por 13 meses (395 dias). A renovação de um certificado exige uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação para os endereços de e-mail associados ao domínio 45 dias antes da expiração. As notificações contêm um link no qual o proprietário do domínio pode clicar para renová-lo. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

(Opcional) Reenviar de 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. Para obter informações sobre como reenviar um e-mail de validação, consulte Reenviar o e-mail de validação

Em caso de problemas persistentes com a validação de e-mail, consulte a seção Solução de problemas de validação de e-mail em Solucionar problemas com o AWS Certificate Manager.

Automatizar a validação por e-mail do AWS Certificate Manager

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.

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
and follow the instructions on the page.

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

Sincerely,
Amazon Web Services

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

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

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

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 nome de domínio ou para o domínio de validação especificado quando você solicita um certificado público. 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 faz com que uma mensagem de e-mail seja enviada por cada domínio solicitado, mesmo se a solicitação incluir subdomínios de outros domínios na solicitação. O proprietário do domínio precisa validar uma mensagem de e-mail para cada um desses domínios antes que o ACM possa emitir o certificado.

  Se você reenviar e-mails de um certificado existente por meio do console do ACM, os e-mails serão enviados para o domínio de validação especificado na solicitação de certificado original ou para o domínio exato se nenhum domínio de validação tiver sido especificado. Para receber e-mails de validação em um domínio diferente, é possível solicitar um novo certificado e especificar o domínio de validação que você deseja usar para validação. Como alternativa, você pode chamar ResendValidationEmail com o parâmetro `ValidationDomain` usando a API, o SDK ou a CLI. No entanto, o domínio de validação especificado na solicitação `ResendValidationEmail` é usado somente para essa chamada e não é salvo no nome do recurso da Amazon (ARN) do certificado para futuros e-mails de validação. Será necessário chamar `ResendValidationEmail` sempre que você quiser receber um e-mail de validação em um nome de domínio que não foi especificado na solicitação de certificado original.

> **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`.

Validação por HTTP do AWS Certificate Manager

O Hypertext Transfer Protocol (HTTP) é um protocolo fundamental para a comunicação de dados na World Wide Web. Quando a validação por HTTP é selecionada para os certificados usados com o CloudFront, o ACM aproveita esse protocolo para verificar a propriedade do seu domínio. O ACM trabalha em conjunto com o CloudFront para fornecer a você um URL específico e um token exclusivo que devem ser colocados à disposição nesse URL em seu domínio. Esse token serve como prova de que você controla o domínio. Ao configurar um redirecionamento do seu domínio para um local controlado pelo ACM na infraestrutura do CloudFront, você demonstra capacidade de modificar conteúdo no domínio, o que valida sua propriedade. Essa integração perfeita entre o ACM e o CloudFront simplifica o processo de emissão de certificados, especialmente para distribuições do CloudFront.

> **Important**
>
> A validação por HTTP não oferece suporte a certificados de domínio curingas (como *.exemplo.com). Para certificados curingas, use a validação por DNS ou a validação por e-mail.

Por exemplo, se você solicitar um certificado para o domínio `example.com` com `www.example.com` como um nome adicional que usa o CloudFront, o ACM fornecerá dois

conjuntos de URLs para validação por HTTP. Cada conjunto contém um URL `redirectFrom` e um URL `redirectTo`, os quais foram criados especificamente para seu domínio e sua conta da AWS. O URL `redirectFrom` é um caminho no seu domínio (por exemplo, `http://example.com/.well-known/pki-validation/example.txt`) que precisa ser configurado. O URL `redirectTo` aponta para um local controlado pelo ACM na infraestrutura do CloudFront, no qual um token de validação exclusivo é armazenado. Você só precisa configurar esses redirecionamentos uma vez. Quando uma autoridade de certificação tenta validar a propriedade do seu domínio, ela solicita o arquivo da URL `redirectFrom`, que o CloudFront redireciona para a URL `redirectTo`, o que permite o acesso ao token de validação. O ACM renova automaticamente seu certificado, desde que o certificado esteja em uso com o CloudFront e seu redirecionamento permaneça em vigor.

Depois de configurar a validação por HTTP para um nome de domínio totalmente qualificado (FQDN) com o CloudFront, você pode solicitar certificados adicionais do ACM para este FQDN sem precisar repetir o processo de validação, desde que o redirecionamento HTTP permaneça 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 por HTTP funciona em qualquer região da AWS em que o CloudFront esteja disponível, você pode recriar o mesmo certificado em várias regiões. Também é possível substituir um certificado excluído sem passar pelo processo de validação novamente, desde que o redirecionamento ainda esteja ativo.

Existem duas opções para a interrupção da renovação automática do seu certificado validado por HTTP. É possível remover o certificado da distribuição do CloudFront à qual ele está associado ou excluir o redirecionamento HTTP configurado para validação. Se estiver sendo usada uma rede de entrega de conteúdo (CDN) ou um servidor web diferente do CloudFront para gerenciar seus redirecionamentos, a documentação correspondente deve ser consultada para saber como remover um redirecionamento. Se o CloudFront estiver sendo usado para gerenciar seus redirecionamentos, o redirecionamento pode ser removido mediante a atualização da configuração da sua distribuição. Para obter mais informações sobre a renovação de certificados gerenciados, consulte Renovação gerenciada do certificado em AWS Certificate Manager. Lembrete: interromper a renovação automática pode levar à expiração do certificado, o que pode interromper seu tráfego HTTPS.

Como funcionam os redirecionamentos HTTP para o ACM

> **Note**
>
> Esta seção foi elaborada para clientes usuários do CloudFront para a entrega de conteúdo e o ACM para o gerenciamento de certificado TLS/SSL.

Quando a validação por HTTP com o ACM e o CloudFront é adotada, é necessário configurar os redirecionamentos HTTP. Esses redirecionamentos permitem que o ACM verifique a propriedade do seu domínio para que ocorra a emissão inicial do certificado e a renovação automática contínua. O mecanismo de redirecionamento funciona indicado um URL específico no seu domínio para um local controlado pelo ACM na infraestrutura do CloudFront na qual um token de validação exclusivo é armazenado.

A tabela a seguir mostra exemplos de configurações de redirecionamento para nomes de domínio. Observe que a validação por HTTP não oferece suporte a domínios curinga (como *.exemplo.com). Cada par Redirecionar de-Redirecionar para da configuração serve para autenticar a propriedade do nome de domínio.

Exemplo de configurações de redirecionamento HTTP

Nome de domínio	Redirecionar de	Redirecionar para	Comentário
exemplo.com	`http://example.com/.well-known/pki-validation/ x2.txt`	`https://validation. region.acm-validations.aws/ y2/.well-known/pki-validation/ x2.txt`	Exclusivo
www.exemplo.com	`http://www.example.com/.well-known/pki-validation/ x3.txt`	`https://validation. region.acm-validations.aws/ y3/.well-known/pki-validation/ x3.txt`	Exclusivo

Nome de domínio	Redirecionar de	Redirecionar para	Comentário
host.exemplo.com	`http://host.example.com/.well-known/pki-validation/ x4.txt`	`https://validation. region.acm-validations.aws/ y4/.well-known/pki-validation/ x4.txt`	Exclusivo
subdomínio.exemplo.com	`http://subdomain.example.com/.well-known/pki-validation/ x5.txt`	`https://validation. region.acm-validations.aws/ y5/.well-known/pki-validation/ x5.txt`	Exclusivo
host.subdomínio.exemplo.com	`http://host.subdomain.example.com/.well-known/pki-validation/ x6.txt`	`https://validation. region.acm-validations.aws/ y6/.well-known/pki-validation/ x6.txt`	Exclusivo

Os valores *xN* nos nomes dos arquivos e os valores *yN* nos domínios controlados pelo ACM são identificadores exclusivos gerados pelo ACM. Por exemplo,

```
http://example.com/.well-known/pki-validation/3639ac514e785e898d2646601fa951d5.txt
```

representa um URL Redirecionar de gerado. O URL Redirecionar para associado pode ser

```
https://validation.region.acm-validations.aws/98d2646601fa/.well-known/pki-
validation/3639ac514e785e898d2646601fa951d5.txt
```

para o mesmo registro de validação.

> **Note**
>
> Se seu servidor web ou rede de distribuição de conteúdo não oferecer suporte para a configuração de redirecionamentos no caminho especificado, consulte Solucionar problemas de validação por HTTP.

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

Nome do domínio	Redirecionar para
exemplo.com	https://validation.*region*.acm-validations.aws/*a424c7224e9b* /.well-known/pki-validation/*a79865eb4cd1a6ab990a45779b4e0b96* .txt

O nome do domínio é o FQDN associado ao certificado. Redirecionar de é o URL do seu domínio em que o ACM buscará o arquivo de validação. Redirecionar para é o URL controlado pelo ACM no qual o arquivo de validação real está hospedado.

Configure seu servidor web ou distribuição do CloudFront para redirecionar solicitações do URL Redirecionar de para o URL Redirecionar para. O método exato para configurar esse redirecionamento depende do software do seu servidor web ou da configuração do CloudFront.

Configure corretamente o redirecionamento para permitir que o ACM valide a propriedade do seu domínio e emita ou renove seu certificado.

Configuração da validação por HTTP

O ACM usa a validação por HTTP para verificar a propriedade do seu domínio quando emite certificados SSL/TLS públicos para uso com o CloudFront. Esta seção descreve como configurar um certificado público para usar a validação por HTTP.

Para configurar a validação por HTTP no console

> **Note**
>
> Este procedimento pressupõe que você já tenha solicitado um certificado pelo CloudFront e que esteja trabalhando na região da AWS onde o criou. A validação por HTTP está disponível somente por meio do atributo CloudFront Distribution Tenants.

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 Domínios, você pode ver os valores Redirecionar de e Redirecionar para de cada domínio em sua solicitação de certificado.
4. Para cada domínio, configure um redirecionamento HTTP do URL Redirecionar de para o URL Redirecionar para. Você pode fazer isso por meio da configuração de distribuição do CloudFront.
5. Configure sua distribuição do CloudFront para redirecionar solicitações do URL Redirecionar de para o URL Redirecionar para. O método para configurar esse redirecionamento depende da configuração do CloudFront.
6. Depois que os redirecionamentos forem configurados, o ACM tentará validar automaticamente a propriedade do seu domínio. Esse processo pode demorar até 30 minutos.

