



Panduan Pengguna

# AWS Certificate Manager



Versi 1.0

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

# AWS Certificate Manager: Panduan Pengguna

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

---

# Table of Contents

Apa itu AWS Certificate Manager? .....	1
Wilayah yang Didukung .....	1
Harga .....	2
Konsep .....	2
ACMSertifikat .....	3
ACMAkar CAs .....	5
Domain Apex .....	5
Kriptografi Kunci Asimetris .....	5
Otoritas Sertifikat .....	6
Pencatatan Transparansi Sertifikat .....	6
Sistem Nama Domain .....	7
Nama Domain .....	7
Enkripsi dan Dekripsi .....	8
Nama Domain Berkualitas Penuh (FQDN) .....	9
Infrastruktur Kunci Publik .....	9
Sertifikat Akar .....	9
Lapisan Soket Aman (SSL) .....	9
Aman HTTPS .....	9
SSLSertifikat Server .....	10
Kriptografi Kunci Simetris .....	10
Keamanan Lapisan Transportasi (TLS) .....	10
Percaya .....	10
Apa yang benar AWS layanan sertifikat untuk kebutuhan saya? .....	10
Sertifikat .....	12
Penyiapan .....	13
Mendaftar untuk Akun AWS .....	13
Buat pengguna dengan akses administratif .....	14
Daftarkan nama domain .....	15
(Opsional) Konfigurasi CAA catatan .....	15
Sertifikat publik .....	18
Karakteristik dan keterbatasan .....	18
Minta sertifikat publik .....	24
Validasi kepemilikan domain .....	27
Sertifikat pribadi .....	40

Ketentuan untuk digunakan .....	41
Minta sertifikat pribadi .....	43
Sertifikat ekspor .....	46
Sertifikat yang diimpor .....	49
Prasyarat .....	50
Format Sertifikat .....	51
Impor sertifikat .....	53
Impor kembali sertifikat .....	55
Daftar sertifikat .....	57
Melihat detail sertifikat .....	60
Hapus sertifikat .....	63
Perpanjangan sertifikat terkelola .....	65
Sertifikat publik .....	66
Perpanjangan untuk domain yang DNS divalidasi .....	67
Validasi email .....	67
Sertifikat pribadi .....	68
Mengotomatiskan ekspor sertifikat yang diperbarui .....	69
Uji perpanjangan terkelola .....	71
Periksa status perpanjangan .....	72
Periksa status (konsol) .....	73
Periksa status (API) .....	74
Periksa status (CLI) .....	74
Periksa status menggunakan Personal Health Dashboard (PHD) .....	74
Memberi tanda pada sumber daya .....	76
Batasan tag .....	76
Mengelola tag .....	77
Mengelola tag (konsol) .....	77
Mengelola tag (CLI) .....	79
Kelola tag .....	79
Layanan terintegrasi .....	80
Keamanan .....	85
Perlindungan data .....	86
Keamanan untuk kunci pribadi sertifikat .....	87
Identity and Access Management .....	88
Audiens .....	88
Mengautentikasi dengan identitas .....	89

Mengelola akses menggunakan kebijakan .....	93
Bagaimana AWS Certificate Manager bekerja dengan IAM .....	95
Contoh kebijakan berbasis identitas .....	102
Referensi izin API ACM .....	107
Kebijakan yang dikelola oleh AWS .....	109
Gunakan tombol kondisi .....	112
Gunakan peran tertaut layanan .....	118
Pemecahan Masalah .....	121
Ketangguhan .....	124
Keamanan infrastruktur .....	124
Memberikan akses programatif ke ACM .....	125
Praktik terbaik .....	126
Pemisahan tingkat akun .....	127
AWS CloudFormation .....	127
Penyematan sertifikat .....	128
Validasi domain .....	129
Menambahkan atau menghapus nama domain .....	129
Memilih keluar dari pencatatan transparansi sertifikat .....	130
Nyalakan AWS CloudTrail .....	131
Monitor dan log .....	133
Amazon EventBridge .....	133
Acara yang didukung .....	133
Contoh tindakan .....	138
CloudTrail .....	148
APITindakan yang didukung .....	149
APIpanggilan untuk layanan terintegrasi .....	163
CloudWatch metrik .....	168
Gunakan AWS Certificate Manager dengan SDK untuk Java .....	169
AddTagsToCertificate .....	169
DeleteCertificate .....	171
DescribeCertificate .....	173
ExportCertificate .....	176
GetCertificate .....	179
ImportCertificate .....	181
ListCertificates .....	185
RenewCertificate .....	187

ListTagsForCertificate .....	189
RemoveTagsFromCertificate .....	191
RequestCertificate .....	193
ResendValidationEmail .....	196
Pemecahan Masalah .....	199
Permintaan sertifikat .....	199
Minta waktu habis .....	199
Permintaan gagal .....	200
Validasi sertifikat .....	201
DNSvalidasi .....	202
Validasi email .....	205
Perpanjangan sertifikat .....	207
Mempersiapkan validasi domain otomatis .....	207
Menangani kegagalan dalam perpanjangan sertifikat terkelola .....	207
Masalah lainnya .....	211
CAAcatatan .....	211
Impor sertifikat .....	212
Penyematan sertifikat .....	212
APIGerbang .....	213
Kegagalan tak terduga .....	213
Masalah dengan peran ACM terkait layanan () SLR .....	214
Menangani pengecualian .....	214
Penanganan pengecualian sertifikat pribadi .....	214
Kuota .....	218
Kuota umum .....	218
APIkuota tarif .....	220
Riwayat dokumen .....	223
.....	CCXXX

# Apa itu AWS Certificate Manager?

AWS Certificate Manager (ACM) menangani kompleksitas pembuatan, penyimpanan, dan pembaruan sertifikat dan kunci publik dan SSL TLS pribadi/X.509 yang melindungi Anda AWS situs web dan aplikasi. Anda dapat memberikan sertifikat untuk [terintegrasi AWS layanan](#) baik dengan menerbitkannya secara langsung dengan ACM atau dengan [mengimpor](#) sertifikat pihak ketiga ke dalam sistem ACM manajemen. ACMsertifikat dapat mengamankan nama domain tunggal, beberapa nama domain tertentu, domain wildcard, atau kombinasi dari ini. ACMsertifikat wildcard dapat melindungi jumlah subdomain yang tidak terbatas. Anda juga dapat [mengeksport](#) ACM sertifikat yang ditandatangani oleh AWS Private CA untuk digunakan di mana saja di internal AndaPKI.

## Note

ACMtidak dimaksudkan untuk digunakan dengan server web yang berdiri sendiri. Jika Anda ingin menyiapkan server aman yang berdiri sendiri di EC2 instans Amazon, tutorial berikut memiliki instruksi: [Konfigurasi SSL/di TLS Amazon Linux 2023](#).

## Topik

- [Wilayah yang Didukung](#)
- [Harga untuk AWS Certificate Manager](#)
- [AWS Certificate Manager konsep](#)
- [Apa yang benar AWS layanan sertifikat untuk kebutuhan saya?](#)

## Wilayah yang Didukung

Kunjungi [AWS Wilayah dan Titik Akhir](#) di Referensi Umum AWSatau [AWS Tabel Wilayah](#) untuk melihat ketersediaan regional untukACM.

Sertifikat di ACM adalah sumber daya regional. Untuk menggunakan sertifikat dengan Elastic Load Balancing untuk nama domain yang memenuhi syarat penuh (FQDN) yang sama atau set FQDNs di lebih dari satu AWS wilayah, Anda harus meminta atau mengimpor sertifikat untuk setiap wilayah. Untuk sertifikat yang disediakan olehACM, ini berarti Anda harus memvalidasi ulang setiap nama domain dalam sertifikat untuk setiap wilayah. Anda tidak dapat menyalin sertifikat antar wilayah.

Untuk menggunakan ACM sertifikat dengan Amazon CloudFront, Anda harus meminta atau mengimpor sertifikat di wilayah AS Timur (Virginia N.). ACMsertifikat di wilayah ini yang terkait dengan CloudFront distribusi didistribusikan ke semua lokasi geografis yang dikonfigurasi untuk distribusi tersebut.

## Harga untuk AWS Certificate Manager

Anda tidak dikenakan biaya tambahan untukSSL/TLSsertifikat yang Anda kelola AWS Certificate Manager. Anda hanya membayar untuk AWS sumber daya yang Anda buat untuk menjalankan situs web atau aplikasi Anda. Untuk informasi ACM harga terbaru, lihat [AWS Certificate Manager](#)Halaman Harga Layanan di AWS situs web.

## AWS Certificate Manager konsep

Bagian ini memberikan definisi konsep yang digunakan oleh AWS Certificate Manager.

### Topik

- [ACMSertifikat](#)
- [ACMAkar CAs](#)
- [Domain Apex](#)
- [Kriptografi Kunci Asimetris](#)
- [Otoritas Sertifikat](#)
- [Pencatatan Transparansi Sertifikat](#)
- [Sistem Nama Domain](#)
- [Nama Domain](#)
- [Enkripsi dan Dekripsi](#)
- [Nama Domain Berkualitas Penuh \(FQDN\)](#)
- [Infrastruktur Kunci Publik](#)
- [Sertifikat Akar](#)
- [Lapisan Soket Aman \(SSL\)](#)
- [Aman HTTPS](#)
- [SSLSertifikat Server](#)
- [Kriptografi Kunci Simetris](#)
- [Keamanan Lapisan Transportasi \(TLS\)](#)



- [Percaya](#)

## ACMSertifikat

ACM menghasilkan sertifikat X.509 versi 3. Masing-masing berlaku selama 13 bulan (395 hari) dan berisi ekstensi berikut.

- Kendala Dasar - menentukan apakah subjek sertifikat adalah otoritas sertifikasi (CA)
- Authority Key Identifier - memungkinkan identifikasi kunci publik yang sesuai dengan kunci pribadi yang digunakan untuk menandatangani sertifikat.
- Subject Key Identifier - memungkinkan identifikasi sertifikat yang berisi kunci publik tertentu.
- Key Usage - mendefinisikan tujuan dari kunci publik yang tertanam dalam sertifikat.
- Penggunaan Kunci yang Diperpanjang - menentukan satu atau lebih tujuan yang dapat digunakan kunci publik selain tujuan yang ditentukan oleh ekstensi Penggunaan Kunci.
- CRLPoin Distribusi - menentukan di mana CRL informasi dapat diperoleh.

Teks biasa dari sertifikat ACM yang diterbitkan menyerupai contoh berikut:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      f2:16:ad:85:d8:42:d1:8a:3f:33:fa:cc:c8:50:a8:9e
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O=Example CA
    Validity
      Not Before: Jan 30 18:46:53 2018 GMT
      Not After : Jan 31 19:46:53 2018 GMT
    Subject: C=US, ST=VA, L=Herndon, O=Amazon, OU=AWS, CN=example.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:ba:a6:8a:aa:91:0b:63:e8:08:de:ca:e7:59:a4:
        69:4c:e9:ea:26:04:d5:31:54:f5:ec:cb:4e:af:27:
        e3:94:0f:a6:85:41:6b:8e:a3:c1:c8:c0:3f:1c:ac:
        a2:ca:0a:b2:dd:7f:c0:57:53:0b:9f:b4:70:78:d5:
        43:20:ef:2c:07:5a:e4:1f:d1:25:24:4a:81:ab:d5:
        08:26:73:f8:a6:d7:22:c2:4f:4f:86:72:0e:11:95:
```

```
03:96:6d:d5:3f:ff:18:a6:0b:36:c5:4f:78:bc:51:
b5:b6:36:86:7c:36:65:6f:2e:82:73:1f:c7:95:85:
a4:77:96:3f:c0:96:e2:02:94:64:f0:3a:df:e0:76:
05:c4:56:a2:44:72:6f:8a:8a:a1:f3:ee:34:47:14:
bc:32:f7:50:6a:e9:42:f5:f4:1c:9a:7a:74:1d:e5:
68:09:75:19:4b:ac:c6:33:90:97:8c:0d:d1:eb:8a:
02:f3:3e:01:83:8d:16:f6:40:39:21:be:1a:72:d8:
5a:15:68:75:42:3e:f0:0d:54:16:ed:9a:8f:94:ec:
59:25:e0:37:8e:af:6a:6d:99:0a:8d:7d:78:0f:ea:
40:6d:3a:55:36:8e:60:5b:d6:0d:b4:06:a3:ac:ab:
e2:bf:c9:b7:fe:22:9e:2a:f6:f3:42:bb:94:3e:b7:
08:73
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Authority Key Identifier:

keyid:84:8C:AC:03:A2:38:D9:B6:81:7C:DF:F1:95:C3:28:31:D5:F7:88:42

X509v3 Subject Key Identifier:

97:06:15:F1:EA:EC:07:83:4C:19:A9:2F:AF:BA:BB:FC:B2:3B:55:D8

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 CRL Distribution Points:

Full Name:

URI:http://example.com/crl

Signature Algorithm: sha256WithRSAEncryption

```
69:03:15:0c:fb:a9:39:a3:30:63:b2:d4:fb:cc:8f:48:a3:46:
69:60:a7:33:4a:f4:74:88:c6:b6:b6:b8:ab:32:c2:a0:98:c6:
8d:f0:8f:b5:df:78:a1:5b:02:18:72:65:bb:53:af:2f:3a:43:
76:3c:9d:d4:35:a2:e2:1f:29:11:67:80:29:b9:fe:c9:42:52:
cb:6d:cd:d0:e2:2f:16:26:19:cd:f7:26:c5:dc:81:40:3b:e3:
d1:b0:7e:ba:80:99:9a:5f:dd:92:b0:bb:0c:32:dd:68:69:08:
e9:3c:41:2f:15:a7:53:78:4d:33:45:17:3e:f2:f1:45:6b:e7:
17:d4:80:41:15:75:ed:c3:d4:b5:e3:48:8d:b5:0d:86:d4:7d:
94:27:62:84:d8:98:6f:90:1e:9c:e0:0b:fa:94:cc:9c:ee:3a:
8a:6e:6a:9d:ad:b8:76:7b:9a:5f:d1:a5:4f:d0:b7:07:f8:1c:
03:e5:3a:90:8c:bc:76:c9:96:f0:4a:31:65:60:d8:10:fc:36:
44:8a:c1:fb:9c:33:75:fe:a6:08:d3:89:81:b0:6f:c3:04:0b:
a3:04:a1:d1:1c:46:57:41:08:40:b1:38:f9:57:62:97:10:42:
8e:f3:a7:a8:77:26:71:74:c2:0a:5b:9e:cc:d5:2c:c5:27:c3:
12:b9:35:d5
```

## ACMAkar CAs

Sertifikat entitas akhir publik yang dikeluarkan oleh ACM memperoleh kepercayaan mereka dari root Amazon berikut: CAs

Nama yang terhormat	Enkripsi algoritme
cn = Amazon Root CA 1, O = Amazon, C = AS	2048-bit () RSA RSA_2048
cn = Amazon Root CA 2, O = Amazon, C = AS	4096-bit () RSA RSA_4096
cn = Amazon Root CA 3, O = Amazon, C = AS	Kurva Perdana Elips 256 bit () EC_prime256v1
cn = Amazon Root CA 4, O = Amazon, C = AS	Kurva Perdana Elips 384 bit () EC_secp384r1

Akar kepercayaan default untuk sertifikat yang ACM diterbitkan adalah CN = Amazon Root CA 1, O = Amazon, C = US, yang menawarkan keamanan 2048-bit. RSA Akar lainnya dicadangkan untuk penggunaan masa depan. Semua akar ditandatangani silang oleh sertifikat Otoritas Sertifikat Root Layanan Starfield.

Untuk informasi selengkapnya, lihat [Amazon Trust Services](#).

## Domain Apex

Lihat [Nama Domain](#).

## Kriptografi Kunci Asimetris

Tidak seperti [Kriptografi Kunci Simetris](#), kriptografi asimetris menggunakan kunci yang berbeda tetapi terkait secara matematis untuk mengenkripsi dan mendekripsi konten. Salah satu kuncinya bersifat publik dan biasanya tersedia dalam sertifikat X.509 v3. Kunci lainnya bersifat privat dan disimpan dengan aman. Sertifikat X.509 mengikat identitas pengguna, komputer, atau sumber daya lain (subjek sertifikat) ke kunci publik.

ACMsertifikat adalah SSL TLS X.509/sertifikat yang mengikat identitas situs web Anda dan rincian organisasi Anda ke kunci publik yang terkandung dalam sertifikat. ACMmenggunakan Anda AWS KMS key untuk mengenkripsi kunci pribadi. Untuk informasi selengkapnya, lihat [Keamanan untuk kunci pribadi sertifikat](#).

## Otoritas Sertifikat

Otoritas sertifikat (CA) adalah entitas yang mengeluarkan sertifikat digital. Secara komersial, jenis sertifikat digital yang paling umum didasarkan pada standar ISO X.509. CA mengeluarkan sertifikat digital yang ditandatangani yang menegaskan identitas subjek sertifikat dan mengikat identitas itu ke kunci publik yang terkandung dalam sertifikat. CA juga biasanya mengelola pencabutan sertifikat.

## Pencatatan Transparansi Sertifikat

Untuk menjaga terhadapSSL/TLSsertifikat yang dikeluarkan secara tidak sengaja atau oleh CA yang dikompromikan, beberapa browser mengharuskan sertifikat publik yang dikeluarkan untuk domain Anda dicatat dalam log transparansi sertifikat. Nama domain dicatat. Private key tidak. Sertifikat yang tidak dicatat biasanya menghasilkan kesalahan di browser.

Anda dapat memantau log untuk memastikan bahwa hanya sertifikat yang telah Anda otorisasi telah dikeluarkan untuk domain Anda. Anda dapat menggunakan layanan seperti [Certificate Search](#) untuk memeriksa log.