Se o ACM não puder validar o nome do domínio em até 72 horas a partir do momento em que gera um valor de redirecionamento para você, o ACM altera o status do certificado para Prazo de validação esgotado. O motivo mais provável para esse resultado é que os redirecionamentos HTTP não tenham sido configurados. Para corrigir esse problema, você deve solicitar um novo certificado após revisar as instruções de redirecionamento.

Important

Para evitar problemas de validação, assegure que o conteúdo no local Redirecionar de corresponda ao conteúdo no local Redirecionar para. Se você tiver problemas, consulte Solução de problemas de validação por HTTP.

Note

Ao contrário da validação por DNS, você não pode solicitar de forma programática que o ACM crie automaticamente seus redirecionamentos HTTP. Esses redirecionamentos precisam ser configurados por meio das configurações de distribuição do CloudFront.

Para obter mais informações sobre como a validação por HTTP funciona, consulte Como funcionam os redirecionamentos HTTP para o ACM.

Certificados privados no AWS Certificate Manager

Se você tiver acesso a uma CA privada existente criada pela CA privada da AWS, o AWS Certificate Manager (ACM) poderá solicitar um certificado adequado para uso em sua infraestrutura de chave privada (PKI). 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. Consequentemente, 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 obter 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.

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

Tópicos

Condições de uso do CA Privada da AWS para assinar certificados privados do ACM

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

- Conta única: a CA signatária e o certificado do AWS Certificate Manager (ACM) que é emitido residem na mesma conta da AWS.

  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 por meio da ação CreatePermission da API CA privada da AWS ou via comando create-permission da AWS CLI. O proprietário da conta atribui essas permissões a um usuário, grupo ou perfil do IAM responsável pela emissão dos certificados.
- Intercontas: a AC signatária e o certificado do ACM que é emitido residem em contas diferentes da AWS e o acesso à CA foi concedido à conta onde o certificado reside.

  Para habilitar a emissão e as renovações entre contas, o administrador da CA privada da AWS deve anexar uma política baseada em recursos à CA usando a ação PutPolicy da API CA privada da AWS ou o comando put-policy da 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 do ACM deve ser ativamente associado a um serviço da AWS suportado para que possa ser renovado automaticamente. Para obter informações sobre os recursos que o ACM suporta, consulte Serviços integrados ao ACM.

Solicitar um certificado privado no AWS Certificate Manager

Solicitar um certificado privado (console)

1. Faça login no Console de Gerenciamento da AWS 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 Detalhes da autoridade de certificação, selecione o menu 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 vaziou 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 Assunto e na extensão 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 algoritmo.

   Para obter informações que possam ajudar você a escolher um algoritmo, consulte a publicação no blog da AWS Como avaliar e usar certificados ECDSA no AWS Certificate Manager.

6. Na seção Tags (Etiquetas), é possível marcar seu certificado opcionalmente. As tags são pares chave-valor que servem como metadados para identificar e organizar recursos da AWS. Para obter uma lista de parâmetros de tag do ACM e instruções sobre como adicionar tags a certificados após a criação, consulte Marcar recursos 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 privado (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 da CA Privada da AWS, a família especificada de algoritmos de assinatura (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":"AAAAAAA0000000BBBBBBB",
      "Arn":"arn:aws:iam::{account_no}:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager",
      "CreateDate":"2020-08-01T23:10:41Z",
      "AssumeRolePolicyDocument":{
         "Version":"2012-10-17",
         "Statement":[
            {
               "Effect":"Allow",
               "Principal":{
                  "Service":"acm.amazonaws.com"
               },
               "Action":"sts:AssumeRole"
            }
         ]
      },
      "Description":"SLR for ACM Service for accessing cross-account Private CA",
      "MaxSessionDuration":3600,
      "RoleLastUsed":{
         "LastUsedDate":"2020-08-01T23:11:04Z",
         "Region":"ap-southeast-1"
      }
   }
}
```

Se a SLR estiver ausente, consulte Uso de uma função vinculada ao serviço com o ACM.

Exportar um certificado privado do AWS Certificate Manager

É possível exportar um certificado emitido pelo CA privada da AWS para uso em qualquer lugar do seu ambiente PKI privado. 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 o CA privada da AWS, consulte o Guia do usuário do Autoridade de Certificação Privada da AWS.

> **Note**
>
> Não é possível exportar um certificado publicamente confiável nem sua chave privada, independentemente de ele ter sido emitido pelo ACM ou ser importado.

Tópicos

Exportar um certificado privado (console)

1. Faça login no Console de Gerenciamento da AWS 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.

```
[Windows/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)"'
```

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-----
MIIDTDCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwWOdLOkxpwkkKWtcEkQuHE1v5Vn6HpbfFmxkdPEasoDhthH
FFWIf4/+VOlbDLgjU4HgtmV4IJDtqM9rGOZ42eFYmmc3eQO0GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmannS8j6YxmtpPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
```

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

Para gerar a saída de tudo para um arquivo, acrescente o redirecionamento > 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
```

Importar certificados para AWS Certificate Manager

Além de solicitar SSL/TLS certificados 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 obter 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 os balanceadores de carga elásticos do Elastic Load Balancing em diferentes regiões da AWS , 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 obter mais informações, consulte Regiões do 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 do ACM
- Formato de chaves e certificados para importação

- Importar um certificado
- Reimportar um certificado

Pré-requisitos para importação de certificados do ACM

Para importar um SSL/TLS certificado autoassinado para o ACM, você deve fornecer o certificado e sua chave privada. Para importar um certificado assinado por uma autoridade não certificadora (CA) da AWS , 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 as chaves RSA de 1024 bits, RSA de 2048 bits, RSA de 3072 bits, RSA de 4096 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.
- Um 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 renova (reimporta) um certificado, não é possível adicionar uma extensão `KeyUsage` ou `ExtendedKeyUsage` se a extensão não estiver presente no certificado importado anteriormente.

  Exceção: você pode reimportar um certificado sem a Autenticação do Cliente ExtendedKeyUsage em comparação com o certificado anterior. Isso acomoda as mudanças do setor em que as autoridades de certificação não emitem mais certificados com o ClientAuth EKU para cumprir os requisitos do programa raiz do Chrome.

  > **Important**
  >
  > Se a funcionalidade de autenticação de cliente for necessária, validações adicionais precisarão ser implementadas, pois o ACM não oferece suporte à reversão para os certificados importados 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 PRIVATE KEY-----
Base64-encoded private key
-----END 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-----
```

Importar 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 Console de gerenciamento da AWS AWS CLI, a ou a ACM. Os tópicos a seguir mostram como usar o Console de gerenciamento da AWS e AWS CLI o. Os procedimentos para obter um certificado de um não AWS emissor estão fora do escopo deste guia.

> **Important**
>
> O algoritmo de assinatura selecionado deve atender aos Pré-requisitos para importação de certificados do ACM.

Tópicos

Importar (console)

O exemplo a seguir mostra como importar um certificado usando o Console de gerenciamento da AWS.

1. Abra o console do ACM em https://console.aws.amazon.com/acm/casa. 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 descriptografada 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. (Opcional) Para adicionar tags ao seu certificado importado, escolha Tags. Uma tag um rótulo atribuído a um recurso AWS . Cada tag consiste em uma chave e um valor opcional, ambos definidos por você. Você pode usar tags para organizar seus recursos ou monitorar seus custos na AWS .
5. Escolha 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.

Reimportar 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, consulteServiços integrados ao ACM.

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.

  Exceção: é possível remover o ClientAuth EKU. Isso acomoda as mudanças do setor em que as autoridades de certificação não emitem mais certificados com o ClientAuth EKU para cumprir os requisitos do programa raiz do Chrome.

  > **Important**
  >
  > Se a funcionalidade de autenticação de cliente for necessária, validações adicionais precisarão ser implementadas, pois o ACM não oferece suporte à reversão para os certificados importados anteriormente.

- 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)

O exemplo a seguir mostra como reimportar um certificado usando o Console de gerenciamento da AWS.

1. Abra o console do ACM em https://console.aws.amazon.com/acm/casa.
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. 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.

Gerenciamento de certificado

Você pode usar o console do ACM ou o AWS CLI para gerenciar os certificados em sua conta.

- Listar certificados para ver os certificados gerenciados pelo ACM. A lista mostra informações resumidas sobre cada certificado.
- Visualizar detalhes do certificado do para visualizar os detalhes de um certificado individual.
- Excluir certificados para removê-los da sua conta. Os certificados excluídos podem aparecer nas listas por um curto período após a exclusão.

Listar certificados gerenciados por AWS Certificate Manager

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 ELB ou. CloudFront 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: Elegible (Elegível) | Inelegible (Inelegível). Para visualizar as regras de qualificação, consulte Renovação gerenciada do certificado em AWS Certificate Manager.

Ao selecionar o ícone de configurações no canto superior direito do console, é possível personalizar o número de certificados mostrados 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 Exibir detalhes do AWS Certificate Manager certificado.

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
```

Exibir detalhes do AWS Certificate Manager certificado

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 AWS Certificate Manager certificados públicos, Solicitar um certificado privado no AWS Certificate Manager ou Importar 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.
- Gerenciado por – Identifica o serviço da AWS que gerencia o certificado com o ACM.
- 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 do certificado em AWS Certificate Manager.
- 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/E12KXPQHVLSYVC"
        ],
```

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

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

Excluir certificados gerenciados por AWS Certificate Manager

Você pode usar o console do ACM ou o AWS CLI para excluir um certificado. A exclusão de um tíquete é consistente. O certificado pode aparecer nas listas por um curto período após a exclusão.

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 Autoridade de Certificação Privada da AWS .

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
```

Renovação gerenciada do certificado em AWS Certificate Manager

O ACM fornece renovação gerenciada para seus certificados emitidos pela Amazon SSL/TLS . 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 ELB ou CloudFront.
- ELEGÍVEL se exportado desde a sua emissão ou da última renovação.
- ELEGÍVEL se for um certificado privado emitido por uma chamada da API RequestCertificate do ACM e depois exportado ou associado a outro serviço da AWS .
- 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	Satisfazo n.º 1	Satisfazo n.º 2	Permit	Observação
exemplo.com	n/a	n/a	✓	Não começa com “<character><character>--”
a--example.com	n/a	n/a	✓	Não começa com “<character><character>--”
abc--example.com	n/a	n/a	✓	Não começa com “<character><character>--”
xn--xyz.com	Sim	Sim	✓	Nome de domínio internacionalizado válido (é resolvido para 简.com)
xn--example.com	Sim	Não	✗	Não é um nome de domínio internacionalizado válido
ab--example.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

- Renovar certificados públicos do ACM
- Renovação de certificado privado em AWS Certificate Manager
- Verificar o status de renovação de um certificado

Renovar certificados públicos do ACM

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

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 se não puder validar automaticamente um domínio durante a renovação. Esses eventos são enviados 45 dias, 30 dias, 15 dias, 7 dias, 3 dias e 1 dia antes da expiração da validade. Para obter 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). A renovação de um certificado exige uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação para os endereços de e-mail associados ao domínio 45 dias antes da expiração. As notificações contêm

um link no qual o proprietário do domínio pode clicar para renová-lo. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

O ACM envia AWS Health eventos e EventBridge eventos da Amazon se não puder validar automaticamente um domínio durante a renovação. Esses eventos são enviados 45 dias, 30 dias, 15 dias, 7 dias, 3 dias e 1 dia antes da expiração da validade. Para obter mais informações, consulte EventBridge Suporte da Amazon para ACM.

Para obter mais informações sobre mensagens de validação por e-mail, consulte Validação de e-mail do AWS Certificate Manager

Para saber como é possível responder de forma programática ao e-mail de validação, consulte Automatizar a validação por e-mail do AWS Certificate Manager.

Reenviar o e-mail de validação

Depois de configurar a validação de e-mail para seu domínio ao solicitar um certificado (consulteValidação de e-mail do AWS Certificate Manager), você pode usar a AWS Certificate Manager API para solicitar que o ACM lhe 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 enviar e-mails de validação para um domínio diferente do que você configurou originalmente em sua solicitação de certificado, você pode usar a ResendValidationEmailoperação na API do ACM AWS CLI, ou AWS SDKs. O ACM enviará e-mails para o domínio de validação especificado. Você pode acessar o AWS CLI navegador usando as AWS CloudShell regiões suportadas.

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/casa.
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 ResendValidationEmailoperação 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 subdomain.example.com \
 --validation-domain example.com
```

Renovação de domínios validados por HTTP

O ACM fornece renovação gerenciada automatizada para certificados que foram originalmente emitidos usando a validação HTTP por meio CloudFront de.

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

- O certificado está atualmente em uso por CloudFront.
- Todos os registros de validação por HTTP necessários estão acessíveis e contêm o conteúdo esperado.

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 se não puder validar automaticamente um domínio durante a renovação. Esses eventos são enviados 45 dias, 30 dias, 15 dias, 7 dias, 3 dias e 1 dia antes da expiração da validade. Para obter mais informações, consulte EventBridge Suporte da Amazon para ACM.

Para garantir a renovação, assegure que o conteúdo no local `RedirectFrom` corresponda ao conteúdo no local `RedirectTo` em relação a cada domínio no certificado.

Renovação de certificado privado em AWS Certificate Manager

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 ação RequestCertificate da API do ACM são elegíveis para renovação gerenciada. Os certificados emitidos diretamente pelo CA privada da AWS uso da IssueCertificateação 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 ação 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 Lambdaseguinte forma. Para obter mais informações, consulte Automatizar a exportação de certificados renovados.

Automatizar a 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 ExportCertificateação da API do ACM.

JSON

```
{
   "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.

Testar a renovação gerenciada de certificados PKI privados

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**
>
> É possível testar somente 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 RenewCertificatesolicitação, especificando o ARN do certificado privado a ser renovado. Em seguida, use a DescribeCertificateoperação 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 obter 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 neo 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.

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 ELB 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 Solucionar problemas de solicitações de certificado.

Tópicos

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/casa.
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 DescribeCertificateação para verificar o status, consulteDescrição 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 AWS Health Guia do usuário do .

> **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 no 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.

Marcar recursos 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 tag

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 valores das 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 Console de gerenciamento da AWS.

Para obter informações gerais sobre convenções de marcação da AWS, consulte Marcação de recursos da AWS.

Como 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 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 Console de gerenciamento da AWS 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

Serviços integrados ao ACM

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**
>
> Os certificados públicos do ACM podem ser instalados em EC2 instâncias da Amazon conectadas a um Nitro Enclave. Você também pode exportar um certificado público para usar em qualquer EC2 instância da Amazon. Para obter informações sobre como configurar um servidor web autônomo em uma EC2 instância da Amazon 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:

ELB

O ELB distribui automaticamente o tráfego de entrada do seu aplicativo em várias instâncias da 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 ELB dimensiona automaticamente sua capacidade de tratamento 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 fornecer conteúdo seguro por meio de SSL/TLS, load balancers require that SSL/TLS certificados, ele deve ser instalado no balanceador de carga ou na instância back-end da Amazon EC2. O ACM é integrado ao ELB para implantar certificados do ACM no 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 por meio de SSL/TLS, CloudFront requires that SSL/TLS certificados, seja instalado 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 SSL/TLS certificado.

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

Amazon Elastic Kubernetes Service

O Amazon Elastic Kubernetes Service é um serviço gerenciado do Kubernetes que facilita a execução do Kubernetes sem a necessidade de instalar, operar e manter seu próprio plano de controle do Kubernetes AWS . Para obter mais informações sobre o Amazon EKS, consulte o Guia do usuário do Amazon Elastic Kubernetes Service.

Você pode usar o ACM com AWS Controllers for Kubernetes (ACK) para emitir e exportar certificados TLS para suas cargas de trabalho do Kubernetes. Essa integração permite que você proteja os pods do Amazon EKS e encerre o TLS em seu Kubernetes Ingress ou em um balanceador de carga. AWS O ACM renova automaticamente os certificados e o controlador ACK atualiza seus segredos do Kubernetes com certificados renovados. Para obter mais informações, consulte Proteja cargas de trabalho do Kubernetes com certificados ACM.

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 APIs criar dispositivos que possam ser usados para acessar dados e interagir com sistemas de back-end. AWS Você pode usar o API Gateway para publicar, manter,

monitorar e proteger seu 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 EC2 recurso da Amazon que permite criar ambientes de execução isolados, chamados enclaves, a partir de instâncias da 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).

EC2 instâncias conectadas ao Nitro Enclaves oferecem suporte a certificados ACM. Para obter mais informações, consulte AWS Certificate Manager para Nitro Enclaves.

> **Note**
>
> Você não pode associar certificados do ACM a uma EC2 instância que não esteja conectada a um Nitro Enclave.

AWS CloudFormation

CloudFormation ajuda você a modelar e configurar seus recursos da Amazon Web Services. Você cria um modelo que descreve os AWS recursos que você deseja usar, como ELB ou API Gateway. Em seguida, o 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; CloudFormation lida com tudo isso. Os certificados ACM são incluídos como um recurso de modelo, o que significa que 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. CloudFormation

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

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

> **Note**
>
> Se você criar um certificado ACM com CloudFormation, a 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 full-stack sem servidor com implantação contínua. O Amplify Studio é um ambiente de desenvolvimento visual que simplifica a criação de aplicações Web e móveis full-stack e escaláveis. 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. Se você usar a inspeção TLS no Firewall de Rede, deverá configurar um certificado ACM para a descriptografia e recriptografia do tráfego que passa pelo SSL/TLS firewall. Para obter informações sobre como o Network Firewall funciona com o ACM para inspeção de TLS, consulte Requisitos para usar SSL/TLS certificados com configurações de inspeção de TLS no Guia do Desenvolvedor.AWS Network Firewall

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

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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD 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 AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- 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 sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags 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 AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Segurança para chaves privadas de certificados

Quando você solicita um certificado público, o AWS Certificate Manager (ACM) gera um par de public/private chaves. 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 ao ACM.

   > **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 AWS Certificate Manager

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. 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 você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões do administrador se você não conseguir acessar atributos (consulte Solução de problemas AWS Certificate Manager de identidade e acesso).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como AWS Certificate Manager funciona com o IAM)
- Administrador do IAM: grave políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para AWS Certificate Manager).

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como AWS IAM Identity Center (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Para ver as tarefas que exigem credenciais de usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem perfis que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos AWS IAM Identity Center. Para obter mais informações, consulte O que é o IAM Identity Center? no Guia do usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com

um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para obter mais informações, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

As funções do IAM são úteis para acesso de usuários federados, permissões temporárias de usuários do IAM, acesso entre contas, acesso entre serviços e aplicativos executados na Amazon. EC2 Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Usando políticas, os administradores especificam quem tem acesso ao quê definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona a funções, que os usuários podem acabar assumindo. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de política de permissões JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma

política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente a uma única identidade) ou políticas gerenciadas (políticas independentes anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para obter mais informações, consulte Limites de permissões para entidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para obter mais informações, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas passadas como um parâmetro durante a criação de uma sessão temporária para uma função ou um usuário federado. 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. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como 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 AWS Certificate Manager

Recurso do IAM	Compatível com o ACM
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Sim

Para ter uma visão de alto nível de como o ACM e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para o ACM

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento 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 AWS Certificate Manager.

Políticas baseadas em recursos no ACM

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas para o ACM

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 podem ser usadas para permitir ou negar acesso em uma política. 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 declaração, 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 AWS Certificate Manager.

Recursos de políticas para o ACM

Compatível com recursos de políticas: sim

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

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não deem suporte a permissões no nível do recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do ACM e seus ARNs, consulte Recursos definidos por AWS Certificate Manager na Referência de Autorização de 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 AWS Certificate Manager.

Chaves de condição de políticas para o ACM

Compatível com chaves de condição de política específicas de serviço: sim

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

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global 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 você pode usar uma chave de condição, consulte Ações definidas por AWS Certificate Manager.

Para visualizar exemplos de políticas baseadas em identidade do ACM, consulte Exemplos de políticas baseadas em identidade para AWS Certificate Manager.

ACLs em ACM

Suportes ACLs: Não

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

ABAC com ACM

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

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

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. 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 e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões de entidade principal entre serviços para o ACM

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Perfis de serviço do ACM

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar 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

Compatibilidade com perfis vinculados a serviços: sim

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

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS Certificate Manager

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do ACM. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ACM, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Certificate Manager na Referência de Autorização de Serviço. ARNs

Tópicos

Práticas recomendadas de política

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 sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS 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.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando

SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS 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 Configuração de 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 AWS Certificate Manager console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do ACM em seu 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 perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do ACM, anexe também a política `AWSCertificateManagerReadOnly` AWS gerenciada do ACM às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os 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 programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Lista de certificados

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

JSON

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

> **Note**
>
> Essa permissão é necessária para que os certificados ACM apareçam no ELB e CloudFront nos consoles.

Solicitar um certificado

A política a seguir impede que um usuário solicite certificados públicos exportáveis do ACM.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenyACMCertificateRequest",
      "Effect": "Deny",
      "Action": [
        "acm:RequestCertificate"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "acm:Export": "ENABLED"
        }
      }
    }
  ]
}
```