Sebelum Amazon CA mengeluarkan TLS sertifikat yang dipercaya SSL publik untuk domain Anda, Amazon mengirimkan sertifikat ke setidaknya tiga server log transparansi sertifikat. Server ini menambahkan sertifikat ke database publik mereka dan mengembalikan timestamp sertifikat yang ditandatangani (SCT) ke Amazon CA. CA kemudian menyematkan SCT sertifikat, menandatangani sertifikat, dan menerbitkannya kepada Anda. Stempel waktu disertakan dengan ekstensi X.509 lainnya.

```
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

Pencatatan transparansi sertifikat otomatis saat Anda meminta atau memperbarui sertifikat kecuali Anda memilih untuk tidak ikut serta. Untuk informasi selengkapnya tentang memilih keluar, lihat [Memilih keluar dari pencatatan transparansi sertifikat](#).

## Sistem Nama Domain

Domain Name System (DNS) adalah sistem penamaan terdistribusi hierarkis untuk komputer dan sumber daya lain yang terhubung ke internet atau jaringan pribadi. DNS terutama digunakan untuk menerjemahkan nama domain tekstual, seperti `aws.amazon.com`, ke alamat IP numerik (Internet Protocol) dari formulir `111.122.133.144`. DNS Database untuk domain Anda, bagaimanapun, berisi sejumlah catatan yang dapat digunakan untuk tujuan lain. Misalnya, dengan ACM Anda dapat menggunakan CNAME catatan untuk memvalidasi bahwa Anda memiliki atau mengontrol domain saat Anda meminta sertifikat. Untuk informasi selengkapnya, lihat [AWS Certificate Manager DNS validasi](#).

## Nama Domain

Nama domain adalah string teks seperti `www.example.com` yang dapat diterjemahkan oleh Domain Name System (DNS) ke alamat IP. Jaringan komputer, termasuk internet, menggunakan alamat IP, bukan nama teks. Nama domain terdiri dari label berbeda yang dipisahkan oleh periode:

### TLD

Label paling kanan disebut domain tingkat atas (TLD). Contoh umumnya termasuk `.com`, `.net`, dan `.edu`. Juga, TLD untuk entitas yang terdaftar di beberapa negara adalah singkatan dari nama negara dan disebut kode negara. Contohnya termasuk `.uk` untuk Inggris, `.ru` untuk Rusia, dan `.fr` untuk Prancis. Ketika kode negara digunakan, hierarki tingkat kedua untuk TLD sering diperkenalkan untuk mengidentifikasi jenis entitas terdaftar. Misalnya, `.co.uk` TLD mengidentifikasi perusahaan komersial di Inggris.

## Domain Apex

Nama domain puncak mencakup dan diperluas pada domain tingkat atas. Untuk nama domain yang menyertakan kode negara, domain apex menyertakan kode dan label, jika ada, yang mengidentifikasi jenis entitas terdaftar. Domain apex tidak menyertakan subdomain (lihat paragraf berikut). Di `www.example.com`, nama domain apexnya adalah `example.com`. Di `www.example.co.uk`, nama domain apex adalah `example.co.uk`. Nama lain yang sering digunakan sebagai pengganti apex adalah `base`, `bare`, `root`, `root apex`, atau `zone apex`.

## Subdomain

Nama subdomain mendahului nama domain puncak dan dipisahkan darinya dan satu sama lain dengan titik. Nama subdomain yang paling umum adalah `www`, tetapi nama apa pun dimungkinkan. Nama subdomain juga dapat memiliki beberapa level. Misalnya, di `jake.dog.animals.example.com`, subdomainnya adalah `jake`, `dog`, dan `animals` dalam urutan itu.

## Superdomain

Domain yang menjadi milik subdomain.

## FQDN

Nama domain yang sepenuhnya memenuhi syarat (FQDN) adalah DNS nama lengkap untuk komputer, situs web, atau sumber daya lain yang terhubung ke jaringan atau ke internet. Misalnya `aws.amazon.com` FQDN untuk Amazon Web Services. An FQDN mencakup semua domain hingga domain tingkat atas. Misalnya, `[subdomain1].[subdomain2]. . . [subdomainn].[apex domain].[top-level domain]` mewakili format umum dari sebuah FQDN.

## PQDN

Nama domain yang tidak sepenuhnya memenuhi syarat disebut nama domain yang memenuhi syarat sebagian (PQDN) dan ambigu. Nama seperti `[subdomain1.subdomain2.]` adalah PQDN karena domain root tidak dapat ditentukan.

## Enkripsi dan Dekripsi

Enkripsi adalah proses penyediaan kerahasiaan data. Dekripsi membalikkan proses dan memulihkan data asli. Data yang tidak terenkripsi biasanya disebut plaintext apakah itu teks atau bukan. Data terenkripsi biasanya disebut ciphertext. HTTPS enkripsi pesan antara klien dan server menggunakan

algoritma dan kunci. Algoritma mendefinisikan step-by-step prosedur dimana data plaintext diubah menjadi ciphertext (enkripsi) dan ciphertext diubah kembali menjadi plaintext asli (dekripsi). Kunci digunakan oleh algoritma selama proses enkripsi atau dekripsi. Kunci dapat berupa pribadi atau publik.

## Nama Domain Berkualitas Penuh (FQDN)

Lihat [Nama Domain](#).

## Infrastruktur Kunci Publik

Infrastruktur kunci publik (PKI) terdiri dari perangkat keras, perangkat lunak, orang, kebijakan, dokumen, dan prosedur yang diperlukan untuk membuat, menerbitkan, mengelola, mendistribusikan, menggunakan, menyimpan, dan mencabut sertifikat digital. PKI memfasilitasi transfer informasi yang aman di seluruh jaringan komputer.

## Sertifikat Akar

Otoritas sertifikat (CA) biasanya ada dalam struktur hierarkis yang berisi beberapa lainnya CAs dengan hubungan orangtua-anak yang jelas di antara mereka. Anak atau bawahan CAs disertifikasi oleh orang tua mereka CAs, membuat rantai sertifikat. CA di bagian atas hierarki disebut sebagai CA akar, dan sertifikatnya disebut sertifikat akar. Sertifikat ini biasanya ditandatangani sendiri.

## Lapisan Soket Aman (SSL)

Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) adalah protokol kriptografi yang memberikan keamanan komunikasi melalui jaringan komputer. TLS adalah penerus SSL. Keduanya menggunakan sertifikat X.509 untuk mengautentikasi server. Kedua protokol menegosiasikan kunci simetris antara klien dan server yang digunakan untuk mengenkripsi data yang mengalir antara dua entitas.

## Aman HTTPS

HTTPS singkatan HTTP dari over SSL/TLS, bentuk aman HTTP yang didukung oleh semua browser dan server utama. Semua HTTP permintaan dan tanggapan dienkripsi sebelum dikirim melalui jaringan. HTTPS menggabungkan HTTP protokol dengan teknik kriptografi berbasis sertifikat simetris, asimetris, dan X.509. HTTPS bekerja dengan memasukkan lapisan keamanan kriptografi di bawah lapisan HTTP aplikasi dan di atas lapisan TCP transport dalam model Open Systems Interconnection

()OSI. Lapisan keamanan menggunakan protokol Secure Sockets Layer (SSL) atau protokol Transport Layer Security (TLS).

## SSLSertifikat Server

HTTPStransaksi memerlukan sertifikat server untuk mengautentikasi server. Sertifikat server adalah struktur data X.509 v3 yang mengikat kunci publik dalam sertifikat ke subjek sertifikat. TLSSertifikat SSL /ditandatangani oleh otoritas sertifikat (CA) dan berisi nama server, masa berlaku, kunci publik, algoritma tanda tangan, dan banyak lagi.

## Kriptografi Kunci Simetris

Kriptografi kunci simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data digital. Lihat juga [Kriptografi Kunci Asimetris](#).

## Keamanan Lapisan Transportasi (TLS)

Lihat [Lapisan Soket Aman \(SSL\)](#).

## Percaya

Agar peramban web mempercayai identitas situs web, peramban harus dapat memverifikasi sertifikat situs web. Namun, peramban hanya mempercayai sejumlah kecil sertifikat yang dikenal sebagai sertifikat akar CA. Pihak ketiga tepercaya, yang dikenal sebagai otoritas sertifikasi (CA), memvalidasi identitas situs web dan menerbitkan sertifikat digital yang ditandatangani ke operator situs web. Peramban kemudian dapat memeriksa tanda tangan digital untuk memvalidasi identitas situs web. Jika validasi berhasil, peramban menampilkan ikon kunci di bilah alamat.

## Apa yang benar AWS layanan sertifikat untuk kebutuhan saya?

AWS menawarkan dua opsi kepada pelanggan yang menerapkan sertifikat X.509 terkelola. Pilih yang terbaik untuk kebutuhan Anda.

1. AWS Certificate Manager (ACM) —Layanan ini untuk pelanggan perusahaan yang membutuhkan kehadiran web yang aman menggunakanTLS. ACMsertifikat digunakan melalui Elastic Load Balancing, Amazon CloudFront, API Amazon Gateway, dan terintegrasi lainnya [AWS layanan](#). Aplikasi paling umum dari jenis ini adalah situs web publik yang aman dengan persyaratan lalu lintas yang signifikan. ACMjuga menyederhanakan manajemen keamanan dengan



mengotomatiskan pembaruan sertifikat yang kedaluwarsa. Anda berada di tempat yang tepat untuk layanan ini.

2. **AWS Private CA**—Layanan ini untuk pelanggan perusahaan yang membangun infrastruktur kunci publik (PKI) di dalam AWS cloud dan ditujukan untuk penggunaan pribadi dalam suatu organisasi. Dengan AWS Private CA, Anda dapat membuat hierarki otoritas sertifikat (CA) Anda sendiri dan mengeluarkan sertifikat dengannya untuk mengautentikasi pengguna, komputer, aplikasi, layanan, server, dan perangkat lain. Sertifikat yang dikeluarkan oleh CA pribadi tidak dapat digunakan di internet. Untuk informasi lebih lanjut, lihat [AWS Private CA Panduan Pengguna](#).

# AWS Certificate Manager sertifikat

ACM mengelola sertifikat publik, swasta, dan impor. Sertifikat digunakan untuk membangun komunikasi yang aman di internet atau dalam jaringan internal. Anda dapat meminta sertifikat yang dipercaya secara publik langsung dari ACM (“ACMsertifikat”), mengimpor sertifikat tepercaya publik yang dikeluarkan oleh pihak ketiga. Sertifikat yang ditandatangani sendiri juga didukung. Untuk menyediakan internal organisasi Anda PKI, Anda dapat menerbitkan ACM sertifikat yang ditandatangani oleh otoritas sertifikat pribadi (CA) yang dibuat dan dikelola oleh [AWS Private CA](#). CA dapat berada di akun Anda atau dibagikan dengan Anda oleh akun lain.

## Note

ACM Sertifikat publik dapat diinstal pada EC2 instans Amazon yang terhubung ke [Enclave Nitro](#), tetapi tidak ke instans Amazon lainnya. EC2 Untuk informasi tentang pengaturan server web mandiri pada EC2 instans Amazon yang tidak terhubung ke Enclave Nitro, lihat [Tutorial: Menginstal LAMP server web di Amazon Linux 2](#) atau [Tutorial: Menginstal server LAMP web dengan Amazon Linux. AMI](#)

## Note

Karena sertifikat yang ditandatangani oleh CA pribadi tidak dipercaya secara default, administrator harus menginstalnya di toko kepercayaan klien.

Untuk mulai menerbitkan sertifikat, masuk ke AWS Konsol Manajemen dan buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>. Jika halaman pengantar muncul, pilih Memulai. Jika tidak, pilih Certificate Manager atau Private CAs di panel navigasi kiri.

## Topik

- [Siapkan untuk digunakan AWS Certificate Manager](#)
- [AWS Certificate Manager sertifikat publik](#)
- [Sertifikat pribadi di AWS Certificate Manager](#)
- [Impor sertifikat ke AWS Certificate Manager](#)
- [Daftar sertifikat yang dikelola oleh AWS Certificate Manager](#)

- [Tayang AWS Certificate Manager rincian sertifikat](#)
- [Hapus sertifikat yang dikelola oleh AWS Certificate Manager](#)

## Siapkan untuk digunakan AWS Certificate Manager

Dengan AWS Certificate Manager (ACM) Anda dapat menyediakan dan SSL TLS mengelola/ sertifikat untuk Anda AWS situs web dan aplikasi berbasis. Anda gunakan ACM untuk membuat atau mengimpor dan kemudian mengelola sertifikat. Anda harus menggunakan yang lain AWS layanan untuk menyebarkan sertifikat ke situs web atau aplikasi Anda. Untuk informasi selengkapnya tentang layanan yang terintegrasi ACM, lihat [Layanan terintegrasi dengan ACM](#). Bagian berikut membahas langkah-langkah yang perlu Anda lakukan sebelum menggunakan ACM.

### Topik

- [Mendaftar untuk Akun AWS](#)
- [Buat pengguna dengan akses administratif](#)
- [Daftarkan nama domain untuk ACM](#)
- [\(Opsional\) Konfigurasi CAA catatan](#)

## Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Ketika Anda mendaftar untuk Akun AWS, sebuah Pengguna root akun AWS diciptakan. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimkan Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

## Buat pengguna dengan akses administratif

Setelah Anda mendaftar untuk Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

### Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan Anda Akun AWS alamat email. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuknya, lihat [Mengaktifkan MFA perangkat virtual untuk Akun AWS root user \(konsol\)](#) di Panduan IAM Pengguna.

### Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk petunjuk, lihat [Mengaktifkan AWS IAM Identity Center](#) di AWS IAM Identity Center Panduan Pengguna.

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di AWS IAM Identity Center Panduan Pengguna.

### Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke AWS akses portal](#) di AWS Sign-In Panduan Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di AWS IAM Identity Center Panduan Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di AWS IAM Identity Center Panduan Pengguna.

## Daftarkan nama domain untuk ACM

Nama domain yang sepenuhnya memenuhi syarat (FQDN) adalah nama unik organisasi atau individu di Internet diikuti oleh ekstensi domain tingkat atas seperti .com atau .org. Jika Anda belum memiliki nama domain terdaftar, Anda dapat mendaftarkannya melalui Amazon Route 53 atau lusinan pendaftar komersial lainnya. Biasanya Anda pergi ke situs web registrar dan meminta nama domain. Eregistrasi nama domain biasanya berlangsung selama jangka waktu tertentu seperti satu atau dua tahun sebelum harus diperpanjang.

Untuk informasi selengkapnya tentang mendaftarkan nama domain dengan Amazon Route 53, lihat [Mendaftarkan Nama Domain Menggunakan Amazon Route 53](#) di Panduan Pengembang Amazon Route 53.

## (Opsional) Konfigurasi CAA catatan

CAACatatan menentukan otoritas sertifikat (CAs) mana yang diizinkan mengeluarkan sertifikat untuk domain atau subdomain. Membuat CAA catatan untuk digunakan dengan ACM membantu CAs mencegah kesalahan menerbitkan sertifikat untuk domain Anda. CAACatatan bukanlah pengganti persyaratan keamanan yang ditentukan oleh otoritas sertifikat Anda, seperti persyaratan untuk memvalidasi bahwa Anda adalah pemilik domain.

Setelah ACM memvalidasi domain Anda selama proses permintaan sertifikat, ia memeriksa keberadaan CAA catatan untuk memastikannya dapat mengeluarkan sertifikat untuk Anda. Mengkonfigurasi CAA catatan adalah opsional.

Gunakan nilai berikut saat Anda mengonfigurasi CAA rekaman Anda:

bendera

Menentukan apakah nilai bidang tag didukung oleh ACM. Tetapkan nilai ini ke 0.

tag

Bidang tag dapat menjadi salah satu nilai berikut. Perhatikan bahwa bidang iodef saat ini diabaikan.

masalah

Menunjukkan bahwa ACM CA yang Anda tentukan di bidang nilai diotorisasi untuk menerbitkan sertifikat untuk domain atau subdomain Anda.

issuewild

Menunjukkan bahwa ACM CA yang Anda tentukan di bidang nilai diotorisasi untuk menerbitkan sertifikat wildcard untuk domain atau subdomain Anda. Sertifikat wildcard berlaku untuk domain atau subdomain dan semua subdomainnya.

nilai

Nilai bidang ini tergantung pada nilai bidang tag. Anda harus melampirkan nilai ini dalam tanda kutip ("").

Saat tag menjadi masalah

Bidang nilai berisi nama domain CA. Bidang ini dapat berisi nama CA selain Amazon CA. Namun, jika Anda tidak memiliki CAA catatan yang menentukan salah satu dari empat Amazon berikut CA, ACM tidak dapat menerbitkan sertifikat ke domain atau subdomain Anda:

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

Bidang nilai juga dapat berisi titik koma (;) untuk menunjukkan bahwa tidak ada CA yang diizinkan mengeluarkan sertifikat untuk domain atau subdomain Anda. Gunakan bidang ini jika Anda memutuskan pada titik tertentu bahwa Anda tidak lagi menginginkan sertifikat dikeluarkan untuk domain tertentu.

## Saat tag adalah issuewild

Bidang nilai sama dengan ketika tag diterbitkan kecuali nilainya berlaku untuk sertifikat wildcard.

Ketika ada CAA catatan issuewild yang tidak menyertakan nilai ACM CA, maka tidak ada kartu liar yang dapat dikeluarkan oleh. ACM Jika tidak ada issuewild hadir, tetapi ada CAA catatan masalah untuk ACM, maka kartu liar dapat dikeluarkan oleh. ACM

## Example CAAContoh Rekam

Dalam contoh berikut, nama domain Anda pertama kali diikuti oleh tipe record (CAA). Bidang bendera selalu 0. Bidang tag dapat berupa issue atau issuewild. Jika bidang bermasalah dan Anda mengetikkan nama domain server CA di bidang nilai, CAA catatan menunjukkan bahwa server yang Anda tentukan diizinkan untuk mengeluarkan sertifikat yang Anda minta. Jika Anda mengetik titik koma ";" di bidang nilai, CAA catatan menunjukkan bahwa tidak ada CA yang diizinkan untuk mengeluarkan sertifikat. Konfigurasi CAA catatan bervariasi menurut DNS penyedia.

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	";"

Untuk informasi selengkapnya tentang cara menambahkan atau memodifikasi DNS catatan, hubungi DNS penyedia Anda. Route 53 mendukung CAA catatan. Jika Route 53 adalah DNS penyedia Anda, lihat [CAAFormat](#) untuk informasi selengkapnya tentang membuat rekaman.

## AWS Certificate Manager sertifikat publik

Setelah Anda meminta sertifikat publik, Anda harus memvalidasi kepemilikan domain, seperti yang dijelaskan dalam [Validasi kepemilikan domain untuk AWS Certificate Manager sertifikat publik](#).

ACMSertifikat publik mengikuti standar X.509 dan tunduk pada batasan berikut:

- Nama: Anda harus menggunakan nama subjek DNS yang sesuai. Untuk informasi selengkapnya, lihat [Nama Domain](#).
- Algoritma: Untuk enkripsi, algoritma kunci privat sertifikat harus berupa 2048-bitRSA, ECDSA 256-bit, atau 384-bit. ECDSA
- Kedaluwarsa: Setiap sertifikat berlaku selama 13 bulan (395 hari).
- Perpanjangan: ACM upaya untuk memperbarui sertifikat pribadi secara otomatis setelah 11 bulan.

Administrator dapat menggunakan [Kebijakan Kunci ACM Bersyarat](#) untuk mengontrol cara pengguna akhir mengeluarkan sertifikat baru. Kunci bersyarat ini memungkinkan pembatasan ditempatkan pada domain, metode validasi, dan atribut lain yang terkait dengan permintaan sertifikat. Jika Anda mengalami masalah saat meminta sertifikat, lihat [Memecahkan masalah permintaan sertifikat](#).

Untuk meminta sertifikat untuk PKI penggunaan pribadi AWS Private CA, lihat [Minta sertifikat pribadi di AWS Certificate Manager](#).

## AWS Certificate Manager karakteristik dan batasan sertifikat publik

Sertifikat publik yang disediakan oleh ACM memiliki karakteristik dan batasan yang dijelaskan di bagian ini. Karakteristik ini hanya berlaku untuk sertifikat yang disediakan oleh ACM. Mereka mungkin tidak berlaku untuk [sertifikat yang diimpor](#).

### Browser dan kepercayaan aplikasi

ACMsertifikat dipercaya oleh semua browser utama termasuk Google Chrome, Microsoft Internet Explorer dan Microsoft Edge, Mozilla Firefox, dan Apple Safari. Browser yang mempercayai ACM sertifikat menampilkan ikon kunci di bilah status atau bilah alamat saat dihubungkan olehSSL/TLSke situs yang menggunakan ACM sertifikat. ACMSertifikat juga dipercaya oleh Java.



## Otoritas sertifikat dan hierarki

Sertifikat publik yang Anda minta ACM diperoleh dari [Amazon Trust Services](#), [otoritas sertifikat publik \(CA\)](#) yang dikelola Amazon. Amazon Root CAs 1 hingga 4 ditandatangani silang oleh root lama bernama Starfield G2 Root Certificate Authority - G2. Root Starfield dipercaya pada perangkat Android dimulai dengan versi Gingerbread yang lebih baru, dan oleh iOS mulai dari versi 4.1. Akar Amazon dipercaya oleh iOS mulai dari versi 11. Setiap browser, aplikasi, atau OS yang mencakup akar Amazon atau Starfield akan mempercayai sertifikat publik yang diperoleh dari ACM.

Sertifikat daun atau entitas akhir yang diterbitkan kepada ACM pelanggan memperoleh otoritas mereka dari root CA Amazon Trust Services melalui salah satu dari beberapa perantara. CAs ACM secara acak menetapkan CA perantara berdasarkan jenis sertifikat (RSA atau ECDSA) yang diminta. Karena CA perantara dipilih secara acak setelah permintaan dibuat, ACM tidak memberikan informasi CA perantara.

## Validasi Domain (DV)

ACM sertifikat adalah domain yang divalidasi. Artinya, bidang subjek ACM sertifikat mengidentifikasi nama domain dan tidak lebih. Ketika Anda meminta ACM sertifikat, Anda harus memvalidasi bahwa Anda memiliki atau mengontrol semua domain yang Anda tentukan dalam permintaan Anda. Anda dapat memvalidasi kepemilikan dengan menggunakan email atau DNS. Untuk informasi selengkapnya, silakan lihat [AWS Certificate Manager validasi email](#) dan [AWS Certificate Manager DNS validasi](#).

## Rotasi CA menengah dan akar

Untuk mempertahankan infrastruktur sertifikat yang tangguh dan gesit, Amazon dapat sewaktu-waktu memilih untuk menghentikan CA perantara tanpa pemberitahuan sebelumnya. Perubahan semacam ini tidak berdampak pada pelanggan. Untuk informasi lebih lanjut, lihat posting blog, [“Amazon memperkenalkan otoritas sertifikat menengah dinamis.”](#)

Jika Amazon menghentikan root CA, perubahan akan terjadi secepat yang diperlukan oleh keadaan. Karena dampak besar dari perubahan tersebut, Amazon akan menggunakan setiap mekanisme yang tersedia untuk memberi tahu AWS pelanggan, termasuk AWS Health Dashboard, email ke pemilik akun, dan penjangkauan ke manajer akun teknis.

## Akses firewall untuk pencabutan

Jika sertifikat entitas akhir tidak lagi dapat dipercaya, maka akan dicabut. OCSP dan CRLs merupakan mekanisme standar yang digunakan untuk memverifikasi apakah sertifikat telah dicabut atau tidak. OCSP dan CRLs merupakan mekanisme standar yang digunakan untuk

mempublikasikan informasi pencabutan. Beberapa firewall pelanggan mungkin memerlukan aturan tambahan untuk memungkinkan mekanisme ini berfungsi.

Contoh pola URL wildcard berikut dapat digunakan untuk mengidentifikasi lalu lintas pencabutan. Wildcard asterisk (\*) mewakili satu atau lebih karakter alfanumerik, tanda tanya (?) mewakili karakter alfanumerik tunggal, dan tanda hash (#) mewakili angka.

- OCSP

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

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

- CRL

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

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

## Algoritma kunci

Sertifikat harus menentukan algoritma dan ukuran kunci. Saat ini, algoritma kunci publik berikut RSA dan Elliptic Curve Digital Signature Algorithm (ECDSA) didukung oleh ACM. ACM dapat meminta masalah sertifikat baru menggunakan algoritma yang ditandai dengan tanda bintang (\*). Algoritma yang tersisa hanya didukung untuk sertifikat yang [diimpor](#).

### Note

Saat Anda meminta PKI sertifikat pribadi yang ditandatangani oleh CA dari AWS Private CA, keluarga algoritma penandatanganan yang ditentukan (RSA atau ECDSA) harus cocok dengan keluarga algoritme kunci rahasia CA.

- RSA1024 bit () RSA\_1024
- RSA2048 bit (RSA\_2048) \*
- RSA3072 bit () RSA\_3072
- RSA4096 bit () RSA\_4096
- ECDSA256 bit (EC\_prime256v1) \*
- ECDSA384 bit (EC\_secp384r1) \*
- ECDSA521 bit () EC\_secp521r1

ECDSA kunci lebih kecil, menawarkan keamanan yang sebanding dengan RSA kunci tetapi dengan efisiensi komputasi yang lebih besar. Namun, ECDSA tidak didukung oleh semua klien jaringan. Tabel berikut, diadaptasi dari [NIST](#), menunjukkan kekuatan keamanan yang representatif dari RSA dan ECDSA dengan kunci berbagai ukuran. Semua nilai dalam bit.

Membandingkan keamanan untuk algoritma dan kunci

Kekuatan keamanan	RSA ukuran kunci	ECDSA ukuran kunci
128	3072	256
192	7680	384
256	15360	521

Kekuatan keamanan, dipahami sebagai kekuatan 2, terkait dengan jumlah tebakan yang diperlukan untuk memecahkan enkripsi. Misalnya, kunci 3072-bit dan RSA kunci 256-bit ECDSA dapat diambil dengan tidak lebih dari 2<sup>128</sup> tebakan.

Untuk informasi yang membantu Anda memilih algoritme, lihat AWS posting blog [Cara mengevaluasi dan menggunakan ECDSA sertifikat di AWS Certificate Manager](#).

#### Important

Perhatikan bahwa [layanan terintegrasi](#) hanya memungkinkan algoritma dan ukuran kunci yang mereka dukung untuk dikaitkan dengan sumber daya mereka. Selanjutnya, dukungan mereka berbeda tergantung pada apakah sertifikat diimpor ke dalam IAM atau ke ACM. Untuk informasi selengkapnya, lihat dokumentasi untuk setiap layanan.

- Untuk Elastic Load Balancing, lihat [HTTPSListener untuk Application Load Balancer](#) Anda.
- Untuk CloudFront, lihat [Didukung SSL/TLS Protokol dan Cipher](#).

## Pembaruan dan Penerapan Terkelola

ACM mengelola proses memperbarui ACM sertifikat dan penyediaan sertifikat setelah diperpanjang. Perpanjangan otomatis dapat membantu Anda menghindari waktu henti karena sertifikat yang tidak dikonfigurasi, dicabut, atau kedaluwarsa secara tidak benar. Untuk informasi selengkapnya, lihat [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#).

## Beberapa Nama Domain

Setiap ACM sertifikat harus menyertakan setidaknya satu nama domain yang memenuhi syarat (FQDN), dan Anda dapat menambahkan nama tambahan jika Anda mau. Misalnya, ketika Anda membuat ACM sertifikat untuk `www.example.com`, Anda juga dapat menambahkan nama `www.example.net` jika pelanggan dapat mencapai situs Anda dengan menggunakan salah satu nama. Ini juga berlaku untuk domain telanjang (juga dikenal sebagai zona puncak atau domain telanjang). Artinya, Anda dapat meminta ACM sertifikat untuk `www.example.com` dan menambahkan nama `example.com`. Untuk informasi selengkapnya, lihat [AWS Certificate Manager sertifikat publik](#).

## Kode Punycode

Persyaratan [Punycode](#) berikut yang berkaitan dengan [Nama Domain Internasional](#) harus dipenuhi:

1. Nama domain yang dimulai dengan pola “<character><character>--” harus cocok dengan “xn--”.
2. Nama domain yang diawali dengan “xn--” juga harus merupakan Nama Domain Internasional yang valid.

## Contoh Punycode

Nama Domain	Memenu #1	Memenu #2	Diizinkan	Catatan
<code>contoh.com</code>	tidak berlaku	T/A	✓	Tidak dimulai dengan “<character><character>--”
<code>a--example.com</code>	tidak berlaku	T/A	✓	Tidak dimulai dengan “<character><character>--”
<code>abc--example.com</code>	tidak berlaku	T/A	✓	Tidak dimulai dengan “<character><character>--”
<code>xn--xyz.com</code>	Ya	Ya	✓	Nama Domain Internasional yang Valid (diselesaikan ke <code>.com</code> )
<code>xn--example.com</code>	Ya	Tidak	✗	Bukan Nama Domain Internasionalisasi yang valid

Nama Domain	Memenuhkan #1	Memenuhi #2	Diizinkan	Catatan
ab--example.com	Tidak	Tidak	X	Harus dimulai dengan "xn--"

## Periode Validitas

Masa berlaku ACM sertifikat adalah 13 bulan (395 hari).

## Nama Wildcard

ACM memungkinkan Anda menggunakan tanda bintang (\*) di nama domain untuk membuat ACM sertifikat yang berisi nama wildcard yang dapat melindungi beberapa situs dalam domain yang sama. Misalnya, \*.example.com melindungi www.example.com dan images.example.com.

### Note

Saat Anda meminta sertifikat wildcard, tanda bintang (\*) harus berada di posisi paling kiri dari nama domain dan hanya dapat melindungi satu tingkat subdomain. Misalnya, \*.example.com dapat melindungi login.example.com dan test.example.com, tetapi tidak dapat melindungi test.login.example.com. Perhatikan juga bahwa \*.example.com melindungi hanya subdomain dari example.com, itu tidak melindungi domain telanjang atau apex (.example.com). Namun, Anda dapat meminta sertifikat yang melindungi domain kosong atau apex dan subdomainnya dengan menentukan beberapa nama domain dalam permintaan Anda. Misalnya, Anda dapat meminta sertifikat yang melindungi example.com dan \*.example.com.

## Batasan

Batasan berikut berlaku untuk sertifikat publik.

- ACM tidak menyediakan sertifikat validasi diperpanjang (EV) atau sertifikat validasi organisasi (OV).
- ACM tidak memberikan sertifikat untuk apa pun selain TLS protokol SSL/TLS.
- Anda tidak dapat menggunakan ACM sertifikat untuk enkripsi email.

- ACM saat ini tidak mengizinkan Anda untuk memilih keluar dari [perpanjangan sertifikat terkelola](#) untuk ACM sertifikat. Selain itu, perpanjangan terkelola tidak tersedia untuk sertifikat yang Anda impor ACM.
- Anda tidak dapat meminta sertifikat untuk nama domain milik Amazon seperti yang diakhiri dengan amazonaws.com, cloudfront.net, atau elasticbeanstalk.com.
- Anda tidak dapat mengunduh kunci pribadi untuk ACM sertifikat.
- Anda tidak dapat langsung menginstal ACM sertifikat di situs web atau aplikasi Amazon Elastic Compute Cloud (Amazon EC2) Anda. Namun, Anda dapat menggunakan sertifikat Anda dengan layanan terintegrasi apa pun. Untuk informasi selengkapnya, lihat [Layanan terintegrasi dengan ACM](#).
- Kecuali Anda memilih untuk memilih keluar, ACM sertifikat tepercaya publik secara otomatis dicatat dalam setidaknya dua database transparansi sertifikat. Saat ini Anda tidak dapat menggunakan konsol untuk memilih keluar. Anda harus menggunakan AWS CLI atau ACM API. Untuk informasi selengkapnya, lihat [Memilih keluar dari pencatatan transparansi sertifikat](#). Untuk informasi umum tentang log transparansi, lihat [Pencatatan Transparansi Sertifikat](#).

## Minta sertifikat publik di AWS Certificate Manager

Bagian berikut membahas cara menggunakan ACM konsol atau AWS CLI untuk meminta ACM sertifikat publik.

Topik

- [Minta sertifikat publik menggunakan konsol](#)
- [Meminta sertifikat publik menggunakan CLI](#)

### Minta sertifikat publik menggunakan konsol

Untuk meminta sertifikat ACM publik (konsol)

1. Masuk ke AWS Konsol Manajemen dan buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>.

Pilih Minta sertifikat.

2. Di bagian Nama domain, ketikkan nama domain Anda.

Anda dapat menggunakan nama domain yang sepenuhnya memenuhi syarat (FQDN), seperti **www.example.com**, atau nama domain telanjang atau apex seperti **example.com**. Anda juga dapat menggunakan tanda bintang (\*) sebagai kartu liar di posisi paling kiri untuk melindungi beberapa nama situs di domain yang sama. Misalnya, **\*.example.com** melindungi **corp.example.com**, dan **images.example.com**. Nama kartu liar akan muncul di bidang Subjek dan di ekstensi Nama Alternatif Subjek sertifikat. ACM

Saat Anda meminta sertifikat kartu liar, tanda bintang (\*) harus berada di posisi paling kiri dari nama domain dan hanya dapat melindungi satu tingkat subdomain. Misalnya, **\*.example.com** dapat melindungi **login.example.com**, dan **test.example.com**, tetapi tidak dapat melindungi **test.login.example.com**. Perhatikan juga bahwa **\*.example.com** melindungi hanya subdomain dari **example.com**, itu tidak melindungi domain telanjang atau apex (**example.com**). Untuk melindungi keduanya, lihat langkah selanjutnya.

#### Note

Sesuai dengan [RFC5280](#), panjang nama domain (secara teknis, Nama Umum) yang Anda masukkan dalam langkah ini tidak boleh melebihi 64 oktet (karakter), termasuk periode. Setiap Nama Alternatif Subjek berikutnya (SAN) yang Anda berikan, seperti pada langkah berikutnya, dapat mencapai panjang hingga 253 oktet.

Untuk menambahkan nama lain, pilih Tambahkan nama lain ke sertifikat ini dan ketikkan nama di kotak teks. Ini berguna untuk melindungi domain telanjang atau puncak (seperti **example.com**) dan subdomainnya seperti **\*.example.com**.

3. Di bagian Metode validasi, pilih DNSvalidasi — direkomendasikan atau validasi Email, tergantung pada kebutuhan Anda.

#### Note

Jika Anda dapat mengedit DNS konfigurasi Anda, kami sarankan Anda menggunakan validasi DNS domain daripada validasi email. DNSvalidasi memiliki banyak manfaat dibandingkan validasi email. Lihat [AWS Certificate Manager DNSvalidasi](#).

Sebelum ACM mengeluarkan sertifikat, itu memvalidasi bahwa Anda memiliki atau mengontrol nama domain dalam permintaan sertifikat Anda. Anda dapat menggunakan validasi email atau DNS validasi.

Jika Anda memilih validasi email, ACM mengirimkan email validasi ke domain yang Anda tentukan di bidang nama domain. Jika Anda menentukan domain validasi, ACM kirimkan email ke domain validasi tersebut. Untuk informasi selengkapnya tentang validasi email, lihat [AWS Certificate Manager validasi email](#).

Jika Anda menggunakan DNS validasi, Anda cukup menambahkan CNAME catatan yang disediakan oleh ACM ke DNS konfigurasi Anda. Untuk informasi selengkapnya tentang DNS validasi, lihat [AWS Certificate Manager DNSvalidasi](#).

4. Di bagian Algoritma kunci, pilih algoritma.
5. Di halaman Tag, Anda dapat menandai sertifikat Anda secara opsional. Tag adalah pasangan nilai kunci yang berfungsi sebagai metadata untuk mengidentifikasi dan mengatur AWS sumber daya. Untuk daftar parameter ACM tag dan petunjuk tentang cara menambahkan tag ke sertifikat setelah pembuatan, lihat [Tag AWS Certificate Manager sumber daya](#).

Setelah selesai menambahkan tag, pilih Permintaan.

6. Setelah permintaan diproses, konsol mengembalikan Anda ke daftar sertifikat Anda, di mana informasi tentang sertifikat baru ditampilkan.

Sertifikat memasuki status Validasi tertunda setelah diminta, kecuali jika gagal karena salah satu alasan yang diberikan dalam topik pemecahan masalah Permintaan [sertifikat](#) gagal. ACM melakukan upaya berulang untuk memvalidasi sertifikat selama 72 jam dan kemudian habis waktu. Jika sertifikat menunjukkan status Gagal atau Waktu validasi habis, hapus permintaan, perbaiki masalah dengan [DNSvalidasi atau validasi Email, dan coba lagi](#). Jika validasi berhasil, sertifikat memasuki status Diterbitkan.

#### Note

Bergantung pada bagaimana Anda memesan daftar, sertifikat yang Anda cari mungkin tidak segera terlihat. Anda dapat mengklik segitiga hitam di sebelah kanan untuk mengubah urutan. Anda juga dapat menavigasi melalui beberapa halaman sertifikat menggunakan nomor halaman di kanan atas.



## Meminta sertifikat publik menggunakan CLI

Gunakan perintah [request-certificate](#) untuk meminta ACM sertifikat publik baru pada baris perintah. Nilai opsional untuk metode validasi adalah DNS dan EMAIL. Nilai opsional untuk algoritma kunci adalah RSA\_2048 (default jika parameter tidak disediakan secara eksplisit), EC\_Prime256v1, dan EC\_secp384R1.

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

Perintah ini menampilkan Amazon Resource Name (ARN) dari sertifikat publik baru Anda.

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

## Validasi kepemilikan domain untuk AWS Certificate Manager sertifikat publik

Sebelum otoritas sertifikat Amazon (CA) dapat mengeluarkan sertifikat untuk situs Anda, AWS Certificate Manager (ACM) harus membuktikan bahwa Anda memiliki atau mengontrol semua nama domain yang Anda tentukan dalam permintaan Anda. Anda dapat memilih untuk membuktikan kepemilikan Anda dengan validasi Sistem Nama Domain (DNS) atau dengan validasi email pada saat Anda meminta sertifikat.

### Note

Validasi hanya berlaku untuk sertifikat tepercaya publik yang dikeluarkan oleh ACM. ACM tidak memvalidasi kepemilikan domain untuk [sertifikat yang diimpor](#) atau untuk sertifikat yang ditandatangani oleh CA pribadi. ACM tidak dapat memvalidasi sumber daya di [zona host VPC pribadi](#) Amazon atau domain pribadi lainnya. Untuk informasi selengkapnya, lihat [Memecahkan masalah validasi sertifikat](#).

Secara umum, kami merekomendasikan penggunaan DNS validasi melalui validasi email karena alasan berikut:

- Jika Anda menggunakan Amazon Route 53 untuk mengelola DNS catatan publik Anda, Anda dapat memperbarui catatan Anda secara ACM langsung.
- ACM secara otomatis memperbarui sertifikat DNS yang divalidasi selama sertifikat tetap digunakan dan DNS catatan sudah ada.
- Untuk diperpanjang, sertifikat yang divalidasi email memerlukan tindakan oleh pemilik domain. ACM mulai mengirimkan pemberitahuan perpanjangan 45 hari sebelum kedaluwarsa. Pemberitahuan ini masuk ke satu atau lebih dari lima alamat administrator umum domain. Notifikasi berisi tautan yang dapat diklik pemilik domain untuk perpanjangan yang mudah. Setelah semua domain yang terdaftar divalidasi, ACM mengeluarkan sertifikat yang diperbarui dengan hal yang sama. ARN

Jika Anda tidak memiliki otorisasi untuk mengedit DNS database domain Anda, Anda harus menggunakan [validasi email](#) sebagai gantinya.

#### Note

Setelah Anda membuat sertifikat dengan validasi email, Anda tidak dapat beralih untuk memvalidasinya dengan DNS. Untuk menggunakan DNS validasi, hapus sertifikat dan kemudian buat yang baru yang menggunakan DNS validasi.

#### Topik

- [AWS Certificate Manager DNS validasi](#)
- [AWS Certificate Manager validasi email](#)


## AWS Certificate Manager DNS validasi

Domain Name System (DNS) adalah layanan direktori untuk sumber daya yang terhubung ke jaringan. DNS Penyedia Anda mengelola database yang berisi catatan yang menentukan domain Anda. Ketika Anda memilih DNS validasi, ACM memberi Anda satu atau beberapa CNAME catatan yang harus ditambahkan ke database ini. Catatan ini berisi pasangan kunci-nilai unik yang berfungsi sebagai bukti bahwa Anda mengontrol domain.

 Note

Setelah Anda membuat sertifikat dengan validasi email, Anda tidak dapat beralih untuk memvalidasinya dengan DNS. Untuk menggunakan DNS validasi, hapus sertifikat dan kemudian buat yang baru yang menggunakan DNS validasi.

Misalnya, jika Anda meminta sertifikat untuk `example.com` domain dengan `www.example.com` nama tambahan, ACM buat dua CNAME catatan untuk Anda. Setiap catatan, yang dibuat khusus untuk domain dan akun Anda, berisi nama dan nilai. Nilai adalah alias yang menunjuk ke AWS domain yang ACM digunakan untuk memperbarui sertifikat Anda secara otomatis. CNAME catatan harus ditambahkan ke DNS database Anda hanya sekali. ACM secara otomatis memperbarui sertifikat Anda selama sertifikat digunakan dan CNAME catatan Anda tetap ada.

 Important

Jika Anda tidak menggunakan Amazon Route 53 untuk mengelola DNS catatan publik Anda, hubungi DNS penyedia Anda untuk mengetahui cara menambahkan catatan. Jika Anda tidak memiliki otoritas untuk mengedit DNS database domain Anda, Anda harus menggunakan [validasi email](#) sebagai gantinya.

Tanpa perlu mengulang validasi, Anda dapat meminta ACM sertifikat tambahan untuk nama domain yang sepenuhnya memenuhi syarat (FQDN) selama CNAME catatan tetap ada. Artinya, Anda dapat membuat sertifikat pengganti yang memiliki nama domain yang sama, atau sertifikat yang mencakup subdomain yang berbeda. Karena token CNAME validasi berfungsi untuk apa pun AWS Wilayah, Anda dapat membuat ulang sertifikat yang sama di beberapa Wilayah. Anda juga dapat mengganti sertifikat yang dihapus.

Anda dapat menghentikan perpanjangan otomatis baik dengan menghapus sertifikat dari AWS layanan yang terkait atau dengan menghapus CNAME catatan. Jika Route 53 bukan DNS penyedia Anda, hubungi penyedia Anda untuk mengetahui cara menghapus catatan. Jika Route 53 adalah penyedia Anda, lihat [Menghapus Kumpulan Rekaman Sumber Daya](#) di Panduan Pengembang Route 53. Untuk informasi selengkapnya tentang perpanjangan sertifikat terkelola, lihat [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#).

**Note**

CNAME resolusi akan gagal jika lebih dari lima CNAMEs dirantai bersama dalam DNS konfigurasi Anda. Jika Anda memerlukan rantai yang lebih panjang, sebaiknya gunakan [validasi email](#).

## Bagaimana CNAME catatan untuk ACM bekerja

**Note**

Bagian ini untuk pelanggan yang tidak menggunakan Route 53 sebagai DNS penyedia mereka.

Jika Anda tidak menggunakan Route 53 sebagai DNS penyedia Anda, Anda perlu memasukkan CNAME catatan yang disediakan secara manual ACM ke dalam database penyedia Anda, biasanya melalui situs web. CNAME catatan digunakan untuk sejumlah tujuan, termasuk sebagai mekanisme pengalihan dan sebagai wadah untuk metadata khusus vendor. Untuk ACM, catatan ini memungkinkan validasi kepemilikan domain awal dan perpanjangan sertifikat otomatis yang sedang berlangsung.

Tabel berikut menunjukkan contoh CNAME catatan untuk enam nama domain. Setiap pasangan Record Name - Record Value berfungsi untuk mengautentikasi kepemilikan nama domain.

Dalam tabel, perhatikan bahwa dua pasangan Record Name - Record Value pertama adalah sama. Ini menggambarkan bahwa untuk domain wild-card, seperti `*.example.com`, string yang dibuat oleh ACM sama dengan yang dibuat untuk domain dasarnya, `.example.com`. Jika tidak, Nama Rekaman dan Nilai Rekaman yang dipasangkan berbeda untuk setiap nama domain.

### Contoh CNAME catatan

Nama domain	Nama Rekam	Nilai Rekam	Komentar
<code>*.example.com</code>	<code>_<b>x1</b>.contoh.com.</code>	<code>_<b>x2</b>.acm-validations.a ws.</code>	Identik
<code>contoh.com</code>	<code>_<b>x1</b>.contoh.com.</code>	<code>_<b>x2</b>.acm-validations.a ws.</code>	

Nama domain	Nama Rekam	Nilai Rekam	Komentar
www.example.com	<u>_x3</u> .www.example.com.	<u>_x4</u> .acm-validations.aws.	Unik
host.example.com	<u>_x5</u> .host.example.com.	<u>_x6</u> .acm-validations.aws.	Unik
subdomain.contoh.com	<u>_x7</u> .subdomain.example.com.	<u>_x8</u> .acm-validations.aws.	Unik
host.subdomain.example.com	<u>_x9</u> .host.subdomain.example.com.	<u>_x10</u> .acm-validations.aws.	Unik

Bagian *xN* nilai mengikuti garis bawah (  ) adalah string panjang yang dihasilkan oleh ACM. Misalnya,

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

adalah perwakilan dari Nama Rekaman yang dihasilkan. Nilai Rekaman terkait mungkin

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

untuk DNS catatan yang sama.

#### Note

Jika DNS penyedia Anda tidak mendukung CNAME nilai dengan garis bawah utama, lihat [Memecahkan Masalah DNS Validasi](#).

Saat Anda meminta sertifikat dan menentukan DNS validasi, ACM berikan CNAME informasi dalam format berikut:

Nama Domain	Nama Rekam	Jenis Rekaman	Nilai Rekam
contoh.com	<u>_a79865eb4cd1a6ab990a45779b4e0b96</u> .example.com.	CNAME	

Nama Domain	Nama Rekam	Jenis Rekaman	Nilai Rekam
			<code>_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.</code>

Nama Domain adalah FQDN yang terkait dengan sertifikat. Nama Rekam mengidentifikasi catatan secara unik, berfungsi sebagai kunci dari pasangan kunci-nilai. Record Value berfungsi sebagai nilai pasangan kunci-nilai.

Ketiga nilai ini (Nama Domain, Nama Rekam, dan Nilai Rekam) harus dimasukkan ke dalam bidang yang sesuai dari antarmuka web DNS penyedia Anda untuk menambahkan DNS catatan. Penyedia tidak konsisten dalam penanganan bidang nama rekaman (atau hanya “nama”). Dalam beberapa kasus, Anda diharapkan untuk menyediakan seluruh string seperti yang ditunjukkan di atas. Penyedia lain secara otomatis menambahkan nama domain ke string apa pun yang Anda masukkan, artinya (dalam contoh ini) yang hanya boleh Anda masukkan