Recuperação de um certificado

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

JSON

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

Importação de um certificado

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

JSON

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

Exclusão de um certificado

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "acm:DeleteCertificate",
        "Resource": "arn:aws:acm:us-
east-1:123456789012: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 AWS Certificate Manager da API. 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
AddTagsToCertificate	acm:AddTagsToCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
DeleteCertificate	acm:DeleteCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
DescribeCertificate	acm:DescribeCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
ExportCertificate	acm:ExportCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
GetAccountConfiguration	acm:GetAccountConfiguration	*
GetCertificate	acm:GetCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
ImportCertificate	acm:ImportCertificate	arn:aws:acm: *region*:*account*:certificate/* or *
ListCertificates	acm:ListCertificates	*

Operações de API do ACM	Permissões obrigatórias (operações de API)	Recursos
ListTagsForCertificate	acm:ListTagsForCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
PutAccountConfiguration	acm:PutAccountConfiguration	*
RemoveTagsFromCertificate	acm:RemoveTagsFromCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
RequestCertificate	acm:RequestCertificate	arn:aws:acm: *region*:*account*:certificate/* or *
ResendValidationEmail	acm:ResendValidationEmail	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
UpdateCertificateOptions	acm:UpdateCertificateOptions	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*

AWS políticas gerenciadas para AWS Certificate Manager

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia 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.

Para ver essa política AWS gerenciada no console, acesse https://console.aws.amazon.com/iam/home# policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly.

Para obter uma lista JSON dos detalhes da política, consulte AWSCertificateManagerReadOnly.

AWSCertificateManagerFullAccess

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

Para ver essa política AWS gerenciada no console, acesse https://console.aws.amazon.com/iam/home# policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess.

Para obter uma lista JSON dos detalhes da política, consulte AWSCertificateManagerFullAccess.

Atualizações do ACM nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do 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
Adição de suporte`GetAccountConfiguration` à política AWSCertificateManagerReadOnly.	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 começa a rastrear as alterações nas políticas AWS gerenciadas.	3 de março de 2021

Usar chaves de condição com o ACM

AWS Certificate Manager usa chaves de condição AWS Identity and Access Management (IAM) para limitar o acesso às solicitações de certificado. 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 as chaves de condição AWS globais, `aws:PrincipalArn` para restringir ainda mais as ações a usuários ou funções específicos.

Condições compatíveis com o ACM

Operações da API do ACM e condições compatíveis

Chave de condição	Operações da API do ACM compatíveis	Tipo	Description
`acm:ValidationMethod`	RequestCertificate	Cadeia de caracteres (`DNSEMAIL`,,`HTTP`)	Filtrar solicitações com base no método de validação do ACM

Chave de condição	Operações da API do ACM compatíveis	Tipo	Description
`acm:DomainNames`	RequestCertificate	ArrayOfString	Filtro baseado em nomes de domínio na solicitação do ACM
`acm:KeyAlgorithm`	RequestCertificate	String	Filtrar solicitações com base no algoritmo e no tamanho da chave do ACM
`acm:CertificateTransparencyLogging`	RequestCertificate	String (`ENABLED`, `DISABLED`)	Filtrar solicitações com base na preferência do log de transparência de certificados do ACM
`acm:CertificateAuthority`	RequestCertificate	ARN	Filtrar solicitações com base nas autoridades de certificação 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`.

JSON

```
{
    "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.

JSON

```
{
    "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`

JSON

```
{
    "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.

JSON

```
{
    "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`).

JSON

```
{
    "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.

JSON

```
{
    "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.

JSON

```
{
    "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.

JSON

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

Uso de perfis vinculados 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 privados emitidos por uma CA privada para outra conta compartilhada por. AWS Resource Access Manager Uma função vinculada ao serviço (SLR) é uma função do IAM vinculada diretamente ao serviço do ACM. SLRs são predefinidos pelo ACM e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

A SLR facilita a configuração do ACM porque você não precise 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 compatíveis SLRs, consulte AWS Serviços que funcionam com o IAM e procure os serviços que têm Sim na coluna 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 AWSService RoleForCertificateManager 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 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 Console de gerenciamento da AWS AWS CLI, a ou a AWS API, o ACM cria a SLR para você na primeira vez em que você assina seu certificado como CA privada de outra conta compartilhada AWS RAM .

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 obter 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 SLRs, o ACM criou a AWSService RoleForCertificateManager função em sua conta. Para saber mais, consulte A 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 CreateServiceLinkedRoleou 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 AWSService RoleForCertificateManager serviço. Depois que criar uma SLR, você não pode alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, você poderá editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo a SLR para o ACM

Normalmente, você não precisa excluir a AWSService RoleForCertificateManager 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 pelo ACM SLRs

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

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 (N. da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
Ásia-Pacífico (Mumbai)	ap-south-1	Sim
Ásia Pacifico (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 AWS Certificate Manager de identidade e acesso

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

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 atributo *`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 precisar de ajuda, entre em contato com seu AWS administrador. 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::account::ID: is not authorized to perform: acm:RequestCertificate
```

```
on resource: arn:aws:acm:region:account:certificate/*
with an explicit deny in a service control policy
```

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 realizar 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 esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso 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 precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

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

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o ACM oferece suporte a esses recursos, consulte Como AWS Certificate Manager funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Resiliência em AWS Certificate Manager

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS 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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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 compatibilidade com:

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

Conceder permissões de acesso programático ao ACM

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do Console de gerenciamento da AWS. 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
IAM	(Recomendado) Use as credenciais do console como credenciais temporárias para assinar solicitações programáticas para o AWS CLI,, AWS SDKs ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Login para desenvolvimento AWS local no Guia AWS Command Line Interface do usuário. • Para AWS SDKs isso, consulte Login para desenvolvimento AWS local no Guia de referência de ferramentas AWS SDKs e ferramentas.
Identidade da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity

Qual usuário precisa de acesso programático?	Para	Por
		Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de ferramentas AWS SDKs e ferramentas.
IAM	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.

Qual usuário precisa de acesso programático?	Para	Por
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

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

- Separação em nível de conta
- AWS CloudFormation
- Armazenamentos confiáveis personalizados

- 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

Separação em nível de conta

Use a separação em nível de conta em suas políticas para controlar quem pode acessar certificados em nível de conta. Mantenha seus certificados de produção em contas separadas dos certificados de teste e desenvolvimento. Se você não puder usar a separação em nível de conta, poderá restringir o acesso a funções específicas negando a ação `kms:CreateGrant` em suas políticas. Isso limita quais funções em uma conta podem assinar certificados em alto nível. Para obter informações sobre concessões, incluindo a terminologia relacionada, consulte Concessões no AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

Se você quiser um controle mais granular do que restringir o uso de `kms:CreateGrant` por conta, você pode limitar `kms:CreateGrant` a certificados específicos usando kms: EncryptionContext condition keys. Especifique `arn:aws:acm` como a chave e o valor do ARN a ser restringido. O exemplo de política a seguir impede o uso de um certificado específico, mas permite outros.

JSON

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

```
    ]
}
```

AWS CloudFormation

Com AWS CloudFormation você pode criar um modelo que descreva os AWS recursos que você deseja usar. CloudFormation em seguida, provisiona e configura esses recursos para você. CloudFormation pode provisionar recursos que são suportados pelo ACM, como Elastic Load Balancing, Amazon e CloudFront Amazon API Gateway. Para obter mais informações, consulte Serviços integrados ao ACM.

Se você costuma 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 obter 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 criar repetidamente certificados ACM para nomes de domínio que variam de acordo com apenas um número de versão, como, em vez disso `<version>.service.example.com`, crie um único certificado curinga para. `<*>.service.example.com`

> **Important**
>
> Se você estiver usando CloudFront distribuições da Amazon, observe que a validação HTTP não suporta certificados curinga. Ao incluir certificados curinga em seus CloudFormation modelos para uso com a Amazon CloudFront, você deve usar a validação de DNS ou a validação de e-mail. Recomendamos a validação por DNS para os recursos de renovação automática.

Inclua o certificado curinga no modelo CloudFormation usado para criar seu ambiente de teste.

Armazenamentos confiáveis personalizados

Para garantir a conectividade com os endpoints protegidos por certificados ACM, é recomendável que as raízes da Amazon sejam incluídas em seu armazenamento confiável personalizado. As autoridades de certificação do Amazon Root podem representar diferentes tipos de chaves e algoritmos. A Starfield Services Root Certificate Authority - G2 é uma raiz mais antiga que é

compatível com outros armazenamentos e clientes confiáveis mais antigos que não podem ser atualizados. Ao incluir todas as raízes CAs, você poderá garantir a máxima compatibilidade para seu aplicativo.

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. Portanto, o aplicativo usa a fixação para ignorar a validação da cadeia de SSL/TLS certificados. 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 renova automaticamente seus SSL/TLS certificados emitidos pela Amazon antes que eles Renovação gerenciada do certificado em AWS Certificate Manager expirem. 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 obter mais informações, consulte Validação de DNS do AWS Certificate Manager e Validação de e-mail do AWS Certificate Manager.

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.

A partir de 30 de abril de 2018, o Google Chrome não confia mais em SSL/TLS certificados públicos que não estão registrados em um registro 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 obter 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 vazar 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 RequestCertificateAPI. 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-optionscomando ou a operação da UpdateCertificateOptionsAPI 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-optionscomando. 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, do AWS SDKs, do e do Amazon AWS Command Line Interface Web Services de nível superior. Você também pode identificar quais usuários e contas ligaram para o ACM APIs, o endereço IP de origem a partir do qual as chamadas foram feitas e quando as chamadas 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.

Monitore e registre 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 de vários pontos, 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

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

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 PutAccountConfigurationação da API do ACM.

O ACM inicia automaticamente a renovação dos certificados elegíveis, mas os certificados importados precisam ser reemitidos e reimportados antes do término da validade 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, consulteIniciando 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 certificados expirados 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**
>
> Eventos de ação de renovação de certificado necessária 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
   }
}
```

Evento Certificado ACM revogado

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

> **Note**
>
> Somente os certificados exportados podem ser revogados. Os certificados importados não podem ser revogados por meio de revoke-certificate.

Os eventos Certificado ACM revogado têm a estrutura a seguir.

```
{
  "version": "0",
  "id": "id",
  "detail-type": "ACM Certificate Revoked",
  "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",
    "CertificateExpirationDate" : "2019-12-22T18:43:48Z",
    "Exportable": 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 do certificado em AWS Certificate Manager.

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"
      ]
   }
}
```

Iniciando 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 CSPM, 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 do 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.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LambdaCertificateExpiryPolicy1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "LambdaCertificateExpiryPolicy2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
```

```
                "arn:aws:logs:us-east-1:123456789012: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:::. *<region>* *<account-number>* *<topic-name>*
- (Opcional) SECURITY_HUB_REGION

  Especifica um AWS Security Hub CSPM 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, talvez seja desejável que todas as mensagens de certificado sejam enviadas para o CSPM do 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. (Este período pode ser personalizado usando a operação PutAccountConfiguration 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 CSPM
```

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. É possível visualizar, pesquisar e baixar eventos recentes em sua AWS conta.

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 o seguinte:

- 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 Elemento userIdentity do CloudTrail.

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 AddTagsToCertificateAPI.


```
{

   "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 DeleteCertificateAPI.

```
{

   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:26Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"DeleteCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
         },
         "responseElements":null,
         "requestID":"01234567-89ab-cdef-0123-456789abcdef",
         "eventID":"01234567-89ab-cdef-0123-456789abcdef",
```

```
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

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 especificado. 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 ExportCertificateAPI.

```
{
   "Records":[
      {
         "version":"0",
         "id":"01234567-89ab-cdef-0123-456789abcdef",
         "detail-type":"AWS API Call via CloudTrail",
         "source":"aws.acm",
         "account":"123456789012",
         "time":"2018-05-24T15:28:11Z",
         "region":"us-east-1",
         "resources":[

         ],
         "detail":{
            "eventVersion":"1.04",
            "userIdentity":{
               "type":"Root",
               "principalId":"123456789012",
               "arn":"arn:aws:iam::123456789012:user/Alice",
               "accountId":"123456789012",
               "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
               "userName":"Alice"
            },
            "eventTime":"2018-05-24T15:28:11Z",
            "eventSource":"acm.amazonaws.com",
            "eventName":"ExportCertificate",
            "awsRegion":"us-east-1",
            "sourceIPAddress":"192.0.2.0",
            "userAgent":"aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4",
            "requestParameters":{
              "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
               "passphrase": "HIDDEN_DUE_TO_SECURITY_REASONS"
```

```
            },
            "responseElements":{
                "certificateChain":
                "-----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----
                -----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----",
                "privateKey":"**********",
                "certificate":
                "-----BEGIN CERTIFICATE-----
                base64 certificate
                -----END CERTIFICATE-----",
                "privateKey": "HIDDEN_DUE_TO_SECURITY_REASONS"
            },
            "requestID":"01234567-89ab-cdef-0123-456789abcdef",
            "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
            "readOnly": false,
            "eventType":"AwsApiCall"
                "managementEvent": true,
                "recipientAccountId": "123456789012",
                "eventCategory": "Management",
                "tlsDetails": {
                     "tlsVersion": "TLSv1.3",
                     "cipherSuite": "TLS_AES_128_GCM_SHA256",
                     "clientProvidedHostHeader": "acm.us-east-1.amazonaws.com"
                 },
                 "sessionCredentialFromConsole": "true"
}
```

Importar um certificado (ImportCertificate)

O exemplo a seguir mostra a entrada de CloudTrail registro que registra uma chamada para a operação da ImportCertificateAPI 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":"cdfe1051-88aa-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 ListTagsForCertificateAPI.

> **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 ListTagsForCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-04-06T13:30:11Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ListTagsForCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.10.16",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
         },
         "responseElements":null,
         "requestID":"b010767f-fbfb-11e5-b596-79e9a97a2544",
         "eventID":"32181be6-a4a0-48d3-8014-c0d972b5163b",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Remoção das tags de um certificado (RemoveTagsFromCertificate)

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a RemoveTagsFromCertificateAPI.


```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
```

```
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-04-06T14:10:01Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"RemoveTagsFromCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.10.16",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
            "tags":[
               {
                  "value":"Bob",
                  "key":"Admin"
               }
            ]
         },
         "responseElements":null,
         "requestID":"40ded461-fc01-11e5-a747-85804766d6c9",
         "eventID":"0cfa142e-ef74-4b21-9515-47197780c424",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Solicitação de um certificado (RequestCertificate)

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a RequestCertificateAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
```

```
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:49Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"RequestCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "domainName":"example.com",
            "validationMethod": "DNS",
            "idempotencyToken":"8186023d89681c3ad5",
            "options": {
            "export": "ENABLED"
        },
        "keyAlgorithm": "RSA_2048"
         },
         "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",
         "tlsDetails": {
           "tlsVersion": "TLSv1.3",
           "cipherSuite": "TLS_AES_128_GCM_SHA256",
           "clientProvidedHostHeader": "acm.us-east-1.amazonaws.com"
          },
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Revogar um certificado (RevokeCertificate)

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a RevokeCertificateAPI.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:Role-Session-Name",
        "arn": arn:aws:sts::111122223333:assumed-role/Role-Name/Role-Session-Name",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2016-01-01T19:35:52Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime":"2016-01-01T21:11:45Z",
    "eventSource": "acm.amazonaws.com",
    "eventName": "RevokeCertificate",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
 Firefox/128.0",
    "requestParameters": {
        "certificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
        "revocationReason": "UNSPECIFIED"
    },
    "responseElements": {
        "certificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
    },
    "requestID": "01234567-89ab-cdef-0123-456789abcdef",
    "eventID": "01234567-89ab-cdef-0123-456789abcdef",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "acm.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Reenvio do e-mail de validação (ResendValidationEmail)

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a ResendValidationEmailAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-17T23:58:25Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ResendValidationEmail",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "domain":"example.com",
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
            "validationDomain":"example.com"
         },
         "responseElements":null,
         "requestID":"23760b88-ec9c-11e5-b6f4-cb861a6f0a28",
         "eventID":"41c11b06-ca91-4c1c-8c61-af349ea8bab8",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Recuperação de um certificado (GetCertificate)

O CloudTrail exemplo a seguir mostra os resultados de uma chamada para a GetCertificateAPI.


```
{

   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:41Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"GetCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
         },
         "responseElements":{
            "certificateChain":

            "-----BEGIN CERTIFICATE-----
            Base64-encoded certificate chain
            -----END CERTIFICATE-----",
            "certificate":
            "-----BEGIN CERTIFICATE-----
            Base64-encoded certificate
            -----END CERTIFICATE-----"

         },
         "requestID":"744dd891-ec9c-11e5-ac34-d1e4dfe1a11b",
         "eventID":"7aa4f909-00dd-478a-9a00-b2709bcad2bb",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
```