```
_a79865eb4cd1a6ab990a45779b4e0b96
```

ke bidang nama. Jika Anda salah menebak tentang hal ini, dan memasukkan nama rekaman yang berisi nama domain (seperti `.example.com`), Anda mungkin berakhir dengan yang berikut:

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

Validasi akan gagal dalam kasus ini. Akibatnya, Anda harus mencoba menentukan terlebih dahulu jenis input yang diharapkan penyedia Anda.

## Menyiapkan DNS validasi

Bagian ini menjelaskan cara mengonfigurasi sertifikat publik untuk menggunakan DNS validasi.

Untuk mengatur DNS validasi di konsol

### Note

Prosedur ini mengasumsikan bahwa Anda telah membuat setidaknya satu sertifikat dan bahwa Anda bekerja di AWS Wilayah tempat Anda membuatnya. Jika Anda mencoba membuka konsol dan melihat layar penggunaan pertama, atau Anda berhasil membuka

konsol dan tidak melihat sertifikat Anda dalam daftar, konfirmasi bahwa Anda telah menentukan Wilayah yang benar.

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/>.
2. Dalam daftar sertifikat, pilih ID Sertifikat sertifikat dengan status Validasi tertunda yang ingin Anda konfigurasi. Ini membuka halaman detail untuk sertifikat.
3. Di bagian Domain, lengkapi salah satu dari dua prosedur berikut:
  - a. (Opsional) Validasi dengan Route 53.

Tombol Buat catatan aktif di Route 53 muncul jika kondisi berikut benar:

- Anda menggunakan Route 53 sebagai DNS penyedia Anda.
- Anda memiliki izin untuk menulis ke zona yang dihosting oleh Route 53.
- Anda FQDN belum divalidasi.

#### Note

Jika Anda sebenarnya menggunakan Route 53 tetapi tombol Buat catatan di Route 53 hilang atau dinonaktifkan, lihat [ACMKonsol tidak menampilkan tombol "Buat catatan di Rute 53"](#).


Pilih tombol Buat catatan di Route 53, lalu pilih Buat catatan. Halaman status Sertifikat harus terbuka dengan spanduk status yang melaporkan DNSCatatan yang berhasil dibuat.

Sertifikat baru Anda mungkin terus menampilkan status validasi Tertunda hingga 30 menit.

#### Tip

Anda tidak dapat meminta secara terprogram yang secara ACM otomatis membuat catatan Anda di Route 53. Namun, Anda dapat membuat AWS CLI atau API panggil ke Route 53 untuk membuat catatan di DNS database Route 53. Untuk informasi selengkapnya tentang kumpulan rekaman Route 53, lihat [Bekerja dengan Kumpulan Rekaman Sumber Daya](#).

- b. (Opsional) Jika Anda tidak menggunakan Route 53 sebagai DNS penyedia Anda, Anda harus mengambil CNAME informasi dan menambahkannya ke DNS database Anda. Pada halaman detail untuk sertifikat baru, Anda dapat melakukan ini dengan salah satu dari dua cara:
- Salin CNAME komponen yang ditampilkan di bagian Domain. Informasi ini perlu ditambahkan secara manual ke DNS database Anda.
  - Atau, pilih Ekspor ke CSV. Informasi dalam file yang dihasilkan perlu ditambahkan secara manual ke DNS database Anda.

 Important

Untuk menghindari masalah validasi, tinjau [Bagaimana CNAME catatan untuk ACM bekerja](#) sebelum menambahkan informasi ke database DNS penyedia Anda. Jika Anda mengalami masalah, lihat [Memecahkan masalah validasi DNS](#).

Jika ACM tidak dapat memvalidasi nama domain dalam waktu 72 jam dari waktu itu menghasilkan CNAME nilai untuk Anda, ACM ubah status sertifikat menjadi validasi habis waktu. Alasan yang paling mungkin untuk hasil ini adalah bahwa Anda tidak berhasil memperbarui DNS konfigurasi Anda dengan nilai yang ACM dihasilkan. Untuk memperbaiki masalah ini, Anda harus meminta sertifikat baru setelah meninjau CNAME instruksi.

## AWS Certificate Manager validasi email

Sebelum otoritas sertifikat Amazon (CA) dapat mengeluarkan sertifikat untuk situs Anda, AWS Certificate Manager (ACM) harus memverifikasi bahwa Anda memiliki atau mengontrol semua domain yang Anda tentukan dalam permintaan Anda. Anda dapat melakukan verifikasi menggunakan email atau DNS. Topik ini membahas validasi email.

Jika Anda mengalami masalah dalam menggunakan validasi email, lihat [Memecahkan masalah validasi email](#).

### Cara kerja validasi email

ACM mengirimkan pesan email validasi ke lima email sistem umum berikut untuk setiap domain. Atau, Anda dapat menentukan superdomain sebagai domain validasi jika Anda ingin menerima email ini di domain itu sebagai gantinya. Subdomain apa pun hingga alamat situs web minimal valid, dan



digunakan sebagai domain untuk alamat email sebagai akhiran setelahnya. @ Misalnya, Anda dapat menerima email ke `admin@example.com` jika Anda menentukan `example.com` sebagai domain validasi untuk `subdomain.example.com`.

- `administrator @your_domain_name`
- `tuan rumah @your_domain_name`
- `kepala pos @your_domain_name`
- `webmaster @your_domain_name`
- `admin @your_domain_name`

Untuk membuktikan bahwa Anda memiliki domain, Anda harus memilih tautan validasi yang disertakan dalam email ini. ACM juga mengirimkan email validasi ke alamat yang sama untuk memperbarui sertifikat ketika sertifikat 45 hari dari kedaluwarsa.

Validasi email untuk permintaan sertifikat multi-domain menggunakan ACM API atau CLI menghasilkan pesan email yang dikirim oleh setiap domain yang diminta, bahkan jika permintaan tersebut menyertakan subdomain domain lain dalam permintaan. Pemilik domain perlu memvalidasi pesan email untuk masing-masing domain ini sebelum ACM dapat mengeluarkan sertifikat.

Pengecualian untuk proses ini

Jika Anda meminta ACM sertifikat untuk nama domain yang dimulai dengan `www` atau tanda bintang wild-card (\*), ACM hapus tanda depan `www` atau tanda bintang dan kirim email ke alamat administratif. Alamat ini dibentuk oleh `admin@`, `administrator@`, `hostmaster@`, `postmaster@`, dan `webmaster@` yang tertunda ke bagian sisa nama domain. Misalnya, jika Anda meminta ACM sertifikat untuk `www.example.com`, email dikirim ke `admin@example.com` dan bukan ke `admin@www.example.com`. Demikian juga, jika Anda meminta ACM sertifikat untuk `*.test.example.com`, email dikirim ke `admin@test.example.com`. Alamat administrasi umum yang tersisa dibentuk dengan cara yang sama.

#### Important

Mulai Juni 2024, ACM tidak lagi mendukung validasi email baru melalui alamat WHOIS kontak. Untuk sertifikat yang ada, mulai Oktober 2024, ACM tidak akan mengirimkan pemberitahuan perpanjangan ke alamat kontak domain. WHOIS ACM akan terus mengirim email validasi ke lima alamat sistem umum untuk domain yang diminta. Untuk detail

selengkapnya, lihat [AWS Certificate Manager akan menghentikan WHOIS pencarian untuk sertifikat yang divalidasi email](#)

## Pertimbangan

Perhatikan pertimbangan berikut tentang validasi email.

- Anda memerlukan alamat email yang berfungsi yang terdaftar di domain Anda untuk menggunakan validasi email. Prosedur untuk menyiapkan alamat email berada di luar cakupan panduan ini.
- Validasi hanya berlaku untuk sertifikat tepercaya publik yang dikeluarkan oleh ACM. ACM tidak memvalidasi kepemilikan domain untuk [sertifikat yang diimpor](#) atau untuk sertifikat yang ditandatangani oleh CA pribadi. ACM tidak dapat memvalidasi sumber daya di [zona host VPC pribadi](#) Amazon atau domain pribadi lainnya. Untuk informasi selengkapnya, lihat [Memecahkan masalah validasi sertifikat](#).
- Setelah Anda membuat sertifikat dengan validasi email, Anda tidak dapat beralih untuk memvalidasinya dengan DNS. Untuk menggunakan DNS validasi, hapus sertifikat dan kemudian buat yang baru yang menggunakan DNS validasi.

## Kedaluwarsa dan perpanjangan sertifikat

ACM sertifikat berlaku selama 13 bulan (395 hari). Memperpanjang sertifikat memerlukan tindakan oleh pemilik domain. ACM mulai mengirimkan pemberitahuan perpanjangan ke alamat email yang terkait dengan domain 45 hari sebelum kedaluwarsa. Notifikasi berisi tautan yang dapat diklik pemilik domain untuk perpanjangan. Setelah semua domain yang terdaftar divalidasi, ACM mengeluarkan sertifikat yang diperbarui dengan hal yang sama. ARN

### (Opsional) Kirim ulang email validasi

Setiap email validasi berisi token yang dapat Anda gunakan untuk menyetujui permintaan sertifikat. Namun, karena email validasi yang diperlukan untuk proses persetujuan dapat diblokir oleh filter spam atau hilang saat transit, token secara otomatis kedaluwarsa setelah 72 jam. Jika Anda tidak menerima email asli atau token telah kedaluwarsa, Anda dapat meminta agar email tersebut di-resent. Untuk informasi tentang cara mengirim ulang email validasi, lihat [Kirim ulang email validasi](#)

Untuk masalah terus-menerus dengan validasi email, lihat [Memecahkan masalah validasi email](#) bagian di [Memecahkan masalah dengan AWS Certificate Manager](#).

## Mengotomatiskan AWS Certificate Manager validasi email

ACMSertifikat yang divalidasi email biasanya memerlukan tindakan manual oleh pemilik domain. Organizations yang berurusan dengan sejumlah besar sertifikat email yang divalidasi mungkin lebih memilih untuk membuat parser yang dapat mengotomatiskan tanggapan yang diperlukan. Untuk membantu pelanggan menggunakan validasi email, informasi di bagian ini menjelaskan template yang digunakan untuk pesan email validasi domain dan alur kerja yang terlibat dalam menyelesaikan proses validasi.

### Templat email validasi

Pesan email validasi memiliki salah satu dari dua format berikut, tergantung pada apakah sertifikat baru diminta atau sertifikat yang ada sedang diperbarui. Konten string yang disorot harus diganti dengan nilai yang spesifik untuk domain yang divalidasi.

### Memvalidasi sertifikat baru

#### Teks templat email:

```
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

## Memvalidasi sertifikat untuk perpanjangan

### Teks templat email:

Greetings from Amazon Web Services,

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

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

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

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

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

Sincerely,  
Amazon Web Services

--

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

This message produced and distributed by Amazon Web Services, Inc.,

410 Terry Ave. North, Seattle, WA 98109-5210.

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

Setelah Anda menerima pesan validasi baru dari AWS, kami menyarankan Anda menggunakannya sebagai template yang paling up-to-date dan otoritatif untuk parser Anda. Pelanggan dengan pengurai pesan yang dirancang sebelum November 2020, harus memperhatikan perubahan berikut yang mungkin telah dilakukan pada templat:

- Baris subjek email sekarang berbunyi `Certificate request for domain name` bukannya `"Certificate approval for domain name"`.
- Sekarang AWS account ID disajikan tanpa tanda hubung atau tanda hubung.
- Certificate Identifier Sekarang menyajikan seluruh sertifikat ARN alih-alih formulir yang dipersingkat, misalnya, `arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369` bukan `3b4d78e1-0882-4f51-954a-298ee44ff369`.
- Persetujuan sertifikat URL sekarang berisi `acm-certificates.amazon.com` alih-alih `certificates.amazon.com`.
- Formulir persetujuan dibuka dengan mengklik persetujuan sertifikat URL sekarang berisi tombol persetujuan. Nama tombol persetujuan div sekarang `approve-button` bukan `approval_button`.
- Pesan validasi untuk sertifikat yang baru diminta dan sertifikat pembaruan memiliki format email yang sama.

## Alur kerja validasi

Bagian ini memberikan informasi tentang alur kerja pembaruan untuk sertifikat yang divalidasi email.

- Saat ACM konsol memproses permintaan sertifikat multi-domain, konsol akan mengirimkan pesan email validasi ke nama domain atau domain validasi yang Anda tentukan saat meminta sertifikat publik. Pemilik domain perlu memvalidasi pesan email untuk setiap domain sebelum ACM dapat mengeluarkan sertifikat. Untuk informasi selengkapnya, lihat [Menggunakan Email untuk Memvalidasi Kepemilikan Domain](#).
- Validasi email untuk permintaan sertifikat multi-domain menggunakan ACM API atau CLI menghasilkan pesan email yang dikirim oleh setiap domain yang diminta, bahkan jika permintaan tersebut menyertakan subdomain domain lain dalam permintaan. Pemilik domain perlu

memvalidasi pesan email untuk masing-masing domain ini sebelum ACM dapat mengeluarkan sertifikat.

Jika Anda mengirim ulang email untuk sertifikat yang ada melalui ACM konsol, email akan dikirim ke domain validasi yang ditentukan dalam permintaan sertifikat asli, atau domain yang tepat jika tidak ada domain validasi yang ditentukan. Untuk menerima email validasi di domain yang berbeda, Anda dapat meminta sertifikat baru, menentukan domain validasi yang ingin Anda gunakan untuk validasi. Atau, Anda dapat memanggil [ResendValidationEmail](#) dengan `ValidationDomain` parameter menggunakan API, SDK, atau CLI. Namun, domain validasi yang ditentukan dalam `ResendValidationEmail` permintaan hanya digunakan untuk panggilan tersebut dan tidak disimpan ke sertifikat Amazon Resource Name (ARN) untuk email validasi future. Anda harus menelepon `ResendValidationEmail` setiap kali Anda ingin menerima email validasi pada nama domain yang tidak ditentukan dalam permintaan sertifikat asli.

#### Note

Sebelum November 2020, pelanggan hanya perlu memvalidasi domain apex dan ACM akan mengeluarkan sertifikat yang juga mencakup subdomain apa pun. Pelanggan dengan pengurai pesan yang dirancang sebelum waktu itu harus mencatat perubahan pada alur kerja validasi email.

- Dengan ACM API atau CLI, Anda dapat memaksa semua pesan email validasi agar permintaan sertifikat multi-domain dikirim ke domain apex. Dalam API, gunakan `DomainValidationOptions` parameter [RequestCertificate](#) tindakan untuk menentukan nilai untuk `ValidationDomain`, yang merupakan anggota dari [DomainValidationOption](#) tipe. Dalam CLI, gunakan `--domain-validation-options` parameter perintah [request-certificate](#) untuk menentukan nilai untuk `ValidationDomain`


## Sertifikat pribadi di AWS Certificate Manager

Jika Anda memiliki akses ke CA pribadi yang ada yang dibuat oleh AWS Private CA, AWS Certificate Manager (ACM) dapat meminta sertifikat yang cocok untuk digunakan dalam infrastruktur kunci pribadi Anda (PKI). CA dapat berada di akun Anda atau dibagikan dengan Anda oleh akun lain. Untuk informasi tentang membuat CA pribadi, lihat [Membuat Otoritas Sertifikat Pribadi](#).

Sertifikat yang ditandatangani oleh CA pribadi tidak dipercaya secara default, dan ACM tidak mendukung segala bentuk validasi untuk mereka. Akibatnya, administrator harus mengambil tindakan untuk menginstalnya di toko kepercayaan klien organisasi Anda.

ACMSertifikat privat mengikuti standar X.509 dan tunduk pada batasan berikut:

- Nama: Anda harus menggunakan nama subjek DNS yang sesuai. Untuk informasi selengkapnya, lihat [Nama Domain](#).
- Algoritma: Untuk enkripsi, algoritma kunci privat sertifikat harus berupa 2048-bitRSA, ECDSA 256-bit, atau 384-bit. ECDSA


 Note

Keluarga algoritma penandatanganan yang ditentukan (RSAatauECDSA) harus cocok dengan keluarga algoritme kunci rahasia CA.

- Kedaluwarsa: Setiap sertifikat berlaku selama 13 bulan (395 hari). Tanggal akhir sertifikat CA penandatanganan harus melebihi tanggal akhir sertifikat yang diminta, atau permintaan sertifikat akan gagal.
- Perpanjangan: ACM upaya untuk memperbarui sertifikat pribadi secara otomatis setelah 11 bulan.

CA pribadi yang digunakan untuk menandatangani sertifikat entitas akhir tunduk pada batasannya sendiri:

- CA harus memiliki status Aktif.
- Algoritma kunci pribadi CA harus RSA 2048 atau RSA 4096.

 Note

Tidak seperti sertifikat yang dipercaya publik, sertifikat yang ditandatangani oleh CA pribadi tidak memerlukan validasi.

## Ketentuan untuk menggunakan AWS Private CA untuk menandatangani sertifikat ACM pribadi

Anda dapat menggunakan AWS Private CA untuk menandatangani ACM sertifikat Anda dalam salah satu dari dua kasus:

- Akun tunggal: CA penandatanganan dan AWS Certificate Manager (ACM) sertifikat yang dikeluarkan berada di tempat yang sama AWS akun.

Agar penerbitan dan pembaruan akun tunggal diaktifkan, AWS Private CA administrator harus memberikan izin kepada kepala ACM layanan untuk membuat, mengambil, dan membuat daftar sertifikat. Hal ini dilakukan dengan menggunakan AWS Private CA API tindakan [CreatePermission](#) atau AWS CLI perintah [buat-izin](#). Pemilik akun memberikan izin ini kepada IAM pengguna, grup, atau peran yang bertanggung jawab untuk menerbitkan sertifikat.

- Cross-account: CA penandatanganan dan ACM sertifikat yang dikeluarkan berada di tempat yang berbeda AWS akun, dan akses ke CA telah diberikan ke akun tempat sertifikat berada.

Untuk mengaktifkan penerbitan dan pembaruan lintas akun, AWS Private CA administrator harus melampirkan kebijakan berbasis sumber daya ke CA menggunakan AWS Private CA API tindakan [PutPolicy](#) atau AWS CLI perintah [put-policy](#). Kebijakan ini menetapkan prinsipal di akun lain yang diizinkan akses terbatas ke CA. Untuk informasi selengkapnya, lihat [Menggunakan Kebijakan Berbasis Sumber Daya dengan CA ACM Pribadi](#).

Skenario lintas akun juga mengharuskan ACM untuk menyiapkan peran terkait layanan (SLR) untuk berinteraksi sebagai prinsipal dengan kebijakan. PCA ACM membuat secara SLR otomatis saat mengeluarkan sertifikat pertama.

ACM mungkin mengingatkan Anda bahwa itu tidak dapat menentukan apakah SLR ada di akun Anda. Jika `iam:GetRole` izin yang diperlukan telah diberikan kepada akun Anda, maka peringatan tidak akan terulang kembali setelah SLR dibuat. ACM SLR Jika terulang kembali, Anda atau administrator akun Anda mungkin perlu memberikan `iam:GetRole` izin ACM, atau mengaitkan akun Anda dengan kebijakan ACM -managed. `AWSCertificateManagerFullAccess`

Untuk informasi selengkapnya, lihat [Menggunakan Peran Tertaut Layanan dengan ACM](#).

#### Important

ACM Sertifikat Anda harus secara aktif dikaitkan dengan dukungan AWS layanan sebelum dapat diperpanjang secara otomatis. Untuk informasi tentang sumber daya yang ACM mendukung, lihat [Layanan terintegrasi dengan ACM](#).



# Minta sertifikat pribadi di AWS Certificate Manager

## Minta sertifikat pribadi (konsol)

1. Masuk ke AWS Konsol Manajemen dan buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>.

Pilih Minta sertifikat.

2. Pada halaman Permintaan sertifikat, pilih Minta sertifikat pribadi dan Berikutnya untuk melanjutkan.
3. Di bagian Detail otoritas sertifikat, klik menu Otoritas sertifikat dan pilih salah satu privat yang tersedia. Jika CA dibagikan dari akun lain, maka akan ARN diawali oleh informasi kepemilikan.

Detail tentang CA ditampilkan untuk membantu Anda memverifikasi bahwa Anda telah memilih yang benar:

- Pemilik
  - Jenis
  - Nama umum (CN)
  - Organisasi (O)
  - Unit organisasi (OU)
  - Nama negara (C)
  - Negara bagian atau provinsi
  - Nama lokalitas
4. Di bagian Nama domain, ketikkan nama domain Anda. Anda dapat menggunakan nama domain yang sepenuhnya memenuhi syarat (FQDN), seperti **www.example.com**, atau nama domain telanjang atau apex seperti **example.com**. Anda juga dapat menggunakan tanda bintang (\*) sebagai kartu liar di posisi paling kiri untuk melindungi beberapa nama situs di domain yang sama. Misalnya, **\*.example.com** melindungi **corp.example.com**, dan **images.example.com**. Nama kartu liar akan muncul di bidang Subjek dan di ekstensi Nama Alternatif Subjek sertifikat. ACM

**Note**

Saat Anda meminta sertifikat kartu liar, tanda bintang (\*) harus berada di posisi paling kiri dari nama domain dan hanya dapat melindungi satu tingkat subdomain. Misalnya, **\*.example.com** dapat melindungi **login.example.com**, dan **test.example.com**, tetapi tidak dapat melindungi **test.login.example.com**. Perhatikan juga bahwa **\*.example.com** melindungi hanya subdomain dari **example.com**, itu tidak melindungi domain telanjang atau apex (**example.com**). Untuk melindungi keduanya, lihat langkah selanjutnya

Secara opsional, pilih Tambahkan nama lain ke sertifikat ini dan ketikkan nama di kotak teks. Ini berguna untuk mengautentikasi domain telanjang atau apex (seperti **example.com**) dan subdomainnya seperti **\*.example.com**

5. Di bagian Algoritma kunci, pilih algoritma.

Untuk informasi yang membantu Anda memilih algoritme, lihat [Tag AWS Certificate Manager sumber daya](#).

6. Di bagian Tag, Anda dapat menandai sertifikat Anda secara opsional. Tag adalah pasangan nilai kunci yang berfungsi sebagai metadata untuk mengidentifikasi dan mengatur AWS sumber daya. Untuk daftar parameter ACM tag dan petunjuk tentang cara menambahkan tag ke sertifikat setelah pembuatan, lihat [Tag AWS Certificate Manager sumber daya](#).
7. Di bagian Izin perpanjangan sertifikat, akui pemberitahuan tentang izin perpanjangan sertifikat. Izin ini memungkinkan perpanjangan otomatis PKI sertifikat pribadi yang Anda tandatangani dengan CA yang dipilih. Untuk informasi selengkapnya, lihat [Menggunakan Peran Tertaut Layanan dengan ACM](#).
8. Setelah memberikan semua informasi yang diperlukan, pilih Permintaan. Konsol mengembalikan Anda ke daftar sertifikat, tempat Anda dapat melihat sertifikat baru Anda.

**Note**

Bergantung pada bagaimana Anda memesan daftar, sertifikat yang Anda cari mungkin tidak segera terlihat. Anda dapat mengklik segitiga hitam di sebelah kanan untuk mengubah urutan. Anda juga dapat menavigasi melalui beberapa halaman sertifikat menggunakan nomor halaman di kanan atas.

## Minta sertifikat pribadi (CLI)

Gunakan perintah [request-certificate](#) untuk meminta sertifikat pribadi di ACM

### Note

Saat Anda meminta PKI sertifikat pribadi yang ditandatangani oleh CA dari AWS Private CA, keluarga algoritma penandatanganan yang ditentukan (RSA atau ECDSA) harus cocok dengan keluarga algoritme kunci rahasia 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
```

Perintah ini menampilkan Amazon Resource Name (ARN) dari sertifikat pribadi baru Anda.

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

Dalam kebanyakan kasus, ACM secara otomatis melampirkan peran terkait layanan (SLR) ke akun Anda saat pertama kali Anda menggunakan CA bersama. SLR ini memungkinkan perpanjangan otomatis sertifikat entitas akhir yang Anda terbitkan. Untuk memeriksa apakah SLR ada, Anda dapat melakukan query IAM dengan perintah berikut:

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

Jika SLR ada, output perintah harus menyerupai yang berikut:

```
{
  "Role": {
    "Path": "/aws-service-role/acm.amazonaws.com/",
    "RoleName": "AWSServiceRoleForCertificateManager",
    "RoleId": "AAAAAAAA00000000BBBBBBB",
    "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"
}
}
```

Jika SLR tidak ada, lihat [Menggunakan Peran Tertaut Layanan dengan ACM](#).

## Ekspor AWS Certificate Manager sertifikat pribadi

Anda dapat mengekspor sertifikat yang dikeluarkan oleh AWS Private CA untuk digunakan di mana saja di PKI lingkungan pribadi Anda. File yang diekspor berisi sertifikat, rantai sertifikat, dan kunci pribadi terenkripsi. File ini harus disimpan dengan aman. Untuk informasi lebih lanjut tentang AWS Private CA, lihat [AWS Private Certificate Authority Panduan Pengguna](#).

### Note

Anda tidak dapat mengekspor sertifikat yang dipercaya publik atau kunci pribadinya, terlepas dari apakah itu dikeluarkan oleh ACM atau diimpor.

### Topik

- [Ekspor sertifikat pribadi \(konsol\)](#)
- [Ekspor sertifikat pribadi \(CLI\)](#)

## Ekspor sertifikat pribadi (konsol)

1. Masuk ke AWS Konsol Manajemen dan buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>.
2. Pilih Certificate Manager
3. Pilih tautan sertifikat yang ingin Anda ekspor.
4. Pilih Ekspor.
5. Masukkan dan konfirmasi frasa sandi untuk kunci pribadi.

### Note

Saat membuat frasa sandi Anda, Anda dapat menggunakan ASCII karakter apa pun kecuali #, \$, atau%.

6. Pilih Hasilkan PEM Pengkodean.
7. Anda dapat menyalin sertifikat, rantai sertifikat, dan kunci terenkripsi ke memori atau memilih Ekspor ke file untuk masing-masing file.
8. Pilih Selesai.

## Ekspor sertifikat pribadi (CLI)

Gunakan perintah [ekspor-sertifikat](#) untuk mengekspor sertifikat pribadi dan kunci pribadi. Anda harus menetapkan frasa sandi ketika Anda menjalankan perintah. Untuk keamanan tambahan, gunakan editor file untuk menyimpan frasa sandi Anda dalam file, lalu berikan frasa sandi dengan memasok file tersebut. Ini mencegah frasa sandi Anda disimpan dalam riwayat perintah dan mencegah orang lain melihat frasa sandi saat Anda mengetiknya.

### Note

File yang berisi frasa sandi tidak boleh diakhiri dengan terminator baris. Anda dapat memeriksa file kata sandi Anda seperti ini:

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

Contoh berikut menyalurkan output perintah `jq` untuk menerapkan PEM pemformatan.

[Linux]

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

[Windows]

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

Ini menghasilkan sertifikat PEM -format yang dikodekan oleh base64, juga berisi rantai sertifikat dan kunci pribadi terenkripsi, seperti pada contoh singkat berikut.

```
-----BEGIN CERTIFICATE-----
MIIDTCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMtkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQDDAx3d3cuc3B1ZHMuaW8wggeiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwW0dL0kxpwkKkKwTcEkQuHE1v5Vn6HpbFfmxkdPEasoDhthH
FFWIf4/+V01bDLgju4HgtmV4IJDtqM9rG0Z42eFYmmc3eQ00GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmans8j6YxmtPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMtkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQKDAh0cm9sb2xvbkDCCASiWwDQYJKoZIhvcNAQEBBQADggEP
...
j2PA0viqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPd1+KB6M/+H93Z1/Bs8ERqqga/
6lFm6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDANBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCAggAMB0GCWCGSAF1AwQBKqQ0DViroIHStQgN0jr6nTUnuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTpSkNCdCAHqdh0SqBwt65qUTZe3gBt
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrXuHTWjF1
wEuqyd8X/ApkQsYFX/nhep0EIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxf0C1E/GSLBCixv3v
```

```
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs90V/VXzNuHYg==  
-----END ENCRYPTED PRIVATE KEY-----
```

Untuk menampilkan semuanya ke file, tambahkan > redirector ke contoh sebelumnya, menghasilkan yang berikut.

```
$ 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
```

## Impor sertifikat ke AWS Certificate Manager

Selain SSL TLS meminta/sertifikat yang disediakan oleh AWS Certificate Manager (ACM), Anda dapat mengimpor sertifikat yang Anda peroleh di luar AWS. Anda dapat melakukan ini karena Anda sudah memiliki sertifikat dari otoritas sertifikat pihak ketiga (CA), atau karena Anda memiliki persyaratan khusus aplikasi yang tidak dipenuhi oleh sertifikat yang ACM diterbitkan.

Anda dapat menggunakan sertifikat yang diimpor dengan [AWS Layanan yang terintegrasi dengan ACM](#). Sertifikat yang Anda impor bekerja sama dengan yang disediakan oleh ACM, dengan satu pengecualian penting: ACM tidak menyediakan [perpanjangan terkelola](#) untuk sertifikat yang diimpor.

Untuk memperbarui sertifikat yang diimpor, Anda dapat memperoleh sertifikat baru dari penerbit sertifikat Anda dan kemudian [mengimpornya kembali](#) secara manual. ACM Tindakan ini mempertahankan asosiasi sertifikat dan nama Sumber Daya Amazon (ARN). Atau, Anda dapat mengimpor sertifikat yang sama sekali baru. Beberapa sertifikat dengan nama domain yang sama dapat diimpor, tetapi harus diimpor satu per satu.

### Important

Anda bertanggung jawab untuk memantau tanggal kedaluwarsa sertifikat impor Anda dan untuk memperbaruinya sebelum kedaluwarsa. Anda dapat menyederhanakan tugas ini dengan menggunakan Amazon CloudWatch Events untuk mengirim pemberitahuan ketika sertifikat impor Anda mendekati kedaluwarsa. Untuk informasi selengkapnya, lihat [Menggunakan Amazon EventBridge](#).

Semua sertifikat ACM adalah sumber daya regional, termasuk sertifikat yang Anda impor. Untuk menggunakan sertifikat yang sama dengan penyeimbang beban Elastic Load Balancing di berbagai AWS Wilayah, Anda harus mengimpor sertifikat ke setiap Wilayah tempat Anda ingin menggunakannya. Untuk menggunakan sertifikat dengan Amazon CloudFront, Anda harus mengimpornya ke Wilayah AS Timur (Virginia N.). Untuk informasi selengkapnya, lihat [Wilayah yang Didukung](#).

Untuk informasi tentang cara mengimpor sertifikat ke dalam ACM, lihat topik berikut. Jika Anda mengalami masalah saat mengimpor sertifikat, lihat [Masalah impor sertifikat](#).

## Topik

- [Prasyarat untuk mengimpor sertifikat ACM](#)
- [Sertifikat dan format kunci untuk mengimpor](#)
- [Impor sertifikat](#)
- [Impor ulang sertifikat](#)

## Prasyarat untuk mengimpor sertifikat ACM

Untuk mengimpor TLS sertifikat yang ditandatangani SSL sendiri/ke dalam ACM, Anda harus memberikan sertifikat dan kunci pribadinya. Untuk mengimpor sertifikat yang ditandatangani oleh non-AWS otoritas sertifikat (CA), Anda juga harus menyertakan kunci sertifikat pribadi dan publik. Sertifikat Anda harus memenuhi semua kriteria yang dijelaskan dalam topik ini.

Untuk semua sertifikat yang diimpor, Anda harus menentukan algoritma kriptografi dan ukuran kunci. ACM mendukung algoritma berikut (API nama dalam tanda kurung):

- RSA1024 bit () RSA\_1024
- RSA2048 bit () RSA\_2048
- RSA3072 bit () RSA\_3072
- RSA4096 bit () RSA\_4096
- ECDSA256 bit (EC\_prime256v1)
- ECDSA384 bit () EC\_secp384r1
- ECDSA521 bit () EC\_secp521r1

Perhatikan juga persyaratan tambahan berikut:



- ACM [Layanan terintegrasi](#) hanya memungkinkan algoritma dan ukuran kunci yang mereka dukung untuk dikaitkan dengan sumber daya mereka. Misalnya, CloudFront hanya mendukung kunci 256-bitRSA, 2048-bit, 3072-bitRSA, dan Elliptic Prime Curve 256-bitRSA, sedangkan Application Load Balancer mendukung semua algoritma yang tersedia. ACM Untuk informasi selengkapnya, lihat dokumentasi untuk layanan yang Anda gunakan.
- Sertifikat harus berupa SSL TLS sertifikat/X.509 versi 3. Ini harus berisi kunci publik, nama domain yang sepenuhnya memenuhi syarat (FQDN) atau alamat IP untuk situs web Anda, dan informasi tentang penerbit.
- Sertifikat dapat ditandatangani sendiri oleh kunci pribadi yang Anda miliki, atau ditandatangani oleh kunci pribadi CA yang menerbitkan. Anda harus memberikan kunci pribadi, yang mungkin tidak lebih besar dari 5 KB (5.120 byte) dan harus tidak dienkripsi.
- Jika sertifikat ditandatangani oleh CA, dan Anda memilih untuk memberikan rantai sertifikat, rantai harus PEM dikodekan —.
- Sertifikat harus valid pada saat impor. Anda tidak dapat mengimpor sertifikat sebelum masa berlakunya dimulai atau setelah kedaluwarsa. Bidang `NotBefore` sertifikat berisi tanggal mulai validitas, dan `NotAfter` bidang berisi tanggal akhir.
- Semua materi sertifikat yang diperlukan (sertifikat, kunci pribadi, dan rantai sertifikat) harus PEM —dikodekan. Mengunggah materi DER yang dikodekan menghasilkan kesalahan. Untuk informasi selengkapnya dan contoh tambahan, lihat [Sertifikat dan format kunci untuk mengimpor](#).
- Saat Anda memperbarui (mengimpor ulang) sertifikat, Anda tidak dapat menambahkan `KeyUsage` atau `ExtendedKeyUsage` ekstensi jika ekstensi tidak ada dalam sertifikat yang diimpor sebelumnya.
- AWS CloudFormation tidak mendukung impor sertifikat ke dalam ACM.

## Sertifikat dan format kunci untuk mengimpor

ACM mengharuskan Anda untuk secara terpisah mengimpor sertifikat, rantai sertifikat, dan kunci pribadi (jika ada), dan untuk menyandikan setiap komponen dalam PEM format. PEM singkatan dari Privacy Enhanced Mail. PEM Format ini sering digunakan untuk mewakili sertifikat, permintaan sertifikat, rantai sertifikat, dan kunci. Ekstensi khas untuk file yang PEM diformat —adalah `.pem`, tetapi tidak perlu.

 Note

AWS tidak menyediakan utilitas untuk memanipulasi PEM file atau format sertifikat lainnya. Contoh berikut bergantung pada editor teks generik untuk operasi sederhana. Jika Anda perlu melakukan tugas yang lebih kompleks (seperti mengonversi format file atau mengekstrak kunci), alat gratis dan sumber terbuka seperti [Open SSL](#) sudah tersedia.


Contoh berikut menggambarkan format file yang akan diimpor. Jika komponen datang kepada Anda dalam satu file, gunakan editor teks (hati-hati) untuk memisahkannya menjadi tiga file. Perhatikan bahwa jika Anda mengedit salah satu karakter dalam PEM file secara tidak benar atau jika Anda menambahkan satu atau beberapa spasi ke akhir baris apa pun, sertifikat, rantai sertifikat, atau kunci pribadi tidak valid.

## Example 1. PEM—sertifikat yang dikodekan

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

## Example 2. PEM—rantai sertifikat yang dikodekan

Rantai sertifikat berisi satu atau beberapa sertifikat. Anda dapat menggunakan editor teks, copy perintah di Windows, atau cat perintah Linux untuk menggabungkan file sertifikat Anda ke dalam rantai. Sertifikat harus digabungkan agar masing-masing secara langsung mengesahkan yang sebelumnya. Jika mengimpor sertifikat pribadi, salin sertifikat root terakhir. Contoh berikut berisi tiga sertifikat, tetapi rantai sertifikat Anda mungkin berisi lebih banyak atau lebih sedikit.

 Important

Jangan menyalin sertifikat Anda ke dalam rantai sertifikat.

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

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

### Example 3. PEM—kunci pribadi yang dikodekan

Sertifikat X.509 versi 3 menggunakan algoritma kunci publik. Saat Anda membuat sertifikat X.509 atau permintaan sertifikat, Anda menentukan algoritme dan ukuran bit kunci yang harus digunakan untuk membuat private - public key pair. Kunci publik ditempatkan dalam sertifikat atau permintaan. Anda harus menjaga rahasia kunci pribadi terkait. Tentukan kunci pribadi saat Anda mengimpor sertifikat. Kuncinya harus tidak dienkrpsi. Contoh berikut menunjukkan kunci RSA pribadi.

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

Contoh berikutnya menunjukkan kunci pribadi kurva PEM elips yang dikodekan. Bergantung pada bagaimana Anda membuat kunci, blok parameter mungkin tidak disertakan. Jika blok parameter disertakan, ACM hapus sebelum menggunakan kunci selama proses impor.

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

## Impor sertifikat

Anda dapat mengimpor sertifikat yang diperoleh secara eksternal (yaitu, yang disediakan oleh penyedia layanan kepercayaan pihak ketiga) ke dalam ACM dengan menggunakan AWS Management Console, AWS CLI, atau ACM API. Topik berikut menunjukkan kepada Anda cara menggunakan AWS Management Console dan AWS CLI. Prosedur untuk mendapatkan sertifikat dari non-AWS penerbit berada di luar cakupan panduan ini.

### Important

Algoritma tanda tangan yang Anda pilih harus memenuhi [Prasyarat untuk mengimpor sertifikat ACM](#).

## Topik

- [Impor \(konsol\)](#)
- [Impor \(AWS CLI\)](#)

## Impor (konsol)

Contoh berikut menunjukkan cara mengimpor sertifikat menggunakan AWS Management Console.

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>. Jika ini adalah pertama kalinya Anda menggunakan ACM, cari AWS Certificate Manager menuju dan pilih tombol Mulai di bawahnya.
2. Pilih Impor sertifikat.
3. Lakukan hal-hal berikut:
  - a. Untuk badan Sertifikat, tempel sertifikat PEM -encoded untuk diimpor. Itu harus dimulai dengan -----BEGIN CERTIFICATE----- dan diakhiri dengan-----END CERTIFICATE-----.
  - b. Untuk kunci privat Sertifikat, tempel kunci pribadi yang tidak PEM dienkripsi dan tidak terenkripsi sertifikat. Itu harus dimulai dengan -----BEGIN PRIVATE KEY----- dan diakhiri dengan-----END PRIVATE KEY-----.
  - c. (Opsional) Untuk rantai Sertifikat, tempel rantai sertifikat PEM yang dikodekan.
4. (Opsional) Untuk menambahkan tag ke sertifikat impor Anda, pilih Tag. Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan. Anda dapat menggunakan tag untuk mengatur sumber daya Anda atau melacak AWS biaya.
5. Pilih Impor.

## Impor (AWS CLI)

Contoh berikut menunjukkan cara mengimpor sertifikat menggunakan [AWS Command Line Interface \(AWS CLI\)](#). Contohnya mengasumsikan sebagai berikut:

- Sertifikat PEM -encoded disimpan dalam file bernama. `Certificate.pem`
- Rantai sertifikat PEM -encoded disimpan dalam file bernama. `CertificateChain.pem`

- Kunci pribadi yang PEM diencode dan tidak terenkripsi disimpan dalam file bernama `PrivateKey.pem`

Untuk menggunakan contoh berikut, ganti nama file dengan nama Anda sendiri dan ketik perintah pada satu baris kontinu. Contoh berikut mencakup jeda baris dan ruang tambahan untuk memudahkan Anda membaca.

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

Jika `import-certificate` perintah berhasil, ia mengembalikan [Amazon Resource Name \(ARN\)](#) dari sertifikat yang diimpor.

## Impor ulang sertifikat

Jika Anda mengimpor sertifikat dan mengaitkannya dengan yang lain AWS layanan, Anda dapat mengimpor ulang sertifikat itu sebelum kedaluwarsa sambil mempertahankan AWS asosiasi layanan dari sertifikat asli. Untuk informasi lebih lanjut tentang AWS layanan terintegrasi dengan ACM, lihat [Layanan terintegrasi dengan ACM](#).

Ketentuan berikut berlaku saat Anda mengimpor ulang sertifikat:

- Anda dapat menambahkan atau menghapus nama domain.
- Anda tidak dapat menghapus semua nama domain dari sertifikat.
- Jika ekstensi Penggunaan Kunci hadir dalam sertifikat yang diimpor semula, Anda dapat menambahkan nilai ekstensi baru, tetapi Anda tidak dapat menghapus nilai yang ada.
- Jika ekstensi Penggunaan Kunci Diperpanjang hadir dalam sertifikat yang diimpor semula, Anda dapat menambahkan nilai ekstensi baru, tetapi Anda tidak dapat menghapus nilai yang ada.
- Jenis dan ukuran kunci tidak dapat diubah.
- Anda tidak dapat menerapkan tag sumber daya saat mengimpor ulang sertifikat.

### Topik

- [Impor ulang \(konsol\)](#)
- [Impor ulang \(AWS CLI\)](#)

## Impor ulang (konsol)

Contoh berikut menunjukkan cara mengimpor ulang sertifikat menggunakan AWS Management Console.

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/rumah>.
2. Pilih atau perluas sertifikat untuk diimpor ulang.
3. Buka panel detail sertifikat dan pilih tombol Impor ulang sertifikat. Jika Anda memilih sertifikat dengan mencentang kotak di samping namanya, pilih Impor ulang sertifikat pada menu Tindakan.
4. Untuk badan Sertifikat, tempel sertifikat entitas akhir PEM yang dikodekan.
5. Untuk kunci privat Sertifikat, tempel kunci privat PEM -encoded yang tidak terenkripsi yang terkait dengan kunci publik sertifikat.
6. (Opsional) Untuk rantai Sertifikat, tempel rantai sertifikat PEM yang dikodekan. Rantai sertifikat mencakup satu atau lebih sertifikat untuk semua otoritas sertifikasi penerbit menengah, dan sertifikat root. Jika sertifikat yang akan diimpor ditetapkan sendiri, tidak diperlukan rantai sertifikat.
7. Tinjau informasi tentang sertifikat Anda. Jika tidak ada kesalahan, pilih Impor Ulang.

## Impor ulang (AWS CLI)

Contoh berikut menunjukkan cara mengimpor ulang sertifikat menggunakan [AWS Command Line Interface \(AWS CLI\)](#). Contohnya mengasumsikan sebagai berikut:

- Sertifikat PEM -encoded disimpan dalam file bernama. `Certificate.pem`
- Rantai sertifikat PEM -encoded disimpan dalam file bernama. `CertificateChain.pem`
- (Hanya sertifikat pribadi) Kunci pribadi PEM yang dikodekan dan tidak terenkripsi disimpan dalam file bernama. `PrivateKey.pem`
- Anda memiliki sertifikat ARN yang ingin Anda impor ulang.

Untuk menggunakan contoh berikut, ganti nama file dan ARN dengan milik Anda sendiri dan ketik perintah pada satu baris kontinu. Contoh berikut mencakup jeda baris dan ruang tambahan untuk memudahkan Anda membaca.

**Note**

Untuk mengimpor ulang sertifikat, Anda harus menentukan sertifikatARN.

```
$ 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
```

Jika `import-certificate` perintah berhasil, ia mengembalikan [Amazon Resource Name \(ARN\)](#) sertifikat.

## Daftar sertifikat yang dikelola oleh AWS Certificate Manager

Anda dapat menggunakan ACM konsol atau AWS CLI untuk membuat daftar sertifikat yang dikelola oleh ACM. Konsol dapat mencantumkan hingga 500 sertifikat dalam satu halaman, dan CLI hingga 1000.

Untuk mencantumkan sertifikat Anda menggunakan konsol

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/>.
2. Tinjau informasi dalam daftar sertifikat. Anda dapat menavigasi melalui beberapa halaman sertifikat menggunakan nomor halaman di kanan atas. Setiap sertifikat menempati baris dengan kolom berikut ditampilkan secara default untuk setiap sertifikat:

- Nama domain — Nama domain yang sepenuhnya memenuhi syarat (FQDN) untuk sertifikat.
- Jenis - Jenis sertifikat. Nilai yang mungkin adalah: Amazon dikeluarkan | Pribadi | Diimpor
- Status - Status sertifikat. Nilai yang mungkin adalah: Validasi tertunda | Diterbitkan | Tidak aktif | Kedaluwarsa | Dicabut | Gagal | Waktu validasi habis
- Digunakan? — Apakah ACM sertifikat secara aktif dikaitkan dengan AWS layanan seperti Elastic Load Balancing atau CloudFront Nilainya bisa Tidak atau Ya.
- Kelayakan perpanjangan — Apakah sertifikat dapat diperpanjang secara otomatis ACM saat mendekati kedaluwarsa. Nilai yang mungkin adalah: Memenuhi Syarat | Tidak memenuhi syarat. Untuk aturan kelayakan, lihat. [Perpanjangan sertifikat dikelola di AWS Certificate Manager](#)

Dengan memilih ikon pengaturan di sudut kanan atas konsol, Anda dapat menyesuaikan jumlah sertifikat yang ditampilkan pada halaman, menentukan perilaku pembungkus baris konten sel, dan menampilkan bidang informasi tambahan. Bidang opsional berikut tersedia:

- Nama domain tambahan — Satu atau lebih nama domain (nama alternatif subjek) termasuk dalam sertifikat.
- Diminta di — Waktu ketika ACM diminta sertifikat.
- Diterbitkan pada — Waktu ketika sertifikat dikeluarkan. Informasi ini hanya tersedia untuk sertifikat yang dikeluarkan Amazon, bukan untuk impor.
- Tidak sebelumnya — Waktu sebelum sertifikat tidak valid.
- Tidak setelah - Waktu setelah sertifikat tidak valid.
- Dicabut di — Untuk sertifikat yang dicabut, waktu pencabutan.
- Tag nama — Nilai tag pada sertifikat ini disebut Nama, jika tag tersebut ada.
- Status perpanjangan - Status pembaruan sertifikat yang diminta. Bidang ini ditampilkan dan memiliki nilai hanya ketika pembaruan diminta. Nilai yang mungkin adalah: Perpanjangan otomatis yang tertunda | Validasi tertunda | Sukses | Kegagalan.

#### Note

Diperlukan waktu hingga beberapa jam agar perubahan status sertifikat tersedia. Jika terjadi masalah, permintaan sertifikat habis setelah 72 jam, dan proses penerbitan atau perpanjangan harus diulang dari awal.

Preferensi ukuran Halaman menentukan jumlah sertifikat yang dikembalikan pada setiap halaman konsol.

Untuk informasi selengkapnya tentang detail sertifikat yang tersedia, lihat [Tayang AWS Certificate Manager rincian sertifikat](#).

Untuk membuat daftar sertifikat Anda menggunakan AWS CLI

Gunakan perintah [list-certificate](#) untuk mencantumkan sertifikat ACM -managed Anda seperti yang ditunjukkan pada contoh berikut:

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



Perintah mengembalikan informasi yang mirip dengan berikut ini:

```
{
  "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"
    },...
  ]
}
```

Secara default, hanya sertifikat dengan `keyTypesRSA_1024` atau `RSA_2048` dan dengan setidaknya satu domain tertentu yang dikembalikan. Untuk melihat sertifikat lain yang Anda kontrol, seperti sertifikat tanpa domain atau sertifikat menggunakan algoritme atau ukuran bit yang berbeda, berikan `--includes` parameter seperti yang ditunjukkan pada contoh berikut. Parameter ini memungkinkan Anda menentukan anggota struktur [Filter](#).

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

# Tayang AWS Certificate Manager rincian sertifikat


Anda dapat menggunakan ACM konsol atau AWS CLI untuk membuat daftar metadata terperinci tentang sertifikat Anda.

Untuk melihat detail sertifikat di konsol

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/> untuk menampilkan sertifikat Anda. Anda dapat menavigasi melalui beberapa halaman sertifikat menggunakan nomor halaman di kanan atas.
2. Untuk menampilkan metadata terperinci untuk sertifikat yang terdaftar, pilih ID Sertifikat. Halaman terbuka, menampilkan informasi berikut:

- Status sertifikat
  - Identifier - pengidentifikasi unik heksadesimal 32-byte dari sertifikat
  - ARN— Nama Sumber Daya Amazon (ARN) dalam formulir  
`arn:aws:acm:Region:444455556666:certificate/certificate_ID`
  - Jenis - Mengidentifikasi kategori manajemen ACM sertifikat. Nilai yang mungkin adalah: Amazon Diterbitkan | Pribadi | Diimpor. Untuk informasi selengkapnya, lihat [AWS Certificate Manager sertifikat publik](#), [Minta sertifikat pribadi di AWS Certificate Manager](#), atau [Impor sertifikat ke AWS Certificate Manager](#).
  - Status - Status sertifikat. Nilai yang mungkin adalah: Validasi tertunda | Diterbitkan | Tidak aktif | Kedaluwarsa | Dicabut | Gagal | Waktu validasi habis
  - Status terperinci - Tanggal dan waktu ketika sertifikat dikeluarkan atau diimpor
- Domain
  - Domain — Nama domain yang sepenuhnya memenuhi syarat (FQDN) untuk sertifikat.
  - Status — Status validasi domain. Nilai yang mungkin adalah: Validasi tertunda | Dicabut | Gagal | Waktu validasi habis | Sukses
- Detail
  - Digunakan? — Apakah sertifikat dikaitkan dengan [AWS layanan terintegrasi Nilai yang](#) mungkin adalah: Ya | Tidak
  - Nama domain — Nama domain pertama yang memenuhi syarat (FQDN) untuk sertifikat.
  - Jumlah nama tambahan — Jumlah nama domain yang sertifikatnya valid
  - Nomor seri - nomor seri heksadesimal 16-byte dari sertifikat

- Info kunci publik — Algoritma kriptografi yang menghasilkan key pair
- Algoritma tanda tangan — Algoritma kriptografi yang digunakan untuk menandatangani sertifikat.
- Dapat digunakan dengan — Daftar [layanan ACM terintegrasi](#) yang mendukung sertifikat dengan parameter ini
- Diminta pada — Tanggal dan waktu permintaan penerbitan
- Diterbitkan pada — Jika berlaku, tanggal dan waktu penerbitan
- Diimpor pada - Jika berlaku, tanggal dan waktu impor
- Tidak sebelum - Awal masa berlaku sertifikat
- Tidak setelah - Tanggal kedaluwarsa dan waktu sertifikat
- Kelayakan perpanjangan — Nilai yang mungkin adalah: Memenuhi Syarat | Tidak memenuhi syarat. Untuk aturan kelayakan, lihat. [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#)
- Status perpanjangan - Status pembaruan sertifikat yang diminta. Bidang ini ditampilkan dan memiliki nilai hanya ketika pembaruan diminta. Nilai yang mungkin adalah: Perpanjangan otomatis yang tertunda | Validasi tertunda | Sukses | Kegagalan.

 Note

Diperlukan waktu hingga beberapa jam agar perubahan status sertifikat tersedia. Jika terjadi masalah, permintaan sertifikat habis setelah 72 jam, dan proses penerbitan atau perpanjangan harus diulang dari awal.

- CA — ARN Penandatanganan CA
- Tanda
  - Kunci
  - Nilai
- Status validasi - Jika berlaku, nilai yang mungkin adalah:
  - Tertunda — Validasi telah diminta dan belum selesai.
  - Waktu validasi habis - Waktu validasi yang diminta habis, tetapi Anda dapat mengulangi permintaan tersebut.
  - Tidak ada — Sertifikat ini untuk pribadi PKI atau ditandatangani sendiri, dan tidak memerlukan validasi.

## Untuk melihat detail sertifikat menggunakan AWS CLI

Gunakan sertifikat [deskripsikan](#) di AWS CLI untuk menampilkan rincian sertifikat, seperti yang ditunjukkan pada perintah berikut:

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

Perintah mengembalikan informasi yang mirip dengan berikut ini:

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