```
    ]
}
```

Registro 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 EC2 instância da Amazon com um Load Balancer
- 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 EC2 instância da Amazon com um Load Balancer

Quando você provisiona seu site ou aplicativo em uma instância do Amazon Elastic Compute Cloud (Amazon EC2), o balanceador de carga deve estar ciente dessa instância. Isso pode ser feito por meio do console ELB ou do. 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 duas vezes por dia para cada certificado em uma conta até a expiração.

O namespace `AWS/CertificateManager` inclui as métricas a seguir.

Métrica	Description	Unidade	Dimensões
`DaysToExpiry`	Número de dias até que a validade de um certificado expire. O ACM interrompe a publicação dessa métrica depois que um certificado expira.	Inteiro	CertificateArn • Valor: ARN do certificado

Para obter mais informações sobre CloudWatch métricas, consulte os tópicos a seguir:

- Usando o Amazon CloudWatch Metrics
- Criação de CloudWatch alarmes da Amazon

Usar AWS Certificate Manager com o SDK para 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 para Java, para executar algumas das operações disponíveis na API do AWS Certificate Manager.

Tópicos

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: FriOct0608: 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 = 120000l;
      long timeSlept = 0l;
      long sleepInterval = 10000l;
      while (result == null && timeSlept < totalTimeout) {
```

```
         try {
            result = client.getCertificate(req);
         }
         catch (RequestInProgressException ex) {
            Thread.sleep(sleepInterval);
         }
         catch (ResourceNotFoundException ex)
         {
            throw ex;
         }
         catch (InvalidArnException ex)
         {
            throw ex;
         }

         timeSlept += sleepInterval;
      }

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

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:
 *   CertificcateArn - The ARN of the imported certificate.
 *
 */
public class AWSCertificateManagerSample {

   public static void main(String[] args) throws Exception {

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials file in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
```

```
        catch (Exception ex) {
            throw new AmazonClientException(
                "Cannot load the credentials from file.", ex);
        }

        // Create a client.
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()
                .withRegion(Regions.US_EAST_1)
                .withCredentials(new AWSStaticCredentialsProvider(credentials))
                .build();

        // Initialize the file descriptors.
        RandomAccessFile file_certificate = null;
        RandomAccessFile file_chain = null;
        RandomAccessFile file_key = null;

        // Initialize the buffers.
        ByteBuffer buf_certificate = null;
        ByteBuffer buf_chain = null;
        ByteBuffer buf_key = null;

        // Create the file streams for reading.
        try {
           file_certificate = new RandomAccessFile("C:\\Temp\\certificate.pem", "r");
           file_chain = new RandomAccessFile("C:\\Temp\\chain.pem", "r");
           file_key = new RandomAccessFile("C:\\Temp\\private_key.pem", "r");
        }
        catch (IllegalArgumentException ex) {
           throw ex;
        }
        catch (SecurityException ex) {
           throw ex;
        }
        catch (FileNotFoundException ex) {
           throw ex;
        }

        // Create channels for mapping the files.
        FileChannel channel_certificate = file_certificate.getChannel();
        FileChannel channel_chain = file_chain.getChannel();
        FileChannel channel_key = file_key.getChannel();

        // Map the files to buffers.
        try {
```

```
        buf_certificate = channel_certificate.map(FileChannel.MapMode.READ_ONLY, 0,
channel_certificate.size());
        buf_chain = channel_chain.map(FileChannel.MapMode.READ_ONLY, 0,
channel_chain.size());
        buf_key = channel_key.map(FileChannel.MapMode.READ_ONLY, 0,
channel_key.size());

        // The files have been mapped, so clean up.
        channel_certificate.close();
        channel_chain.close();
        channel_key.close();
        file_certificate.close();
        file_chain.close();
        file_key.close();
     }
     catch (IOException ex)
     {
        throw ex;
     }

     // Create a request object and set the parameters.
     ImportCertificateRequest req = new ImportCertificateRequest();
     req.setCertificate(buf_certificate);
     req.setCertificateChain(buf_chain);
     req.setPrivateKey(buf_key);

     // Import the certificate.
     ImportCertificateResult result = null;
     try {
        result = client.importCertificate(req);
     }
     catch(LimitExceededException ex)
     {
        throw ex;
     }
     catch (ResourceNotFoundException ex)
     {
        throw ex;
     }

     // Clear the buffers.
     buf_certificate.clear();
     buf_chain.clear();
     buf_key.clear();
```

```
      // Retrieve and display the certificate ARN.
      String arn = result.getCertificateArn();
      System.out.println(arn);
    }
}
```

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.

Solucionar problemas com o AWS Certificate Manager

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

Solucionar 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

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 ter mais informações, consulte Validação de DNS do AWS Certificate Manager ou Validação de e-mail do AWS Certificate Manager. 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)

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 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 Validação de e-mail do AWS Certificate Manager 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 Suporte. 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 Suporte. Se você não tem um plano de suporte, publique um novo thread no Fórum de discussão do ACM.

Solucionar problemas de validação de certificados

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 para os endereços de e-mail comuns para o domínio solicitado. Para obter mais informações, consulte Validação de e-mail do AWS Certificate Manager. 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 obter mais informações, consulte Validação de DNS do AWS Certificate Manager.

> **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. Você também pode exportar um certificado público para usar em qualquer instância 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 em caso de problemas de validação.

Tópicos

- Solucionar os problemas de validação por DNS
- Solução de problemas de validação de e-mail
- Solução de problemas de validação por HTTP

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

Tópicos

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.

Name	Tipo	Valor
`_<random value>.example.com.`	CNAME	`_<random value>.acm-validations.aws.`
`_<random value>.example.com.`	CNAME	`<random value>.acm-validations.aws.`

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.

Falha na validação de DNS no 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:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

É possível criar um registro CNAME compatível com o GoDaddy truncando o domínio apex (incluindo o ponto) no final do campo NAME, da seguinte forma:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.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, o AWS Certificate Manager poderá interagir diretamente com ele para validar sua propriedade do domínio. Em algumas circunstâncias, o botão Criar registroa 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.

A AWS fornece suporte a domínios não confiáveis publicamente por meio do serviço da CA privada da AWS.

A validação é bem-sucedida, mas a emissão ou renovação falham

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 obter 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

Quando você solicita um certificado do ACM, e escolhe validação por e-mail, o e-mail de validação do domínio é enviado aos cinco endereços administrativos comuns. Para obter mais informações, consulte Validação de e-mail do AWS Certificate Manager. Se você está com problemas de recebimento do e-mail de validação, revise as sugestões a seguir.

Onde procurar o e-mail

O ACM envia mensagens de e-mail de validação para o nome de domínio solicitado. Você também poderá especificar um superdomínio como domínio de validação se quiser receber esses e-mails nesse domínio. Qualquer subdomínio até o endereço mínimo do site é válido e é usado como domínio para o endereço de e-mail como o sufixo após @. Por exemplo, você poderá receber um e-mail para admin@example.com se especificar exemplo.com como o domínio de validação para subdomínio.exemplo.com. 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.

Entre em contato com a Central de suporte

Se, depois de analisar a orientação anterior, você ainda não receber o e-mail de validação de domínio, visite a Central de Suporte e abra um caso. Se você não tiver um contrato de suporte, publique uma mensagem no Fórum de discussão do ACM.

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.

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. Para usar a validação de DNS, exclua o certificado e crie um novo que use a validação de DNS.

Solução de problemas de validação por HTTP

Consulte as orientações a seguir se tiver problemas ao validar um certificado com HTTP.

A primeira etapa na solução de problemas de HTTP é verificar o status atual do seu domínio com ferramentas como as seguintes:

- curl — Linux e Windows
- wget — Linux e Windows

Tópicos

Conteúdo não compatível entre os locais RedirectFrom e Redirect To

Se o conteúdo no local `RedirectFrom` não for compatível com o conteúdo no local `RedirectTo`, a validação apresentará falhas. Assegure que o conteúdo seja idêntico em cada domínio no certificado.

Configuração incorreta do CloudFront

Assegure que a distribuição do CloudFront esteja configurada corretamente para fornecer o conteúdo de validação. Verifique se as configurações de origem e de comportamento estão corretas e se a distribuição foi implantada.

Problemas de redirecionamento HTTP

Se for usado um redirecionamento, em vez de fornecer o conteúdo diretamente, as etapas a seguir devem ser seguidas para que sua configuração seja verificada.

Para verificar a configuração de redirecionamento

1. Copie o URL `RedirectFrom` e cole na barra de endereço do navegador.
2. Em uma nova guia do navegador, cole o URL `RedirectTo`.
3. Compare o conteúdo dos dois URLs para assegurar que sejam exatamente iguais.
4. Verifique se após o redirecionamento o código de status 302 é exibido.

Tempo limite da validação

É possível que a validação por HTTP expire se o conteúdo não estiver disponível dentro do prazo esperado. Para solucionar problemas de validação, siga as etapas abaixo.

Para solucionar o tempo limite da validação

1. Siga um dos procedimentos a seguir para verificar quais domínios estão com validação pendente:

a. Abra o console do ACM e visualize a página de detalhes do certificado. Observe os domínios marcados como Validação pendente.

b. Chame a operação da API `DescribeCertificate` para visualizar o status de validação de cada domínio.

2. Em cada caso de domínio pendente, verifique se o conteúdo da validação pode ser acessado pela internet.

Solucionar 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 do certificado em AWS Certificate Manager.

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 serviço da AWS que esteja integrado com o ACM. Para obter informações sobre os recursos que o ACM suporta, consulte Serviços integrados ao ACM.
- 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 do AWS Certificate Manager.
- Para certificados validados por DNS, certifique-se de que sua configuração de DNS contenha os registros CNAME corretos, conforme descrito em Validação de DNS do AWS Certificate Manager.
- No caso de certificados validados por HTTP, assegure que seus redirecionamentos estejam configurados conforme o descrito em Validação por HTTP do AWS Certificate Manager.

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 obter mais informações, consulte Renovação gerenciada do certificado em AWS Certificate Manager.

Renovação de certificado gerenciada para certificados validados por e-mail

Os certificados do ACM são válidos por 13 meses (395 dias). A renovação de um certificado exige uma ação do proprietário do domínio. O ACM começa a enviar avisos de renovação para os endereços de e-mail associados ao domínio 45 dias antes da expiração. As notificações contêm um link no qual o proprietário do domínio pode clicar para renová-lo. Depois que todos os domínios listados forem validados, o ACM emitirá um certificado renovado com o mesmo ARN.

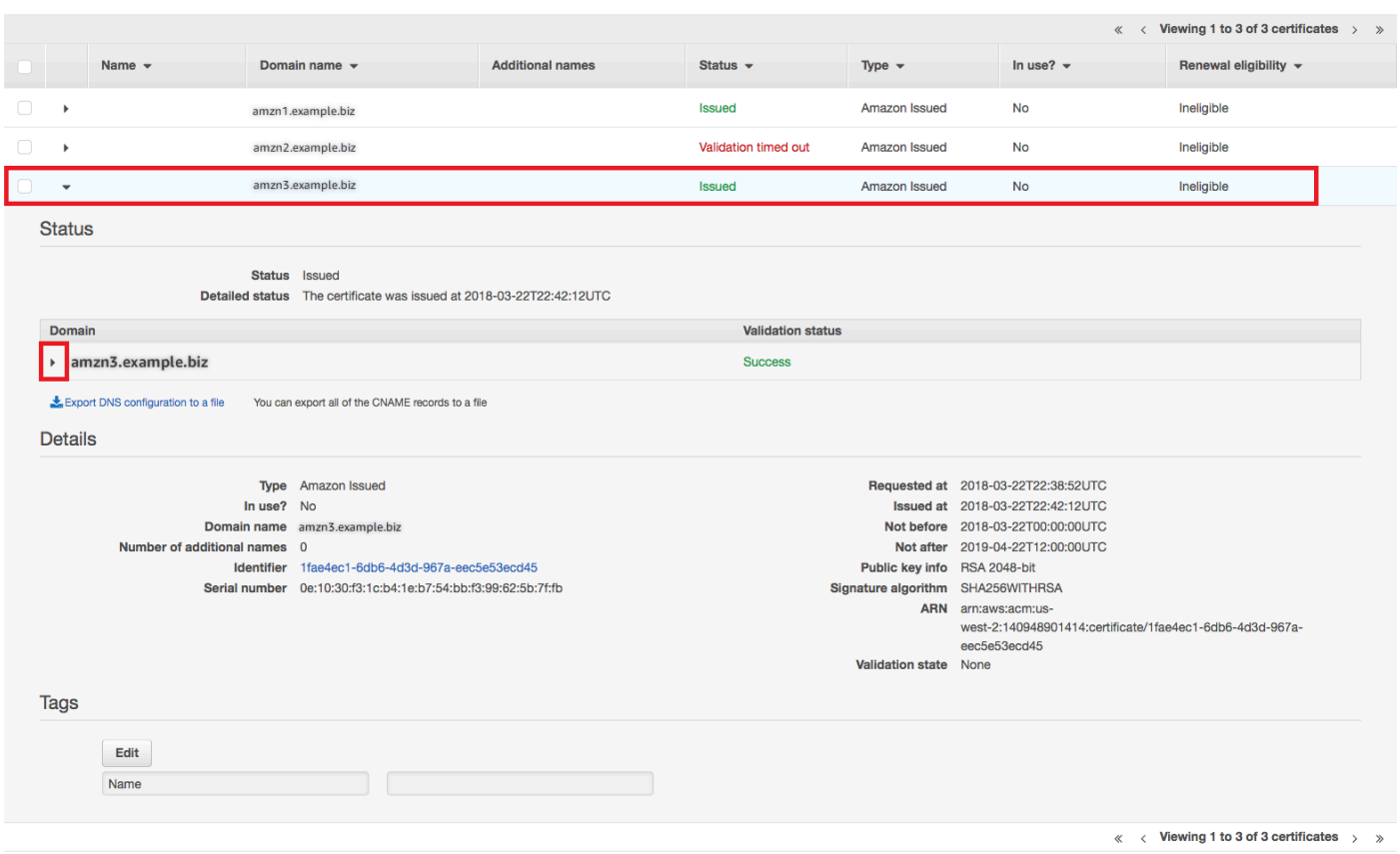
Consulte Validar com e-mail para obter instruções sobre como identificar quais domínios estão no estado `PENDING_VALIDATION` e repita o processo de validação para esses domínios

Renovação de certificado gerenciada para certificados validados por DNS

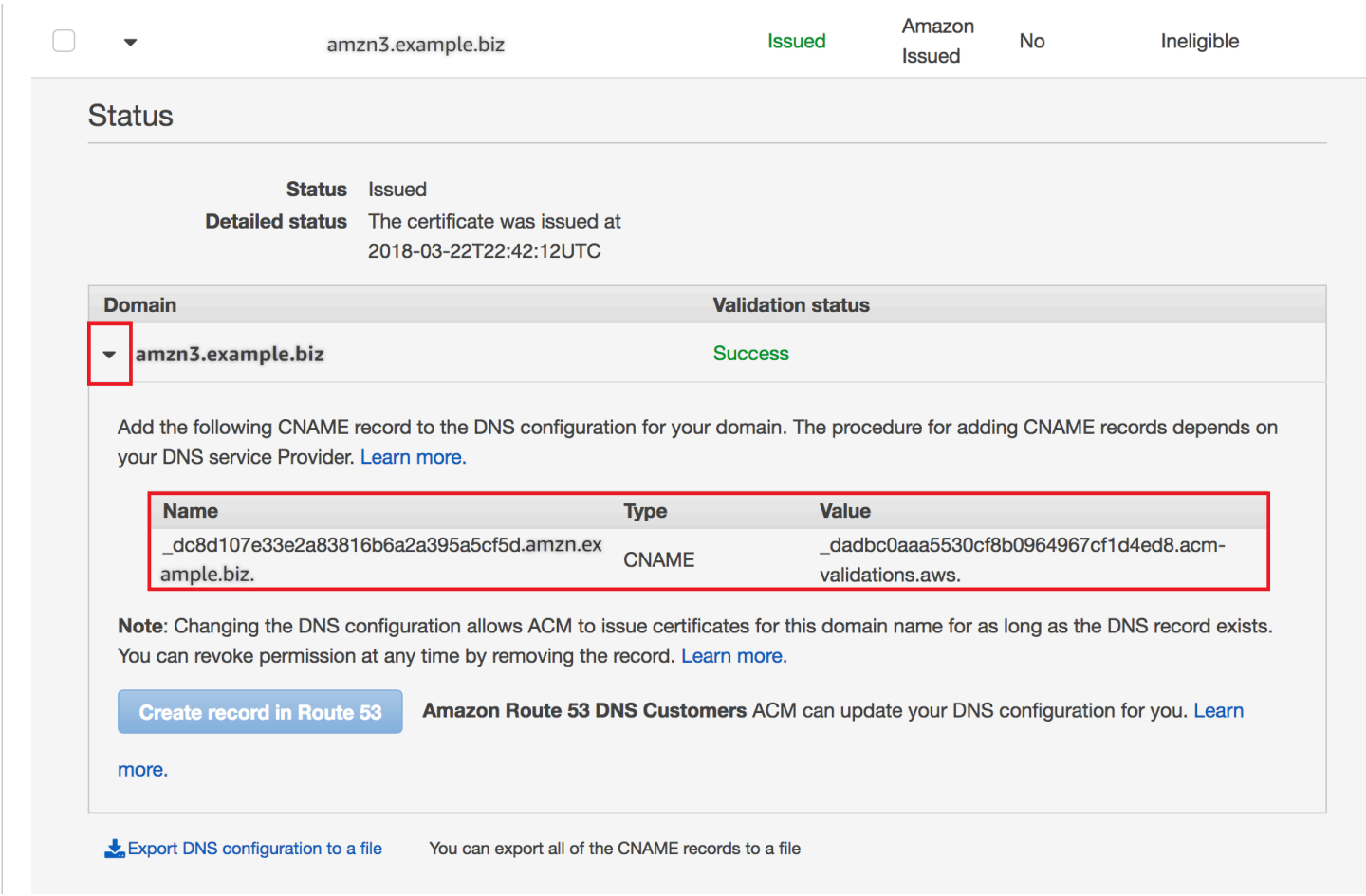
O ACM não tenta realizar a validação de TLS para certificados validados por DNS. Se o ACM não conseguir renovar um certificado validado com a validação por DNS, provavelmente é devido a registros CNAME ausentes ou imprecisos na configuração do DNS. Se isso ocorrer, o ACM notificará você de que o certificado 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 operação DescribeCertificate na API do ACM ou o comando describe-certificate na CLI do ACM. Para obter mais informações, consulte Validação de DNS do AWS Certificate Manager.



Selecione o certificado de destino no console.



Expanda a janela do certificado para encontrar as informações de CNAME.

Se o problema persistir, entre em contato com o Support Center.

Renovação de certificado gerenciada para certificados validados por HTTP

O ACM tenta renovar automaticamente os certificados validados por HTTP. Se houver falha na renovação, é provável que isso esteja ocorrendo devido a problemas com os registros de validação por HTTP. Nesses casos, o ACM notificará que o certificado não pôde ser renovado automaticamente.

> **Important**
>
> Você deve assegurar que o conteúdo no local `RedirectFrom` corresponda ao conteúdo no local `RedirectTo` para cada domínio no certificado.

É possível encontrar as informações de validação por HTTP de seus domínios expandindo seu certificado e as entradas de domínio no console do ACM. Você também pode recuperar essas informações usando a operação DescribeCertificate na API do ACM ou o comando describe-certificate na CLI do ACM. Para obter mais informações, consulte Validação por HTTP do AWS Certificate Manager.

Se o problema persistir, entre em contato com o Support Center.

Prazos de renovação

Renovação gerenciada do certificado em AWS Certificate ManagerO 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 bora 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.

Solucionar 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 ne or 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 do usuário do AWS Certificate Manager e a documentação de cada serviço para garantir que seu certificado funcionará.
- 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 API ListCertificates ou o comando list-certificates da AWS CLI sem especificar o filtro `keyTypes`, somente os certificados `RSA_1024` ou `RSA_2048` serão exibidos.

Problemas de fixação do certificado

Para renovar um certificado, o ACM gera um novo par de chaves pública/privada. Se o seu aplicativo usa Fixação do certificado, às vezes chamada de fixação SSL, para fixar um certificado do ACM, talvez o aplicativo não consiga se conectar ao seu domínio após a 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

Ao implantar um endpoint de API otimizada para borda, o API Gateway configura uma distribuição do CloudFront para você. A distribuição do CloudFront 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) requer permissão para descriptografar uma AWS KMS key que, por sua vez, descriptografa 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 das suas concessões usando o console do AWS KMS 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 em contato com o Suporte 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 compartilhado com você por outra conta, o ACM tenta, no primeiro uso, configurar uma função vinculada ao serviço (SLR) para interagir como entidade principal com uma política de acesso baseada em recursos da CA privada da AWS. 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 comando do AWS Certificate Manager pode falhar por vários motivos. Para obter informações sobre cada exceção, consulte a tabela abaixo.

Tratamento de exceções de certificado privado

As seguintes exceções podem ocorrer quando você tenta renovar um certificado de PKI privado emitido pelo CA privada da AWS.

> **Note**
>
> A CA privada da AWS não está disponível nas regiões China (Pequim) e China (Ningxia).

Código de falha do ACM	Comentário
`PCA_ACCESS_DENIED`	A CA privada não concedeu permissões ao ACM. Isso aciona um código de falha `AccessDeniedException` da CA privada da AWS. Para resolver o problema, conceda as permissões necessárias à entidade principal do serviço do ACM usando a operação CreatePermission da CA privada da AWS.
`PCA_INVALID_DURATION`	O período de validade do certificado solicitado excede o período de validade da CA privada emissora. Isso aciona um código de falha `ValidationException` da CA privada da AWS.