```
    "ExtendedKeyUsages": [
      {
        "OID": "1.3.6.1.5.5.7.3.1",
        "Name": "TLS_WEB_SERVER_AUTHENTICATION"
      },
      {
        "OID": "1.3.6.1.5.5.7.3.2",
        "Name": "TLS_WEB_CLIENT_AUTHENTICATION"
      }
    ],
    "DomainValidationOptions": [
      {
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ],
        "ValidationDomain": "example.com",
        "DomainName": "example.com"
      },
      {
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ],
        "ValidationDomain": "www.example.com",
        "DomainName": "www.example.com"
      }
    ],
    "Subject": "CN=example.com"
  }
}
```

## Hapus sertifikat yang dikelola oleh AWS Certificate Manager

Anda dapat menggunakan ACM konsol atau AWS CLI untuk menghapus sertifikat.

**⚠ Important**

- Anda tidak dapat menghapus ACM sertifikat yang sedang digunakan oleh orang lain AWS layanan. Untuk menghapus sertifikat yang sedang digunakan, Anda harus terlebih dahulu menghapus asosiasi sertifikat. Ini dilakukan menggunakan konsol atau CLI untuk layanan terkait.
- Menghapus sertifikat yang dikeluarkan oleh otoritas sertifikat swasta (CA) tidak berpengaruh pada CA. Anda akan terus dikenakan biaya untuk CA sampai dihapus. Untuk informasi selengkapnya, lihat [Menghapus CA Pribadi Anda](#) di AWS Private Certificate Authority Panduan Pengguna.

Untuk menghapus sertifikat menggunakan konsol

1. Buka ACM konsol di <https://console.aws.amazon.com/acm/>.
2. Dalam daftar sertifikat, pilih kotak centang untuk ACM sertifikat, lalu pilih Hapus.

**ℹ Note**

Bergantung pada bagaimana Anda memesan daftar, sertifikat yang Anda cari mungkin tidak segera terlihat. Anda dapat mengklik segitiga hitam di sebelah kanan untuk mengubah urutan. Anda juga dapat menavigasi melalui beberapa halaman sertifikat menggunakan nomor halaman di kanan atas.

Untuk menghapus sertifikat menggunakan AWS CLI

Gunakan perintah [delete-certificate](#) untuk menghapus sertifikat, seperti yang ditunjukkan pada perintah berikut:

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

# Perpanjangan sertifikat terkelola di AWS Certificate Manager

ACM menyediakan perpanjangan terkelola untuk sertifikat yang dikeluarkan Amazon SSL Anda. TLS Ini berarti bahwa ACM akan memperbarui sertifikat Anda secara otomatis (jika Anda menggunakan DNS validasi), atau akan mengirim Anda pemberitahuan email ketika kedaluwarsa mendekati. Layanan ini disediakan untuk ACM sertifikat publik dan swasta.

Sertifikat memenuhi syarat untuk perpanjangan otomatis dengan pertimbangan berikut:

- **ELIGIBLE** Jika diasosiasikan dengan yang lain AWS layanan, seperti Elastic Load Balancing atau CloudFront
- **ELIGIBLE** jika diekspor sejak diterbitkan atau terakhir diperpanjang.
- **ELIGIBLE** jika itu adalah sertifikat pribadi yang dikeluarkan dengan menelepon ACM [RequestCertificateAPI](#) dan kemudian diekspor atau dikaitkan dengan yang lain AWS layanan.
- **ELIGIBLE** jika itu adalah sertifikat pribadi yang dikeluarkan melalui [konsol manajemen](#) dan kemudian diekspor atau dikaitkan dengan yang lain AWS layanan.
- **NOTELIGIBLE** jika itu adalah sertifikat pribadi yang dikeluarkan dengan menghubungi AWS Private CA [IssueCertificate](#) API.
- **NOTELIGIBLE** jika [diimpor](#).
- **NOTELIGIBLE** jika sudah kadaluarsa.

Selain itu, persyaratan [Punycode](#) berikut yang berkaitan dengan [Nama Domain Internasional](#) harus dipenuhi:

1. Nama domain yang dimulai dengan pola “<character><character>--” harus cocok dengan “xn--”.
2. Nama domain yang diawali dengan “xn--” juga harus merupakan Nama Domain Internasionalisasi yang valid.

## Contoh Punycode

Nama Domain	Memenuhkan #1	Memenuhkan #2	Diizinkan	Catatan
contoh.com	tidak berlaku	T/A	✓	Tidak dimulai dengan “<character><character>--”

Nama Domain	Memenuh #1	Memenuh #2	Diizinkan	Catatan
a--example.com	tidak berlaku	T/A	✓	Tidak dimulai dengan "<character><character>--"
abc--example.com	tidak berlaku	T/A	✓	Tidak dimulai dengan "<character><character>--"
xn--xyz.com	Ya	Ya	✓	Nama Domain Internasional yang Valid (diselesaikan ke .com)
xn--example.com	Ya	Tidak	✗	Bukan Nama Domain Internasionalisasi yang valid
ab--example.com	Tidak	Tidak	✗	Harus dimulai dengan "xn--"

Saat ACM memperbarui sertifikat, Amazon Resource Name (ARN) sertifikat tetap sama. Juga, ACM sertifikat adalah [sumber daya regional](#). Jika Anda memiliki sertifikat untuk nama domain yang sama dalam beberapa AWS Daerah, masing-masing sertifikat ini harus diperbarui secara independen.

#### Topik

- [Perbarui sertifikat ACM publik](#)
- [Perpanjangan sertifikat pribadi di AWS Certificate Manager](#)
- [Periksa status perpanjangan sertifikat](#)

## Perbarui sertifikat ACM publik

Saat mengeluarkan sertifikat yang dikelola dan dipercaya publik, AWS Certificate Manager mengharuskan Anda untuk membuktikan bahwa Anda adalah pemilik domain. Ini terjadi melalui [DNSvalidasi atau validasi email](#). Ketika sertifikat muncul untuk perpanjangan, ACM gunakan metode yang sama yang Anda pilih sebelumnya untuk memvalidasi ulang kepemilikan Anda. Topik-topik berikut menjelaskan bagaimana proses pembaruan bekerja dalam setiap kasus.

#### Topik



- [Perpanjangan untuk domain yang divalidasi oleh DNS](#)
- [Perpanjangan untuk domain yang divalidasi email](#)

## Perpanjangan untuk domain yang divalidasi oleh DNS

Perpanjangan terkelola sepenuhnya otomatis untuk ACM sertifikat yang awalnya diterbitkan menggunakan [DNSvalidasi](#).

Pada 60 hari sebelum kedaluwarsa, ACM periksa kriteria perpanjangan berikut:

- Sertifikat saat ini digunakan oleh AWS layanan.
- Semua DNS CNAME catatan ACM yang disediakan (satu untuk setiap Nama Alternatif Subjek yang unik) ada dan dapat diakses melalui publikDNS.

Jika kriteria ini terpenuhi, ACM pertimbangkan nama domain yang divalidasi dan perbarui sertifikat.

ACM mengirim AWS Health peristiwa dan EventBridge peristiwa Amazon ketika tidak dapat secara otomatis memvalidasi domain selama perpanjangan (misalnya, karena adanya CAA catatan). Peristiwa ini dikirim pada 45 hari, 30 hari, 15 hari, tujuh hari, tiga hari, dan satu hari sebelum kedaluwarsa. Untuk informasi selengkapnya, lihat [EventBridge Dukungan Amazon untuk ACM](#).

## Perpanjangan untuk domain yang divalidasi email

ACM sertifikat berlaku selama 13 bulan (395 hari). Memperpanjang sertifikat memerlukan tindakan oleh pemilik domain. ACM mulai mengirimkan pemberitahuan perpanjangan ke alamat email yang terkait dengan domain 45 hari sebelum kedaluwarsa. Notifikasi berisi tautan yang dapat diklik pemilik domain untuk perpanjangan. Setelah semua domain yang terdaftar divalidasi, ACM mengeluarkan sertifikat yang diperbarui dengan hal yang sama. ARN

Untuk informasi selengkapnya tentang pesan email validasi, lihat [AWS Certificate Manager validasi email](#)

Untuk mempelajari bagaimana Anda dapat merespons email validasi secara terprogram, lihat [Mengotomatiskan AWS Certificate Manager validasi email](#)

### Kirim ulang email validasi

Setelah mengonfigurasi validasi email untuk domain saat meminta sertifikat (lihat [AWS Certificate Manager validasi email](#)), Anda dapat menggunakan AWS Certificate Manager API untuk meminta

Anda ACM mengirimkan email validasi domain untuk perpanjangan sertifikat Anda. Anda harus melakukan ini dalam keadaan berikut:

- Anda menggunakan validasi email saat awalnya meminta sertifikat Anda ACM.
- Status perpanjangan sertifikat Anda sedang menunggu validasi. Untuk informasi tentang menentukan status perpanjangan sertifikat, lihat [Periksa status perpanjangan sertifikat](#).
- Anda tidak menerima atau tidak dapat menemukan pesan email validasi domain asli yang ACM dikirim untuk perpanjangan sertifikat.

Untuk mengirim email validasi ke domain yang berbeda dari yang awalnya Anda konfigurasi dalam permintaan sertifikat, Anda dapat menggunakan [ResendValidationEmail](#) operasi di, ACM API AWS CLI, atau AWS SDKs. ACM akan mengirim email ke domain validasi yang ditentukan. Anda dapat mengakses AWS CLI di browser dengan menggunakan AWS CloudShell di Wilayah yang didukung.

Untuk meminta ACM pengiriman ulang pesan email validasi domain (konsol)

1. Buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/rumah>.
2. Pilih ID Sertifikat sertifikat yang memerlukan validasi.
3. Pilih Kirim ulang email validasi.

Untuk meminta ACM pengiriman ulang email validasi domain () ACM API

Gunakan [ResendValidationEmail](#) operasi di ACM API. Dengan demikian, berikan sertifikat, domain yang memerlukan validasi manual, dan domain tempat Anda ingin menerima email validasi domain. ARN Contoh berikut menunjukkan bagaimana melakukan ini dengan AWS CLI. Contoh ini berisi jeda baris agar lebih mudah dibaca.

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

## Perpanjangan sertifikat pribadi di AWS Certificate Manager

ACM sertifikat yang ditandatangani oleh CA pribadi dari AWS Private CA memenuhi syarat untuk perpanjangan terkelola. Tidak seperti ACM sertifikat yang dipercaya publik, sertifikat untuk privat tidak

PKI memerlukan validasi. Kepercayaan dibuat ketika administrator menginstal sertifikat CA root yang sesuai di toko kepercayaan klien.

#### Note

Hanya sertifikat yang diperoleh menggunakan ACM konsol atau [RequestCertificate](#) tindakan yang memenuhi syarat untuk perpanjangan terkelola. ACM API Sertifikat yang dikeluarkan langsung dari AWS Private CA menggunakan [IssueCertificate](#) tindakan dari AWS Private CA API tidak dikelola oleh ACM.

Ketika sertifikat terkelola 60 hari lagi dari kedaluwarsa, ACM secara otomatis mencoba memperbaruinya. Ini termasuk sertifikat yang diekspor dan diinstal secara manual (misalnya, di pusat data lokal). Pelanggan juga dapat memaksa pembaruan kapan saja menggunakan [RenewCertificate](#) tindakan. ACM API Untuk contoh implementasi Java dari pembaruan paksa, lihat [Memperbarui sertifikat](#).

Setelah perpanjangan, penyebaran sertifikat ke dalam layanan terjadi dengan salah satu cara berikut:

- Jika sertifikat dikaitkan dengan [layanan ACM terintegrasi](#), sertifikat baru menggantikan yang lama tanpa tindakan pelanggan tambahan.
- Jika sertifikat tidak terkait dengan [layanan ACM terintegrasi](#), tindakan pelanggan diperlukan untuk mengeksport dan menginstal sertifikat yang diperbarui. Anda dapat melakukan tindakan ini secara manual, atau dengan bantuan dari [AWS Health](#), [Amazon EventBridge](#), dan [AWS Lambda](#) sebagai berikut. Untuk informasi selengkapnya, silakan lihat [Mengotomatiskan ekspor sertifikat yang diperbarui](#)

## Mengotomatiskan ekspor sertifikat yang diperbarui

Prosedur berikut memberikan contoh solusi untuk mengotomatiskan ekspor PKI sertifikat pribadi Anda saat ACM memperbaruinya. Contoh ini hanya mengeksport sertifikat dan kunci privatnya dari ACM; setelah ekspor, sertifikat masih harus diinstal pada perangkat targetnya.

Untuk mengotomatiskan ekspor sertifikat menggunakan konsol

1. Mengikuti prosedur di AWS Panduan Pengembang Lambda, buat dan konfigurasi fungsi Lambda yang memanggil ekspor. ACM API

- a. [Buat fungsi Lambda](#).
- b. [Buat peran eksekusi Lambda](#) untuk fungsi Anda dan tambahkan kebijakan kepercayaan berikut ke dalamnya. Kebijakan memberikan izin ke kode dalam fungsi Anda untuk mengambil sertifikat yang diperbarui dan kunci pribadi dengan memanggil [ExportCertificate](#) tindakan. ACM API

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

2. [Buat aturan di Amazon EventBridge](#) untuk mendengarkan acara ACM kesehatan dan memanggil fungsi Lambda Anda saat mendeteksi satu. ACM menulis ke AWS Health acara setiap kali mencoba untuk memperbarui sertifikat. Untuk informasi lebih lanjut tentang pemberitahuan ini, lihat [Periksa status menggunakan Personal Health Dashboard \(PHD\)](#).

Konfigurasi aturan dengan menambahkan pola acara berikut.

```
{
  "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. Selesaikan proses perpanjangan dengan menginstal sertifikat secara manual pada sistem target.

## Uji perpanjangan sertifikat pribadi PKI yang dikelola

Anda dapat menggunakan ACM API atau AWS CLI untuk menguji konfigurasi alur kerja perpanjangan ACM terkelola Anda secara manual. Dengan demikian, Anda dapat mengonfirmasi bahwa sertifikat Anda akan diperbarui secara otomatis ACM sebelum kedaluwarsa.

### Note

Anda hanya dapat menguji perpanjangan sertifikat yang dikeluarkan dan diekspor oleh AWS Private CA.

Saat Anda menggunakan API tindakan atau CLI perintah yang dijelaskan di bawah ini, ACM mencoba memperbarui sertifikat. Jika perpanjangan berhasil, ACM perbarui metadata sertifikat yang ditampilkan di konsol manajemen atau dalam output. API Jika sertifikat dikaitkan dengan [layanan ACM terintegrasi](#), sertifikat baru akan digunakan dan acara perpanjangan dibuat di Amazon CloudWatch Events. Jika perpanjangan gagal, ACM mengembalikan kesalahan dan menyarankan tindakan perbaikan. (Anda dapat melihat informasi ini menggunakan [perintah deskripsi-sertifikat](#).) Jika sertifikat tidak digunakan melalui layanan terintegrasi, Anda masih perlu mengekspornya dan menginstalnya secara manual di sumber daya Anda.

### Important

Untuk memperbaharui AWS Private CA sertifikat dengan ACM, Anda harus terlebih dahulu memberikan izin utama ACM layanan untuk melakukannya. Untuk informasi selengkapnya, lihat [Menetapkan Izin Perpanjangan Sertifikat](#) ke. ACM

Untuk menguji perpanjangan sertifikat secara manual (AWS CLI)

1. Gunakan perintah [renew-certificate](#) untuk memperbarui sertifikat ekspor pribadi.

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

2. Kemudian gunakan [perintah deskripsi-sertifikat](#) untuk mengonfirmasi bahwa detail perpanjangan sertifikat telah diperbarui.

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

Untuk menguji perpanjangan sertifikat secara manual () ACM API

- Kirim [RenewCertificate](#) permintaan, tentukan sertifikat pribadi untuk diperpanjang. ARN Kemudian gunakan [DescribeCertificate](#) operasi untuk mengonfirmasi bahwa detail perpanjangan sertifikat telah diperbarui.

## Periksa status perpanjangan sertifikat

Ketika Anda telah mencoba untuk memperbarui sertifikat, ACM menyediakan kolom informasi status perpanjangan dalam rincian sertifikat. Anda dapat menggunakan AWS Certificate Manager konsol, itu ACM API, AWS CLI, atau AWS Health Dashboard untuk memeriksa status pembaruan ACM sertifikat. Jika Anda menggunakan konsol, AWS CLI, atau ACM API, status perpanjangan dapat memiliki salah satu dari empat nilai status yang mungkin tercantum di bawah ini. Nilai serupa ditampilkan jika Anda menggunakan AWS Health Dashboard.

### Perpanjangan otomatis yang tertunda

ACM mencoba untuk secara otomatis memvalidasi nama domain dalam sertifikat. Untuk informasi selengkapnya, lihat [Perpanjangan untuk domain yang divalidasi oleh DNS](#). Tidak diperlukan tindakan lebih lanjut.

### Validasi tertunda

ACM tidak dapat secara otomatis memvalidasi satu atau beberapa nama domain dalam sertifikat. Anda harus mengambil tindakan untuk memvalidasi nama domain ini atau sertifikat tidak akan diperpanjang. Jika Anda awalnya menggunakan validasi email untuk sertifikat, cari email

dari ACM dan kemudian ikuti tautan di email tersebut untuk melakukan validasi. Jika Anda menggunakan DNS validasi, periksa untuk memastikan DNS catatan Anda ada dan sertifikat Anda tetap digunakan.

### Berhasil

Semua nama domain dalam sertifikat divalidasi, dan ACM diperpanjang sertifikat. Tidak diperlukan tindakan lebih lanjut.

### Failed

Satu atau lebih nama domain tidak divalidasi sebelum sertifikat kedaluwarsa, dan ACM tidak memperbarui sertifikat. Anda dapat [meminta sertifikat baru](#).

Sertifikat memenuhi syarat untuk perpanjangan jika dikaitkan dengan yang lain AWS layanan, seperti Elastic Load Balancing atau CloudFront, atau jika telah diekspor sejak diterbitkan atau terakhir diperbarui.

#### Note

Diperlukan waktu hingga beberapa jam agar perubahan status pembaruan tersedia. Jika terjadi masalah, permintaan perpanjangan akan habis setelah 72 jam, dan proses perpanjangan harus diulang dari awal. Untuk bantuan penyelesaian masalah, lihat [Memecahkan masalah permintaan sertifikat](#).

### Topik

- [Periksa status \(konsol\)](#)
- [Periksa status \(API\)](#)
- [Periksa status \(CLI\)](#)
- [Periksa status menggunakan Personal Health Dashboard \(PHD\)](#)

## Periksa status (konsol)

Prosedur berikut membahas cara menggunakan ACM konsol untuk memeriksa status pembaruan ACM sertifikat.

1. Buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/rumah>.

2. Perluas sertifikat untuk melihat detailnya.
3. Temukan status Perpanjangan di bagian Detail. Jika Anda tidak melihat statusnya, ACM belum memulai proses perpanjangan terkelola untuk sertifikat ini.

## Periksa status (API)

Untuk contoh Java yang menunjukkan cara menggunakan [DescribeCertificate](#) tindakan untuk memeriksa status, lihat [Menjelaskan sertifikat](#).

## Periksa status (CLI)

Contoh berikut menunjukkan cara memeriksa status perpanjangan ACM sertifikat Anda dengan [AWS Command Line Interface \(AWS CLI\)](#).

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

Dalam tanggapannya, perhatikan nilai di `RenewalStatus` lapangan. Jika Anda tidak melihat `RenewalStatus` bidang, ACM belum memulai proses perpanjangan terkelola untuk sertifikat Anda.

## Periksa status menggunakan Personal Health Dashboard (PHD)

ACM upaya untuk memperbarui ACM sertifikat Anda secara otomatis 60 hari sebelum kedaluwarsa. Jika ACM tidak dapat memperbarui sertifikat Anda secara otomatis, ia akan mengirimkan pemberitahuan acara perpanjangan sertifikat ke AWS Health Dashboard pada 45 hari, 30 hari, 15 hari, 7 hari, 3 hari, dan interval 1 hari dari kedaluwarsa untuk memberi tahu Anda bahwa Anda perlu mengambil tindakan. Bagian AWS Health Dashboard adalah bagian dari AWS Health layanan. Ini tidak memerlukan pengaturan dan dapat dilihat oleh semua pengguna yang diautentikasi di akun Anda. Untuk informasi selengkapnya, silakan lihat [AWS Health Panduan Pengguna](#).

### Note

ACM menulis pemberitahuan acara pembaruan berturut-turut ke satu acara di garis waktu Anda. PHD Setiap pemberitahuan menimpa yang sebelumnya sampai pembaruan berhasil.

Untuk menggunakan AWS Health Dashboard:

1. Masuk ke AWS Health Dashboard di <https://phd.aws.amazon.com/phd/rumah #/>.



2. Pilih Log peristiwa.
3. Untuk Filter menurut tag atau atribut, pilih Layanan.
4. Pilih Certificate Manager.
5. Pilih Terapkan.
6. Untuk kategori Acara pilih Perubahan Terjadwal.
7. Pilih Terapkan.

# Tag AWS Certificate Manager sumber daya

Tag adalah label yang dapat Anda tetapkan ke ACM sertifikat. Setiap tanda terdiri atas kunci dan nilai. Anda dapat menggunakan AWS Certificate Manager konsol, AWS Command Line Interface (AWS CLI), atau ACM API untuk menambah, melihat, atau menghapus tag untuk ACM sertifikat. Anda dapat memilih tag mana yang akan ditampilkan di ACM konsol.

Anda dapat membuat tanda khusus yang sesuai dengan kebutuhan Anda. Misalnya, Anda dapat menandai beberapa ACM sertifikat dengan `Environment = Beta` tag `Environment = Prod` atau untuk mengidentifikasi lingkungan mana yang dimaksudkan untuk setiap ACM sertifikat. Daftar berikut mencakup beberapa contoh tambahan dari tag kustom lainnya:

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

Lainnya AWS sumber daya juga mendukung penandaan. Oleh karena itu, Anda dapat menetapkan tag yang sama ke sumber daya yang berbeda untuk menunjukkan apakah sumber daya tersebut terkait. Misalnya, Anda dapat menetapkan tag seperti `Website = example.com` ACM sertifikat, penyeimbang beban, dan sumber daya lain yang digunakan untuk situs web `example.com` Anda.

Topik

- [Batasan tag](#)
- [Mengelola tag](#)

## Batasan tag

Pembatasan dasar berikut berlaku untuk tag ACM sertifikat:

- Jumlah maksimum tag per ACM sertifikat adalah 50.
- Panjang maksimum kunci tag adalah 127 karakter.
- Panjang maksimum nilai tag adalah 255 karakter.
- Kunci dan nilai tanda peka huruf besar-kecil.

- `aws` : Awalan dicadangkan untuk AWS gunakan; Anda tidak dapat menambahkan, mengedit, atau menghapus tag yang kuncinya dimulai dengan `aws` : . Tag yang dimulai dengan `aws` : tidak dihitung terhadap tags-per-resource kuota Anda.
- Jika Anda berencana untuk menggunakan skema penandaan di beberapa layanan dan sumber daya, ingatlah bahwa layanan lain mungkin memiliki batasan lain untuk karakter yang diizinkan. Baca dokumentasi ini untuk layanan tersebut.
- ACM tag sertifikat tidak tersedia untuk digunakan di AWS Management Console [Resource Groups](#) dan [Tag Editor](#).

Untuk informasi umum tentang AWS konvensi penandaan, lihat Penandaan [AWS Sumber daya](#).

## Mengelola tag

Anda dapat menambahkan, mengedit, dan menghapus tag dengan menggunakan AWS Konsol Manajemen, AWS Command Line Interface, atau AWS Certificate Manager API.

### Mengelola tag (konsol)

Anda dapat menggunakan AWS Management Console untuk menambah, menghapus, atau mengedit tag. Anda juga dapat menampilkan tag di kolom.

#### Menambahkan tag

Gunakan prosedur berikut untuk menambahkan tag dengan menggunakan ACM konsol.

Untuk menambahkan tag ke sertifikat (konsol)

1. Masuk ke AWS Management Console dan buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/rumah>.
2. Pilih panah di sebelah sertifikat yang ingin Anda tag.
3. Di panel detail, gulir ke bawah ke Tag.
4. Pilih Edit dan Tambahkan Tag.
5. Ketik kunci dan nilai untuk tag.
6. Pilih Simpan.

## Menghapus tag

Gunakan prosedur berikut untuk menghapus tag dengan menggunakan ACM konsol.

Untuk menghapus tanda (konsol)

1. Masuk ke AWS Management Console dan buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/umah>.
2. Pilih panah di sebelah sertifikat dengan tag yang ingin Anda hapus.
3. Di panel detail, gulir ke bawah ke Tag.
4. Pilih Edit.
5. Pilih X di sebelah tag yang ingin Anda hapus.
6. Pilih Simpan.

## Mengedit tag

Gunakan prosedur berikut untuk mengedit tag dengan menggunakan ACM konsol.

Untuk mengedit tag (konsol)

1. Masuk ke AWS Management Console dan buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/umah>.
2. Pilih panah di samping sertifikat yang ingin Anda edit.
3. Di panel detail, gulir ke bawah ke Tag.
4. Pilih Edit.
5. Ubah kunci atau nilai tag yang ingin Anda ubah.
6. Pilih Simpan.

## Menampilkan tag di kolom

Gunakan prosedur berikut untuk menampilkan tag di kolom di ACM konsol.

Untuk menampilkan tag di kolom (konsol)

1. Masuk ke AWS Management Console dan buka AWS Certificate Manager konsol di <https://console.aws.amazon.com/acm/umah>.

2. Pilih tag yang ingin Anda tampilkan sebagai kolom dengan memilih ikon roda gigi



di sudut kanan atas konsol.

3. Pilih kotak centang di samping tag yang ingin Anda tampilkan di kolom.

## Mengelola tag (CLI)

Lihat topik berikut untuk mempelajari cara menambahkan, membuat daftar, dan menghapus tag dengan menggunakan AWS CLI.

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

## Mengelola tag (ACMAPI)

Lihat topik berikut untuk mempelajari cara menambahkan, membuat daftar, dan menghapus tag dengan menggunakan tagAPI.

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

# Layanan terintegrasi dengan ACM

AWS Certificate Manager Mendukung semakin banyak AWS layanan. Anda tidak dapat menginstal ACM sertifikat Anda atau pribadi Anda AWS Private CA sertifikat langsung pada Anda AWS situs web atau aplikasi berbasis.

## Note

ACMSertifikat publik dapat diinstal pada EC2 instans Amazon yang terhubung ke [Enclave Nitro](#), tetapi tidak ke instans Amazon lainnya. EC2 Untuk informasi tentang pengaturan server web mandiri pada EC2 instans Amazon yang tidak terhubung ke Enclave Nitro, lihat [Tutorial: Menginstal LAMP server web di Amazon Linux 2](#) atau [Tutorial: Menginstal server LAMP web dengan Amazon Linux. AMI](#)

ACMsertifikat didukung oleh layanan berikut:

## Penyeimbang Beban Elastis

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas aplikasi masuk Anda di beberapa instans Amazon. EC2 Ini mendeteksi kasus yang tidak sehat dan mengalihkan lalu lintas ke kasus sehat sampai kasus yang tidak sehat dipulihkan. Elastic Load Balancing secara otomatis menskalakan kapasitas penanganannya sebagai respons terhadap lalu lintas yang masuk. Untuk informasi selengkapnya tentang load balancing, lihat Panduan Pengguna [Elastic Load Balancing](#).


Secara umum, untuk menyajikan konten aman melaluiSSL/TLS, penyeimbang beban mengharuskan TLS sertifikatSSL/diinstal pada penyeimbang beban atau instans Amazon back-end. EC2 ACMterintegrasi dengan Elastic Load Balancing untuk menyebarkan ACM sertifikat pada load balancer. Untuk informasi selengkapnya, lihat [Membuat Application Load Balancer](#)

## Amazon CloudFront

Amazon CloudFront adalah layanan web yang mempercepat distribusi konten web dinamis dan statis Anda kepada pengguna akhir dengan mengirimkan konten Anda dari jaringan lokasi edge di seluruh dunia. Saat pengguna akhir meminta konten yang Anda layani CloudFront, pengguna akan diarahkan ke lokasi tepi yang memberikan latensi terendah. Ini memastikan bahwa konten disampaikan dengan kinerja terbaik. Jika konten saat ini berada di lokasi tepi itu, segera CloudFront kirimkan. Jika konten saat ini tidak berada di lokasi tepi tersebut, CloudFront

ambil dari bucket Amazon S3 atau server web yang telah Anda identifikasi sebagai sumber konten definitif. Untuk informasi selengkapnya CloudFront, lihat [Panduan CloudFront Pengembang Amazon](#).

Untuk menyajikan konten aman melalui SSL/TLS, CloudFront mengharuskan SSL/TLS sertifikat diinstal baik pada CloudFront distribusi atau pada sumber konten yang didukung. ACM terintegrasi dengan CloudFront untuk menyebarkan ACM sertifikat pada CloudFront distribusi. Untuk informasi selengkapnya, lihat [Mendapatkan SSL TLS /Sertifikat](#).

 Note

Untuk menggunakan ACM sertifikat dengan CloudFront, Anda harus meminta atau mengimpor sertifikat di wilayah AS Timur (Virginia N.).

## Amazon Cognito

Amazon Cognito menyediakan otentikasi, otorisasi, dan manajemen pengguna untuk web dan aplikasi seluler Anda. Pengguna dapat masuk langsung dengan Akun AWS kredensi atau melalui pihak ketiga seperti Facebook, Amazon, Google, atau Apple. Untuk informasi selengkapnya tentang Amazon Cognito, lihat Panduan Pengembang [Amazon Cognito](#).

Saat Anda mengonfigurasi kumpulan pengguna Cognito untuk menggunakan CloudFront proxy Amazon, CloudFront dapat menempatkan ACM sertifikat untuk mengamankan domain kustom. Ketika ini terjadi, ketahuilah bahwa Anda harus menghapus asosiasi sertifikat dengan CloudFront sebelum Anda dapat menghapusnya.

## AWS Elastic Beanstalk

Elastic Beanstalk membantu Anda menyebarkan dan mengelola aplikasi di AWS Cloud tanpa khawatir tentang infrastruktur yang menjalankan aplikasi tersebut. AWS Elastic Beanstalk mengurangi kompleksitas manajemen. Anda cukup mengunggah aplikasi Anda dan Elastic Beanstalk secara otomatis menangani detail penyediaan kapasitas, penyeimbangan beban, penskalaan, dan pemantauan kesehatan. Elastic Beanstalk menggunakan layanan Elastic Load Balancing untuk membuat load balancer. Untuk informasi lebih lanjut tentang Elastic Beanstalk, lihat [AWS Elastic Beanstalk Panduan Pengembang](#).

Untuk memilih sertifikat, Anda harus mengonfigurasi penyeimbang beban untuk aplikasi Anda di konsol Elastic Beanstalk. Untuk informasi selengkapnya, lihat [Mengonfigurasi Load Balancer Lingkungan Elastic Beanstalk Anda untuk Dihentikan. HTTPS](#)

## AWS App Runner

App Runner adalah AWS layanan yang menyediakan cara cepat, sederhana, dan hemat biaya untuk menyebarkan dari kode sumber atau gambar kontainer langsung ke aplikasi web yang dapat diskalakan dan aman di AWS Awan. Anda tidak perlu mempelajari teknologi baru, memutuskan layanan komputasi mana yang akan digunakan, atau mengetahui cara menyediakan dan mengonfigurasi AWS sumber daya. Untuk informasi selengkapnya tentang App Runner, lihat [AWS App Runner Panduan Pengembang](#).

Saat Anda mengaitkan nama domain kustom dengan layanan App Runner, App Runner secara internal membuat sertifikat yang melacak validitas domain. Mereka disimpan di ACM. App Runner tidak menghapus sertifikat ini selama tujuh hari setelah domain dipisahkan dari layanan Anda atau setelah layanan dihapus. Seluruh proses ini otomatis dan Anda tidak perlu menambahkan atau mengelola sertifikat apa pun sendiri. Untuk informasi selengkapnya, lihat [Mengelola nama domain khusus untuk layanan Pelari Aplikasi](#) di AWS App Runner Panduan Pengembang.

## API Gerbang Amazon

Dengan menjamurnya perangkat seluler dan pertumbuhan Internet of Things (IoT), telah menjadi semakin umum untuk APIs membuat yang dapat digunakan untuk mengakses data dan berinteraksi dengan sistem back-end pada AWS. Anda dapat menggunakan API Gateway untuk mempublikasikan, memelihara, memantau, dan mengamankan Anda APIs. Setelah menerapkan API ke API Gateway, Anda dapat [menyiapkan nama domain khusus](#) untuk menyederhanakan akses ke Gateway. Untuk menyiapkan nama domain kustom, Anda harus memberikan TLS sertifikat SSL/. Anda dapat menggunakan ACM untuk menghasilkan atau mengimpor sertifikat. Untuk informasi selengkapnya tentang Amazon API Gateway, lihat [Panduan Pengembang Amazon API Gateway](#).

## AWS Enklaf Nitro

AWS Nitro Enclave adalah EC2 fitur Amazon yang memungkinkan Anda membuat lingkungan eksekusi terisolasi, yang disebut kantong, dari instans Amazon. EC2 Enklave adalah mesin virtual yang terpisah, mengeras, dan sangat dibatasi. Mereka hanya menyediakan konektivitas soket lokal yang aman dengan instance induknya. Mereka tidak memiliki penyimpanan persisten, akses interaktif, atau jaringan eksternal. Pengguna tidak dapat SSH masuk ke dalam enclave, dan data serta aplikasi di dalam enclave tidak dapat diakses oleh proses, aplikasi, atau pengguna instans induk (termasuk root atau admin).

EC2 instance yang terhubung ke sertifikat dukungan Nitro Enclave. ACM Untuk informasi selengkapnya, silakan lihat [AWS Certificate Manager untuk Nitro](#) Enclave.



**Note**

Anda tidak dapat mengaitkan ACM sertifikat dengan EC2 instance yang tidak terhubung ke Enclave Nitro.

## AWS CloudFormation

AWS CloudFormation membantu Anda memodelkan dan menyiapkan sumber daya Amazon Web Services Anda. Anda membuat template yang menggambarkan AWS sumber daya yang ingin Anda gunakan, seperti Elastic Load Balancing atau API Gateway. Maka AWS CloudFormation mengurus penyediaan dan konfigurasi sumber daya tersebut untuk Anda. Anda tidak perlu membuat dan mengonfigurasi secara individual AWS sumber daya dan mencari tahu apa yang tergantung pada apa; AWS CloudFormation menangani semua itu. ACMsertifikat disertakan sebagai sumber daya template, yang berarti bahwa AWS CloudFormation dapat meminta ACM sertifikat yang dapat Anda gunakan AWS layanan untuk mengaktifkan koneksi yang aman. Selain itu, ACM sertifikat disertakan dengan banyak AWS sumber daya yang dapat Anda atur AWS CloudFormation.

Untuk informasi umum tentang CloudFormation, lihat [AWS CloudFormation Panduan Pengguna](#). Untuk informasi tentang ACM sumber daya yang didukung oleh CloudFormation, lihat [AWS::CertificateManager: :Certificate](#).

Dengan otomatisasi kuat yang disediakan oleh AWS CloudFormation, mudah untuk melebihi [kuota sertifikat](#) Anda, terutama dengan yang baru AWS akun. Kami menyarankan Anda mengikuti [praktik ACM terbaik](#) untuk AWS CloudFormation.

**Note**

Jika Anda membuat ACM sertifikat dengan AWS CloudFormation, AWS CloudFormation tumpukan tetap dalam status CREATE\_IN\_PROGRESS. Setiap operasi tumpukan lebih lanjut ditunda sampai Anda menindaklanjuti instruksi dalam email validasi sertifikat. Untuk informasi selengkapnya, lihat [Sumber Daya Gagal Menstabilkan Selama Operasi Membuat, Memperbarui, atau Menghapus Tumpukan](#).

## AWS Amplify

Amplify adalah seperangkat alat dan fitur yang dibuat khusus yang memungkinkan pengembang web dan seluler front-end untuk dengan cepat dan mudah membangun aplikasi full-stack AWS. Amplify menyediakan dua layanan: Amplify Hosting dan Amplify Studio. Amplify Hosting menyediakan alur kerja berbasis git untuk menghosting aplikasi web tanpa server full-stack dengan penerapan berkelanjutan. Amplify Studio adalah lingkungan pengembangan visual yang menyederhanakan pembuatan aplikasi web dan seluler full-stack yang dapat diskalakan. Gunakan Studio untuk membangun UI front-end Anda dengan satu set komponen ready-to-use UI, buat backend aplikasi, lalu sambungkan keduanya bersama-sama. Untuk informasi selengkapnya tentang Amplify, lihat [AWS Amplify Panduan Pengguna](#).

Jika Anda menghubungkan domain kustom ke aplikasi, konsol Amplify akan mengeluarkan ACM sertifikat untuk mengamankannya.

## OpenSearch Layanan Amazon

Amazon OpenSearch Service adalah mesin pencari dan analitik untuk kasus penggunaan seperti analisis log, pemantauan aplikasi real-time, dan analisis aliran klik. Untuk informasi selengkapnya, lihat [Panduan Pengembang OpenSearch Layanan Amazon](#).

Saat membuat kluster OpenSearch Layanan yang berisi [domain kustom dan titik akhir](#), Anda dapat menggunakan ACM untuk menyediakan Application Load Balancer terkait dengan sertifikat.

## AWS Network Firewall

AWS Network Firewall adalah layanan terkelola yang memudahkan penerapan perlindungan jaringan penting untuk semua Amazon Virtual Private Clouds (VPCs) Anda. Untuk informasi selengkapnya tentang Network Firewall, lihat [AWS Network Firewall Panduan Pengembang](#).

Network Firewall terintegrasi dengan ACM untuk TLS inspeksi. Jika Anda menggunakan TLS inspeksi di Network Firewall, Anda harus mengonfigurasi ACM sertifikat untuk dekripsi dan enkripsi ulang SSL/TLS lalu lintas yang melalui firewall Anda. Untuk informasi tentang cara kerja Network Firewall ACM untuk TLS pemeriksaan, lihat [Persyaratan untuk menggunakan SSL/TLS sertifikat dengan konfigurasi TLS inspeksi](#) di AWS Network Firewall Panduan Pengembang.

# Keamanan di AWS Certificate Manager

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan kamu. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- **Keamanan Cloud** — AWS Bertanggung jawab untuk melindungi infrastruktur yang berjalan AWS layanan di AWS Awan. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [AWS Program Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Certificate Manager, lihat [AWS Layanan dalam Lingkup oleh Program Kepatuhan](#) .
- **Keamanan di cloud** — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Certificate Manager (ACM). Topik berikut menunjukkan cara mengonfigurasi ACM untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan yang lain AWS layanan yang membantu Anda memantau dan mengamankan ACM sumber daya Anda.

## Topik

- [Perlindungan data di AWS Certificate Manager](#)
- [Identity and Access Management untuk AWS Certificate Manager](#)
- [Ketahanan di AWS Certificate Manager](#)
- [Keamanan infrastruktur di AWS Certificate Manager](#)
- [Praktik terbaik](#)

# Perlindungan data di AWS Certificate Manager

Bagian AWS [model tanggung jawab bersama model](#) berlaku untuk perlindungan data di AWS Certificate Manager. Seperti yang dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [Privasi Data FAQ](#). Untuk informasi tentang perlindungan data di Eropa, lihat [AWS Model Tanggung Jawab Bersama dan posting GDPR](#) blog di AWS Blog Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS kegiatan, lihat [Bekerja dengan CloudTrail jalan setapak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan AWS solusi enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan FIPS titik akhir. Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat [Federal Information Processing Standard \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan ACM atau lainnya Layanan AWS menggunakan konsol, API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensi dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

## Keamanan untuk kunci pribadi sertifikat

Ketika Anda [meminta sertifikat publik](#), AWS Certificate Manager (ACM) menghasilkan public/private key pair. Untuk [sertifikat yang diimpor](#), Anda menghasilkan key pair. Kunci publik menjadi bagian dari sertifikat. ACM menyimpan sertifikat dan kunci pribadi yang sesuai, dan menggunakan AWS Key Management Service (AWS KMS) untuk membantu melindungi kunci pribadi. Prosesnya bekerja seperti ini:

1. Pertama kali Anda meminta atau mengimpor sertifikat dalam AWS Wilayah, ACM membuat terkelola AWS KMS key dengan alias `aws/acm`. KMS Kunci ini unik di setiap AWS akun dan masing-masing AWS Wilayah.
2. ACM menggunakan KMS kunci ini untuk mengenkripsi kunci pribadi sertifikat. ACM hanya menyimpan versi terenkripsi dari kunci pribadi; ACM tidak menyimpan kunci pribadi dalam bentuk teks biasa. ACM menggunakan KMS kunci yang sama untuk mengenkripsi kunci pribadi untuk semua sertifikat dalam suatu AWS akun dan spesifik AWS Wilayah.
3. Ketika Anda mengaitkan sertifikat dengan layanan yang terintegrasi dengan AWS Certificate Manager, ACM mengirimkan sertifikat dan kunci pribadi terenkripsi ke layanan. Hibah juga dibuat di AWS KMS yang memungkinkan layanan untuk menggunakan KMS kunci untuk mendekripsi kunci pribadi sertifikat. Untuk informasi selengkapnya tentang hibah, lihat [Menggunakan Hibah](#) di AWS Key Management Service Panduan Pengembang. Untuk informasi selengkapnya tentang layanan yang didukung oleh ACM, lihat [Layanan terintegrasi dengan ACM](#).

### Note

Anda memiliki kendali atas yang dibuat secara otomatis AWS KMS hibah. Jika Anda menghapus hibah ini karena alasan apa pun, Anda kehilangan ACM fungsionalitas untuk layanan terintegrasi.

4. Layanan terintegrasi menggunakan KMS kunci untuk mendekripsi kunci pribadi. Kemudian layanan menggunakan sertifikat dan kunci pribadi yang didekripsi (plaintext) untuk membangun saluran komunikasi yang aman (SSL/TLS sesi) dengan kliennya.

5. Ketika sertifikat dipisahkan dari layanan terintegrasi, hibah yang dibuat pada langkah 3 dihentikan. Ini berarti layanan tidak dapat lagi menggunakan KMS kunci untuk mendekripsi kunci pribadi sertifikat.

## Identity and Access Management untuk AWS Certificate Manager

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAM administrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. ACM IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

### Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Certificate Manager bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#)
- [Izin API ACM: Referensi tindakan dan sumber daya](#)
- [Kebijakan terkelola AWS untuk AWS Certificate Manager](#)
- [Gunakan tombol kondisi dengan ACM](#)
- [Menggunakan peran terkait layanan \( \) SLR dengan ACM](#)
- [Memecahkan masalah AWS Certificate Manager identitas dan akses](#)

## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan ACM.

Pengguna layanan – Jika Anda menggunakan layanan ACM untuk melakukan tugas Anda, administrator Anda akan memberikan kredensial dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur ACM untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di ACM, lihat [Memecahkan masalah AWS Certificate Manager identitas dan akses](#).

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya ACM di perusahaan Anda, Anda mungkin memiliki akses penuh ke ACM. Tugas Anda adalah menentukan fitur dan sumber daya ACM mana yang harus diakses oleh pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakannya IAMACM, lihat [Bagaimana AWS Certificate Manager bekerja dengan IAM](#).

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ACM. Untuk melihat contoh kebijakan ACM berbasis identitas yang dapat Anda gunakan, lihat. IAM [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#)

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Versi AWS Tanda Tangan 4 untuk API permintaan](#) di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-



faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) di Panduan AWS IAM Identity Center Pengguna dan [Autentikasi AWS multi-faktor IAM di Panduan Pengguna](#). IAM

## Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) di IAMPanduan Pengguna.

## Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat [Apa itu Pusat IAM Identitas?](#) dalam AWS IAM Identity Center User Guide.

## Pengguna dan grup IAM

[IAMPengguna](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensial sementara daripada membuat IAM pengguna yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya,



lihat [Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang](#) di IAMPanduan Pengguna.

[IAMGrup](#) adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdmins dan memberikan izin grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk IAM pengguna](#) di Panduan IAM Pengguna.

## Peran IAM

[IAMPeran](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Untuk mengambil IAM peran sementara di dalam AWS Management Console, Anda dapat [beralih dari pengguna ke IAM peran \(konsol\)](#). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustom URL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara

utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FAS permintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).
- Peran layanan — Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon](#) di IAMPanduan Pengguna.

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat [Ringkasan JSON kebijakan](#) di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

### Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna](#). IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat [Memilih antara kebijakan terkelola dan kebijakan sebaris](#) di IAMPanduan Pengguna.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

## Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ikhtisar daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

## Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batas izin** — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang Principal tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat [Batas izin untuk IAM entitas](#) di IAMPanduan Pengguna.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations

adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP Membatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah JSON kebijakan yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui IAM kebijakan yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP Membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) di Panduan IAM Pengguna.

## Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan IAM Pengguna.

## Bagaimana AWS Certificate Manager bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ACM, pelajari IAM fitur apa yang tersedia untuk digunakan ACM.

## IAMfitur yang dapat Anda gunakan dengan AWS Certificate Manager

IAMfitur	Dukungan ACM
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">kunci-kunci persyaratan kebijakan (spesifik layanan)</a>	Ya
<a href="#">ACLs</a>	Tidak
<a href="#">ABAC(tag dalam kebijakan)</a>	Parsial
<a href="#">Kredensial sementara</a>	Ya
<a href="#">Izin principal</a>	Ya
<a href="#">Peran layanan</a>	Tidak
<a href="#">Peran terkait layanan</a>	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara ACM dan AWS layanan lain bekerja dengan sebagian besar IAM fitur, lihat [AWS layanan yang berfungsi IAM](#) di Panduan IAM Pengguna.

## Kebijakan berbasis identitas untuk ACM

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna](#). IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat [referensi elemen IAM JSON kebijakan](#) di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk ACM

Untuk melihat contoh ACM kebijakan berbasis identitas, lihat [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#).

## Kebijakan berbasis sumber daya dalam ACM

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai penanggung jawab kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun IAM di](#) Panduan IAM Pengguna.

## Tindakan kebijakan untuk ACM

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

ActionElemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar ACM tindakan, lihat [Tindakan yang ditentukan oleh AWS Certificate Manager](#) dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di ACM menggunakan prefiks berikut sebelum tindakan:

```
acm
```

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma.

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

Untuk melihat contoh ACM kebijakan berbasis identitas, lihat [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#).

## Sumber daya kebijakan untuk ACM

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.



Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (\*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya dan jenis ACM sumber daya ARNs, lihat [Sumber daya yang ditentukan oleh AWS Certificate Manager](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Certificate Manager](#).

Untuk melihat contoh ACM kebijakan berbasis identitas, lihat [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#).

## Kunci syarat kebijakan untuk ACM

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat [elemen IAM kebijakan: variabel dan tag](#) di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan IAM Pengguna.

Untuk melihat daftar kunci ACM kondisi, lihat [Kunci kondisi untuk AWS Certificate Manager](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh AWS Certificate Manager](#).

Untuk melihat contoh ACM kebijakan berbasis identitas, lihat [Contoh kebijakan berbasis identitas untuk AWS Certificate Manager](#).

## ACLs di ACM

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

## ABAC dengan ACM

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC membantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya ABAC, lihat [Menentukan izin dengan ABAC otorisasi](#) di IAMPanduan Pengguna. Untuk melihat tutorial dengan langkah-langkah penyiapan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di IAMPanduan Pengguna.

## Menggunakan kredensial sementara dengan ACM

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensil sementara, lihat [Layanan AWS yang berfungsi IAM](#) di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat [Beralih dari pengguna ke IAM peran \(konsol\)](#) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensi keamanan sementara](#) di. IAM

## Izin principal lintas layanan untuk ACM

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima

permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

## Peran layanan untuk ACM

Mendukung peran layanan: Tidak

Peran layanan adalah [IAMperan](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam IAMPanduan Pengguna.

### Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas ACM. Edit peran layanan hanya jika ACM memberikan bimbingan untuk melakukannya.

## Peran yang terhubung dengan layanan untuk ACM

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat [AWS layanan yang berfungsi](#) dengannya. IAM Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

## Contoh kebijakan berbasis identitas untuk AWS Certificate Manager

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya ACM. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat

membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat [Membuat JSON IAM kebijakan \(konsol\) di Panduan Pengguna](#). IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh ACM, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk AWS Certificate Manager](#) dalam Referensi Otorisasi Layanan.

## Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol ACM](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Sertifikat daftar](#)
- [Mengambil sertifikat](#)
- [Mengimpor sertifikat](#)
- [Menghapus sertifikat](#)

## Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya ACM yang ada di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan AWS terkelola](#) atau [kebijakan terkelola untuk fungsi pekerjaan](#) di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu,

yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat [Kebijakan dan izin IAM di IAM](#) Panduan Pengguna.

- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [elemen IAM JSON kebijakan: Kondisi](#) dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa IAM kebijakan ( ) JSON dan praktik terbaik. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Memvalidasi kebijakan dengan IAM Access Analyzer](#) di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di dalam Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat [API Akses aman dengan MFA](#) di Panduan IAM Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik di IAM, lihat [Praktik terbaik keamanan IAM di](#) Panduan IAM Pengguna.

## Menggunakan konsol ACM

Untuk mengakses AWS Certificate Manager konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang ACM sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan ACM konsol, lampirkan juga kebijakan ACM *AWSCertificateManagerReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) di Panduan IAM Pengguna.

## Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI AWS API

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

```
}
```

## Sertifikat daftar

Kebijakan berikut memungkinkan pengguna untuk mencantumkan semua ACM sertifikat di akun pengguna.

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

### Note

Izin ini diperlukan agar ACM sertifikat muncul di Elastic Load Balancing dan CloudFront konsol.

## Mengambil sertifikat

Kebijakan berikut memungkinkan pengguna untuk mengambil ACM sertifikat tertentu.

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

## Mengimpor sertifikat

Kebijakan berikut memungkinkan pengguna untuk mengimpor sertifikat.



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

## Menghapus sertifikat

Kebijakan berikut memungkinkan pengguna untuk menghapus ACM sertifikat tertentu.