Código de falha do ACM	Comentário
	Para solucionar o problema, instale um novo certificado CA com um período de validade apropriado.
`PCA_INVALID_STATE`	A CA privada que está sendo chamada não está no estado correto para executar a operação do ACM solicitada. Isso aciona um código de falha `InvalidStateException` da CA privada da AWS. Resolva o problema da seguinte forma: • Se a CA tiver o status `CREATING`, aguarde a conclusão da criação e instale o certificado CA. • Se a CA tiver o status `PENDING_CERTIFICATE`, instale o certificado CA. • Se a CA tiver o status `DISABLED`, atualize-a para o status `ACTIVE`. • Se a CA tiver o status `DELETED`, restaure-a. • Se a autoridade de certificação tiver o status `EXPIRED`, instale um novo certificado • Se a CA tiver o status `FAILED`, e você não conseguir resolver o problema, entre em contato com o Suporte.
`PCA_LIMIT_EXCEEDED`	A CA privada atingiu uma cota de emissão. Isso aciona um código de falha `LimitExceededException` da CA privada da AWS. Tente repetir a solicitação antes de prosseguir com esta ajuda. Se o erro persistir, entre em contato com o Suporte para solicitar um aumento de cota.

Código de falha do ACM	Comentário
PCA_REQUEST_FAILED	Ocorreu um erro de rede ou de sistema. Isso aciona um código de falha `RequestFailedException` da CA privada da AWS. Tente repetir a solicitação antes de prosseguir com esta ajuda. Se o erro persistir, entre em contato com o Suporte.
PCA_RESOURCE_NOT_FOUND	A CA privada foi excluída permanentemente. Isso aciona um código de falha `ResourceNotFoundException` da CA privada da AWS. Verifique se você usou o ARN correto. Se isso falhar, você não poderá usar essa CA. Para solucionar o problema, crie outra CA.
SLR_NOT_FOUND	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 Criação da a SLR para o ACM.

Cotas

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

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 Suporte Center.

Cotas gerais

Item	Cota padrão
Número de certificados do ACM Certificados expirados e revogados continuam a contar para esse total. Os certificados assinados por uma CA da CA privada da AWS não contam para esse total.	2500
Número de certificados do ACM por ano (últimos 365 dias) 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 um dado momento, entre em contato com o Suporte Center.	5.000

Item	Cota padrão
Os certificados assinados por uma CA da CA privada da AWS não contam para esse total.	
Número de certificados importados	2.500
Número de certificados importados por ano (últimos 365 dias)	5.000
Número de nomes de domínio por certificado do ACM A cota padrão é de 10 nomes de domínio para cada certificado do ACM. Sua cota pode ser maior. 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. Você pode solicitar até 100 nomes de domínio. Para solicitar um aumento de cota, cria uma solicitação no console do Service Quotas 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 obter mais informações, consulte Validação de domínio. 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.	10

Item	Cota padrão
Número de CAs privadas O ACM é integrado à Autoridade de Certificação Privada da AWS (CA privada da AWS). É possível usar o console do ACM, a AWS CLI ou a API do ACM para solicitar certificados privados de uma autoridade de certificação (CA) privada hospedada pela 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 obter mais informações, consulte Solicitar um certificado privado no AWS Certificate Manager. Também é possível emitir certificados privadas usando o serviço independente do CA privada da AWS. Para obter mais informações, consulte Emitir um certificado privado de entidade final. 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 Excluir a CA privada.	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 informações atualizadas sobre a cota de taxa sobre `IssueCertificate`, consulte os endpoints e cotas para a CA privada da AWS.

Cota de solicitações por segundo para cada operação de API do ACM

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

Para obter mais informações, consulte Referência de API do AWS Certificate Manager.

Histórico do documento

A tabela a seguir descreve o histórico de lançamento da documentação a AWS Certificate Manager partir de 2018.

Alteração	Descrição	Data
Alteração na reimportação de certificados	O ACM permite a reimportação de um certificado para o mesmo ARN somente quando o ClientAuth EKU está ausente do certificado anterior. Isso acomoda as mudanças do setor em que as autoridades de certificação não emitem mais certificados com o ClientAuth EKU para cumprir os requisitos do programa raiz do Chrome.	22 de outubro de 2025
Observação adicionada sobre a emissão de certificados	Foi adicionada uma nota ao tópico do conceito do certificado do ACM detalhando as alterações na emissão do certificado do ACM com a extensão TLS Web Client Authentication.	23 de julho de 2025
Removida a referência à extensão de autenticação	Removida a referência à extensão TLS Web Client Authentication do certificado de exemplo.	3 de julho de 2025
AWS Certificate Manager certificados públicos exportáveis	É possível exportar certificados públicos do ACM.	17 de junho de 2025

O ACM oferece suporte à validação HTTP com CloudFront	O ACM agora oferece suporte à validação HTTP para verificação da propriedade do domínio ao emitir certificados para CloudFront distribuições.	24 de abril de 2025
Descontinuação da validação de e-mail do Mail Exchanger (MX)	O console do ACM não oferece mais suporte ao Mail Exchanger (MX).	11 de julho de 2024
Adição de prática recomendada em relação à separação em nível de conta	Use a separação em nível de conta em suas políticas sempre que possível. Se não for possível, você poderá restringir as permissões no nível da conta ou por meio de chaves de condição de contexto de criptografia em suas políticas.	11 de junho de 2024
Descontinuação em breve da verificação de e-mail do WHOIS	Adição de uma observaçã o sobre a suspensão da verificação de e-mail do WHOIS a partir de junho de 2024.	5 de fevereiro de 2024
Adição de suporte a chave de condição	Foi adicionado suporte a chaves de condição do IAM na solicitação de certifica dos do ACM. Para ver a lista de condições compatíveis, consulte https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported.	24 de agosto de 2023

Suporte ECDSA adicionado	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 https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms.	8 de novembro de 2022
Novos CloudWatch eventos	Adicionados eventos ACM Certificate Expired, ACM Certificate Available e ACM Certificate Renewal Action Required. Para obter uma lista de CloudWatch eventos compatíveis, consultehttps://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	27 de outubro de 2022
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 obter 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	DaysToExpiry Métrica, evento e suporte adicionados APIs. Para obter mais informações, consulte https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html e https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	3 de março de 2021
Adicionado suporte abrangendo todas as contas	Foi adicionado suporte entre contas para usar o formulário privado CAs . CA privada da AWS Para obter mais informações, consulte https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html.	17 de agosto de 2020

Adição de suporte à região	Foi adicionado suporte regional para as regiões AWS da 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.	4 de março de 2020
Adicionados testes de fluxo de trabalho de renovação	Agora, os clientes podem testar manualmente a configuração do seu fluxo de trabalho de renovação gerenciada do ACM. Para obter mais informações, consulte Testar a configuração de renovação gerenciada do ACM.	14 de março de 2019
O registro em log da transparência dos certificados agora é padrão	Adicionada a capacidade de publicar certificados públicos do ACM em logs de transparência de certificados por padrão.	24 de abril de 2018
Lançamento CA privada da AWS	Lançou o ACM Private Certificate Manager (CM), e sua extensão permite AWS Certificate Manager que os usuários estabeleçam uma infraestrutura gerenciada segura para emitir e revogar certificados digitais privados. Para obter mais informações, consulte AWS Private Certificate Authority.	4 de abril de 2018

Registro em log da transparência dos certificados	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 lançamento da documentação AWS Certificate Manager antes de 2018.

Alteração	Description	Data de lançamento
Novo conteúdo	Validação de DNS adicionada a Validação de DNS do AWS Certificate Manager.	21 de novembro de 2017
Novo conteúdo	Adição de novos exemplos de código Java a Usar AWS Certificate Manager com o SDK para Java.	12 de outubro de 2017
Novo conteúdo	Adição de informações sobre registros de CAA a (Opcional) Configurar um registro de CAA.	21 de setembro de 2017
Novo conteúdo	Informações adicionadas sobre domínios .IO a Solucionar problemas com o AWS Certificate Manager.	07 de julho de 2017
Novo conteúdo	Informações adicionadas sobre reimportação de um certificado a Reimportar um certificado.	07 de julho de 2017
Novo conteúdo	Informações adicionadas sobre fixação de certificado a Práticas recomendadas e a	07 de julho de 2017

Alteração	Description	Data de lançamento
	Solucionar problemas com o AWS Certificate Manager.	
Novo conteúdo	CloudFormation Adicionado Serviços integrados ao ACM a.	27 de maio de 2017
Atualizar	Mais informações adicionadas a Cotas.	27 de maio de 2017
Novo conteúdo	Documentação adicionada sobre Identity and Access Management para AWS Certificate Manager.	28 de abril de 2017
Atualizar	Gráfico adicionado para mostrar para onde o e-mail de validação é enviado. Consulte Validação de e-mail do AWS Certificate Manager.	21 de abril de 2017
Atualizar	Informações adicionadas sobre a configuração de e-mail para o seu domínio. Consulte Validação de e-mail do AWS Certificate Manager.	6 de abril de 2017
Atualizar	Informações adicionadas sobre a verificação de status da renovação do certificado no console. Consulte Verificar o status de renovação de um certificado.	28 de março de 2017
Atualizar	Atualização da documenta ção para usar o Elastic Load Balancing.	21 de março de 2017

Alteração	Description	Data de lançamento
Novo conteúdo	Foi adicionado suporte para AWS Elastic Beanstalk o Amazon API Gateway. Consulte Serviços integrados ao ACM.	21 de março de 2017
Atualizar	Documentação sobre Renovação gerenciada de certificados atualizada.	20 de fevereiro de 2017
Novo conteúdo	Documentação adicionada sobre Certificados importados.	13 de outubro de 2016
Novo conteúdo	Foi adicionado AWS CloudTrail suporte para ações do ACM. Consulte Usando CloudTrail com AWS Certificate Manager.	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.