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

## Izin API ACM: Referensi tindakan dan sumber daya

Saat menyiapkan kontrol akses dan kebijakan izin tulis yang dapat dilampirkan ke pengguna atau peran IAM, Anda dapat menggunakan tabel berikut sebagai referensi. Kolom pertama dalam tabel mencantumkan masing-masing AWS Certificate Manager Operasi API. Anda menentukan tindakan di elemen `Action` kebijakan. Kolom yang tersisa memberikan informasi tambahan:

Anda dapat menggunakan elemen kebijakan IAM dalam kebijakan ACM Anda untuk menyatakan kondisi. Untuk daftar lengkapnya, lihat [Kunci yang Tersedia](#) dalam Panduan Pengguna IAM.

### Note

Untuk menentukan tindakan, gunakan awalan `acm:` diikuti dengan nama operasi API (misalnya, `acm:RequestCertificate`).

## Operasi dan izin API ACM

Operasi API ACM	Izin yang Diperlukan (Operasi API)	Sumber daya
<a href="#">AddTagsToCertificate</a>	acm:AddTagsToCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">DeleteCertificate</a>	acm:DeleteCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">DescribeCertificate</a>	acm:DescribeCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">ExportCertificate</a>	acm:ExportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">GetAccountConfiguration</a>	acm:GetAccountConfiguration	*
<a href="#">GetCertificate</a>	acm:GetCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">ImportCertificate</a>	acm:ImportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/*  or  *
<a href="#">ListCertificates</a>	acm:ListCertificates	*

Operasi API ACM	Izin yang Diperlukan (Operasi API)	Sumber daya
<a href="#">ListTagsForCertificate</a>	acm:ListTagsForCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">PutAccountConfiguration</a>	acm:PutAccountConfiguration	*
<a href="#">RemoveTagsFromCertificate</a>	acm:RemoveTagsFromCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">RequestCertificate</a>	acm:RequestCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/* or *
<a href="#">ResendValidationEmail</a>	acm:ResendValidationEmail	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">UpdateCertificateOptions</a>	acm:UpdateCertificateOptions	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>

## Kebijakan terkelola AWS untuk AWS Certificate Manager

Sebuah AWS kebijakan terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa AWS kebijakan terkelola mungkin tidak memberikan izin paling sedikit hak istimewa untuk kasus penggunaan spesifik Anda karena tersedia untuk semua AWS pelanggan untuk digunakan. Kami menyarankan Anda mengurangi izin lebih lanjut dengan mendefinisikan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam AWS kebijakan yang dikelola. Jika AWS memperbarui izin yang didefinisikan dalam AWS kebijakan terkelola, pembaruan mempengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan. AWS kemungkinan besar akan memperbarui AWS kebijakan terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

## AWSCertificateManagerReadOnly

Kebijakan ini menyediakan akses hanya-baca ke sertifikat ACM; memungkinkan pengguna untuk menjelaskan, mencantumkan, dan mengambil sertifikat ACM.

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

Untuk melihat ini AWS kebijakan terkelola di konsol, pergi ke <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly>.

## AWSCertificateManagerFullAccess

Kebijakan ini menyediakan akses penuh ke semua tindakan dan sumber daya ACM.

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

Untuk melihat ini AWS kebijakan terkelola di konsol, pergi ke <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess>.

## ACM updateAWSkebijakan terkelola

Lihat detail tentang pembaruanAWSkebijakan terkelola untuk ACM sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di ACM [Riwayat dokumen](#) halaman.

Perubahan	Deskripsi	Tanggal
DitambahkanGetAccountConfiguration dukungan untuk <a href="#">AWSCertificateManagerReadOnly</a> kebijakan.	YangAWSCertificateManagerReadOnly kebijakan sekarang termasuk izin untuk memanggilGetAccountConfiguration Tindakan API.	3 Maret 2021
ACM mulai melacak perubahan	ACM mulai melacak perubahanAWSkebijakan yang dikelola.	3 Maret 2021

## Gunakan tombol kondisi dengan ACM

AWS Certificate Manager menggunakan AWS Identity and Access Management (IAM) [kunci kondisi](#) untuk membatasi akses ke permintaan sertifikat. Dengan kunci kondisi dari IAM kebijakan atau Kebijakan Kontrol Layanan (SCP), Anda dapat membuat permintaan sertifikat yang sesuai dengan pedoman organisasi Anda.

### Note

Gabungkan tombol ACM kondisi dengan AWS [kunci kondisi global](#) seperti `aws:PrincipalArn` untuk membatasi tindakan lebih lanjut untuk pengguna atau peran tertentu.

## Kondisi yang didukung untuk ACM

### ACMAPIOperasi dan kondisi yang didukung

Kunci Syarat	ACMAPIOperasi yang Didukung	Tipe	Deskripsi
acm:ValidationMethod	<a href="#">RequestCertificate</a>	Tali (EMAIL,DNS)	Filter permintaan berdasarkan metode ACM <a href="#">validasi</a>
acm:DomainNames	<a href="#">RequestCertificate</a>	ArrayOfString	Filter berdasarkan <a href="#">nama domain</a> dalam ACM permintaan
acm:KeyAlgorithm	<a href="#">RequestCertificate</a>	String	Filter permintaan berdasarkan <a href="#">algoritma dan ukuran ACM kunci</a>
acm:CertificateTransparencyLogging	<a href="#">RequestCertificate</a>	Tali (ENABLED,DISABLED)	Filter permintaan berdasarkan <a href="#">preferensi logging transparansi ACM sertifikat</a>
acm:CertificateAuthority	<a href="#">RequestCertificate</a>	ARN	Filter permintaan berdasarkan <a href="#">otoritas sertifikat</a> dalam ACM permintaan

### Contoh 1: Membatasi metode validasi

Kebijakan berikut menolak permintaan sertifikat baru menggunakan metode [Validasi Email](#) kecuali permintaan yang dibuat menggunakan peran. `arn:aws:iam::123456789012:role/AllowedEmailValidation`

```
{
```

```

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

```

## Contoh 2: Mencegah domain wildcard

Kebijakan berikut menolak permintaan ACM sertifikat baru yang menggunakan domain wildcard.

```

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

```



### Contoh 3: Membatasi domain sertifikat

Kebijakan berikut menolak permintaan ACM sertifikat baru untuk domain yang tidak diakhiri dengan `*.amazonaws.com`

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

Kebijakan ini dapat dibatasi lebih lanjut untuk subdomain tertentu. Kebijakan ini hanya mengizinkan permintaan di mana setiap domain cocok dengan setidaknya satu dari nama domain bersyarat.

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

## Contoh 4: Membatasi algoritma kunci

Kebijakan berikut menggunakan kunci kondisi `StringNotLike` untuk mengizinkan hanya sertifikat yang diminta dengan algoritma kunci ECDSA 384 bit (`EC_secp384r1`).

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

Kebijakan berikut menggunakan kunci kondisi `StringLike` dan `*` pencocokan wildcard untuk mencegah permintaan sertifikat baru ACM dengan algoritma RSA kunci apa pun.

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

## Contoh 5: Membatasi otoritas sertifikat

Kebijakan berikut hanya akan mengizinkan permintaan sertifikat pribadi menggunakan Private Certificate Authority (PCA) yang disediakan ARN.

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

Kebijakan ini menggunakan `acm:CertificateAuthority` ketentuan untuk hanya mengizinkan permintaan sertifikat tepercaya publik yang dikeluarkan oleh Amazon Trust Services. Mengatur Otoritas Sertifikat ARN untuk `false` mencegah permintaan sertifikat pribadi PCA.

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

## Menggunakan peran terkait layanan ( ) SLR dengan ACM

AWS Certificate Manager menggunakan AWS Identity and Access Management (IAM) [peran terkait layanan](#) untuk mengaktifkan perpanjangan otomatis sertifikat pribadi yang dikeluarkan dari CA pribadi untuk akun lain yang dibagikan oleh AWS Resource Access Manager. Peran terkait layanan (SLR) adalah IAM peran yang ditautkan langsung ke layanan. ACM SLR setelah ditentukan sebelumnya oleh ACM dan menyertakan semua izin yang diperlukan layanan untuk memanggil lainnya AWS layanan atas nama Anda.

SLR ini membuat pengaturan ACM lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual untuk penandatanganan sertifikat tanpa pengawasan. ACM mendefinisikan izinnya SLR, dan kecuali ditentukan lain, hanya ACM dapat mengambil peran. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain mana pun. IAM

Untuk informasi tentang layanan lain yang mendukung SLRs, lihat [AWS Layanan yang Bekerja dengan IAM](#) dan mencari layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya dengan tautan untuk melihat SLR dokumentasi untuk layanan itu.

### SLR izin untuk ACM

ACM menggunakan Kebijakan Peran Layanan Amazon Certificate Manager SLR bernama.

AWS Service Role For Certificate Manager SLR Percayakan layanan berikut untuk mengambil peran:

- `acm.amazonaws.com`

Kebijakan izin peran memungkinkan ACM untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` pada "\*" "

Anda harus mengonfigurasi izin untuk mengizinkan IAM entitas (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus. SLR Untuk informasi selengkapnya, lihat [Izin Peran Tertaut Layanan](#) di Panduan Pengguna. IAM

**⚠ Important**

ACM mungkin mengingatkan Anda bahwa itu tidak dapat menentukan apakah SLR ada di akun Anda. Jika `iam:GetRole` izin yang diperlukan telah diberikan kepada akun Anda, maka peringatan tidak akan terulang kembali setelah SLR dibuat. ACM SLR Jika terulang kembali, Anda atau administrator akun Anda mungkin perlu memberikan `iam:GetRole` izin ACM, atau mengaitkan akun Anda dengan kebijakan ACM -managed. `AWSCertificateManagerFullAccess`

## Menciptakan SLR untuk ACM

Anda tidak perlu membuat SLR yang ACM menggunakan secara manual. Saat Anda mengeluarkan ACM sertifikat menggunakan AWS Management Console, AWS CLI, atau AWS API, ACM membuat SLR untuk Anda pertama kalinya bahwa Anda CA pribadi untuk akun lain yang dibagikan oleh AWS RAM untuk menandatangani sertifikat Anda.

Jika Anda menemukan pesan yang menyatakan bahwa ACM tidak dapat menentukan apakah SLR ada di akun Anda, itu mungkin berarti bahwa akun Anda belum memberikan izin baca AWS Private CA membutuhkan. Ini tidak akan mencegah agar tidak diinstal, dan Anda masih dapat menerbitkan sertifikat, tetapi tidak ACM akan dapat memperbarui sertifikat secara otomatis sampai Anda menyelesaikan masalah. SLR Untuk informasi selengkapnya, lihat [Masalah dengan peran ACM terkait layanan \(\) SLR](#).

**⚠ Important**

Ini SLR dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang didukung oleh peran ini. Juga, jika Anda menggunakan ACM layanan sebelum 1 Januari 2017, ketika mulai mendukung SLRs, maka ACM buat `AWSServiceRoleForCertificateManager` peran di akun Anda. Untuk mempelajari lebih lanjut, lihat [Peran Baru Muncul di IAM Akun Saya](#).

Jika Anda menghapus ini SLR, dan kemudian perlu membuatnya lagi, Anda dapat menggunakan salah satu dari metode ini:

- Di IAM konsol, pilih Peran, Buat peran, Certificate Manager untuk membuat peran baru dengan kasus `CertificateManagerServiceRolePolicy` penggunaan.

- Menggunakan IAM API [CreateServiceLinkedRole](#) atau yang sesuai AWS CLI perintah [create-service-linked-role](#), buat SLR dengan nama `acm.amazonaws.com` layanan.

Untuk informasi selengkapnya, lihat [Membuat Peran Tertaut Layanan](#) di IAMPanduan Pengguna.

## Mengedit SLR untuk ACM

ACM tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForCertificateManager` terkait layanan. Setelah membuat SLR, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit Peran Tertaut Layanan](#) di IAMPanduan Pengguna.

## Menghapus untuk SLR ACM

Anda biasanya tidak perlu menghapus file `AWSServiceRoleForCertificateManager` SLR. Namun, Anda dapat menghapus peran secara manual menggunakan IAM konsol, AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Menghapus Peran Tertaut Layanan](#) di Panduan Pengguna. IAM

## Wilayah yang Didukung untuk ACM SLRs

ACM mendukung penggunaan SLRs di semua wilayah di mana keduanya ACM dan AWS Private CA tersedia. Untuk informasi selengkapnya, silakan lihat [AWS Wilayah dan Titik Akhir](#).

Nama Wilayah	Identitas wilayah	Support di ACM
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya

Nama Wilayah	Identitas wilayah	Support di ACM
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Zürich)	eu-central-2	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Europe (Paris)	eu-west-3	Ya
South America (São Paulo)	sa-east-1	Ya
AWS GovCloud (AS-Barat)	us-gov-west-1	Ya
AWS GovCloud (AS-Timur) Timur	us-gov-east-1	Ya

## Memecahkan masalah AWS Certificate Manager identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan ACM dan IAM.

### Topik

- [Saya tidak diotorisasi untuk melakukan tindakan di ACM](#)
- [Saya tidak berwenang untuk meminta sertifikat di ACM](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses ACM sumber daya saya](#)

## Saya tidak diotorisasi untuk melakukan tindakan di ACM

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang `my-example-widget` sumber daya fiksi tetapi tidak memiliki izin `acm:GetWidget` fiksi.

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `acm:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya tidak berwenang untuk meminta sertifikat di ACM

Jika Anda menerima kesalahan ini, administrator Anda ACM atau PKI administrator telah menetapkan aturan yang mencegah Anda meminta sertifikat dalam keadaan saat ini.

Contoh kesalahan berikut terjadi ketika IAM pengguna mencoba menggunakan konsol untuk meminta sertifikat menggunakan opsi yang dikonfigurasi DENY dengan administrator organisasi.

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

Dalam hal ini permintaan harus dibuat lagi dengan cara yang sejalan dengan kebijakan yang ditetapkan oleh administrator Anda. Atau kebijakan perlu diperbarui untuk memungkinkan meminta sertifikat.

## Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ACM.



Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di ACM. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses ACM sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah ACM mendukung fitur-fitur ini, lihat [Bagaimana AWS Certificate Manager bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki](#) di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna yang diautentikasi secara eksternal \(federasi identitas\) di Panduan Pengguna](#). IAM

- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM

## Ketahanan di AWS Certificate Manager

Bagian AWS Infrastruktur global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan jaringan berlatensi rendah, throughput yang tinggi, dan sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi lebih lanjut tentang AWS Wilayah dan Availability Zone, lihat [AWS Infrastruktur Global](#).

## Keamanan infrastruktur di AWS Certificate Manager

Sebagai layanan yang dikelola, AWS Certificate Manager dilindungi oleh AWS keamanan jaringan global. Untuk informasi tentang AWS Layanan keamanan dan bagaimana AWS melindungi infrastruktur, lihat [AWS Keamanan Cloud](#). Untuk mendesain Anda AWS lingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur](#) di Pilar Keamanan AWS Kerangka Kerja yang Diarsiteksikan dengan Baik.

Anda menggunakan AWS API panggilan yang diterbitkan untuk mengakses ACM melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

## Memberikan akses programatif ke ACM

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi AWS di luar AWS Management Console. Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna dikelola di Pusat IAM Identitas)	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDKs, atau AWS APIs.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. <ul style="list-style-type: none"> <li>Untuk AWS CLI, lihat <a href="#">Mengkonfigurasi AWS CLI untuk menggunakan AWS IAM Identity Center</a> di AWS Command Line Interface Panduan Pengguna.</li> <li>Untuk AWS SDKs, alat, dan AWS APIs, lihat <a href="#">otentikasi di Pusat IAM Identitas</a> di AWS SDKs dan Panduan Referensi Alat.</li> </ul>
IAM	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDKs, atau AWS APIs.	Mengikuti petunjuk dalam <a href="#">Menggunakan kredensial sementara dengan AWS sumber daya</a> dalam Panduan IAM Pengguna.
IAM	(Tidak direkomendasikan) Gunakan kredensi jangka panjang untuk menandatangani permintaan terprogram	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
	ke AWS CLI, AWS SDKs, atau AWS APIs.	<ul style="list-style-type: none"> <li>• Untuk AWS CLI, lihat <a href="#">Mengautentikasi menggunakan kredensi IAM pengguna</a> di AWS Command Line Interface Panduan Pengguna.</li> <li>• Untuk AWS SDKs dan alat, lihat <a href="#">Mengautentikasi menggunakan kredensi jangka panjang</a> di AWS SDKs dan Panduan Referensi Alat.</li> <li>• Untuk AWS APIs, lihat <a href="#">Mengelola kunci akses untuk IAM pengguna</a> di Panduan IAM Pengguna.</li> </ul>

## Praktik terbaik

Praktik terbaik adalah rekomendasi yang dapat membantu Anda menggunakan AWS Certificate Manager (AWS Certificate Manager) lebih efektif. Praktik terbaik berikut didasarkan pada pengalaman dunia nyata dari ACM pelanggan saat ini.

### Topik

- [Pemisahan tingkat akun](#)
- [AWS CloudFormation](#)
- [Penyematan sertifikat](#)
- [Validasi domain](#)
- [Menambahkan atau menghapus nama domain](#)
- [Memilih keluar dari pencatatan transparansi sertifikat](#)
- [Nyalakan AWS CloudTrail](#)

## Pemisahan tingkat akun

Gunakan pemisahan tingkat akun dalam kebijakan Anda untuk mengontrol siapa yang dapat mengakses sertifikat di tingkat akun. Simpan sertifikat produksi Anda di akun terpisah dari sertifikat pengujian dan pengembangan Anda. Jika Anda tidak dapat menggunakan pemisahan tingkat akun, Anda dapat membatasi akses ke peran tertentu dengan menolak `kms:CreateGrant` tindakan dalam kebijakan Anda. Ini membatasi peran mana dalam akun yang dapat menandatangani sertifikat pada tingkat tinggi. Untuk informasi tentang hibah, termasuk terminologi hibah, lihat [Hibah di AWS KMS](#) di AWS Key Management Service Panduan Pengembang.

Jika Anda menginginkan kontrol yang lebih terperinci daripada membatasi penggunaan `kms:CreateGrant` berdasarkan akun, Anda dapat membatasi sertifikat tertentu `kms:CreateGrant` menggunakan [kms: EncryptionContext](#) tombol kondisi. Tentukan `arn:aws:acm` sebagai kunci, dan nilai ARN untuk membatasi. Contoh kebijakan berikut mencegah penggunaan sertifikat tertentu, tetapi mengizinkan orang lain.

```
{
  "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

Dengan AWS CloudFormation Anda dapat membuat template yang menggambarkan AWS sumber daya yang ingin Anda gunakan. AWS CloudFormation kemudian menyediakan dan mengonfigurasi sumber daya tersebut untuk Anda. AWS CloudFormation dapat menyediakan sumber daya yang

didukung oleh ACM seperti Elastic Load Balancing, Amazon CloudFront, dan Amazon Gateway. API Untuk informasi selengkapnya, lihat [Layanan terintegrasi dengan ACM](#).

Jika Anda menggunakan AWS CloudFormation untuk membuat dan menghapus beberapa lingkungan pengujian dengan cepat, kami menyarankan Anda untuk tidak membuat ACM sertifikat terpisah untuk setiap lingkungan. Melakukannya akan dengan cepat menghabiskan kuota sertifikat Anda. Untuk informasi selengkapnya, lihat [Kuota](#). Sebagai gantinya, buat sertifikat wildcard yang mencakup semua nama domain yang Anda gunakan untuk pengujian. Misalnya, jika Anda berulang kali membuat ACM sertifikat untuk nama domain yang bervariasi hanya berdasarkan nomor versi, seperti `<version>.service.example.com`, buat sertifikat wildcard tunggal untuk `<*>.service.example.com`. Sertakan sertifikat wildcard dalam template yang AWS CloudFormation digunakan untuk membuat lingkungan pengujian Anda.

## Penyematan sertifikat

Certificate pinning, kadang-kadang dikenal sebagai SSL pinning, adalah proses yang dapat Anda gunakan dalam aplikasi Anda untuk memvalidasi host jarak jauh dengan mengaitkan host tersebut secara langsung dengan sertifikat X.509 atau kunci publik alih-alih dengan hierarki sertifikat. Oleh karena itu aplikasi menggunakan pin untuk mem-bypass SSL /validasi rantai TLS sertifikat. Proses SSL validasi tipikal memeriksa tanda tangan di seluruh rantai sertifikat dari sertifikat root certificate authority (CA) melalui sertifikat CA bawahan, jika ada. Ini juga memeriksa sertifikat untuk host jarak jauh di bagian bawah hierarki. Aplikasi Anda dapat menyematkan ke sertifikat untuk host jarak jauh untuk mengatakan bahwa hanya sertifikat itu dan bukan sertifikat root atau lainnya dalam rantai yang dipercaya. Anda dapat menambahkan sertifikat host jarak jauh atau kunci publik ke aplikasi Anda selama pengembangan. Atau, aplikasi dapat menambahkan sertifikat atau kunci saat pertama kali terhubung ke host.

### Warning

Kami menyarankan agar aplikasi Anda tidak menyematkan ACM sertifikat. ACM melakukan [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#) untuk secara otomatis memperbarui TLS sertifikat yang dikeluarkan Amazon Anda sebelum SSL kedaluwarsa. Untuk memperbarui sertifikat, buat key ACM pair public-private baru. Jika aplikasi Anda menyematkan ACM sertifikat dan sertifikat berhasil diperbarui dengan kunci publik baru, aplikasi mungkin tidak dapat terhubung ke domain Anda.

Jika Anda memutuskan untuk menyematkan sertifikat, opsi berikut tidak akan menghalangi aplikasi Anda untuk terhubung ke domain Anda:

- [Impor sertifikat Anda sendiri](#) ke dalam ACM dan kemudian pin aplikasi Anda ke sertifikat yang diimpor. ACM tidak mencoba memperbarui sertifikat yang diimpor secara otomatis.
- Jika Anda menggunakan sertifikat publik, sematkan aplikasi Anda ke semua [sertifikat root Amazon](#) yang tersedia. Jika Anda menggunakan sertifikat pribadi, sematkan aplikasi Anda ke sertifikat root CA.

## Validasi domain

Sebelum otoritas sertifikat Amazon (CA) dapat mengeluarkan sertifikat untuk situs Anda, AWS Certificate Manager (ACM) harus memverifikasi bahwa Anda memiliki atau mengontrol semua domain yang Anda tentukan dalam permintaan Anda. Anda dapat melakukan verifikasi menggunakan email atau DNS. Untuk informasi selengkapnya, silakan lihat [AWS Certificate Manager DNS validasi](#) dan [AWS Certificate Manager validasi email](#).

## Menambahkan atau menghapus nama domain

Anda tidak dapat menambah atau menghapus nama domain dari ACM sertifikat yang ada. Sebagai gantinya, Anda harus meminta sertifikat baru dengan daftar nama domain yang direvisi. Misalnya, jika sertifikat Anda memiliki lima nama domain dan Anda ingin menambahkan empat lagi, Anda harus meminta sertifikat baru dengan sembilan nama domain. Seperti halnya sertifikat baru, Anda harus memvalidasi kepemilikan semua nama domain dalam permintaan, termasuk nama yang sebelumnya Anda validasi untuk sertifikat asli.

Jika Anda menggunakan validasi email, Anda menerima hingga 8 pesan email validasi untuk setiap domain, setidaknya 1 di antaranya harus ditindaklanjuti dalam waktu 72 jam. Misalnya, ketika Anda meminta sertifikat dengan lima nama domain, Anda menerima hingga 40 pesan validasi, setidaknya 5 di antaranya harus ditindaklanjuti dalam waktu 72 jam. Karena jumlah nama domain dalam permintaan sertifikat meningkat, demikian juga pekerjaan yang diperlukan untuk menggunakan email untuk memvalidasi kepemilikan domain.

Jika Anda menggunakan DNS validasi sebagai gantinya, Anda harus menulis satu DNS catatan baru ke database untuk yang ingin FQDN Anda validasi. ACM mengirim Anda catatan untuk membuat dan kemudian menanyakan database untuk menentukan apakah catatan telah ditambahkan. Menambahkan catatan menegaskan bahwa Anda memiliki atau mengontrol domain. Dalam contoh

sebelumnya, jika Anda meminta sertifikat dengan lima nama domain, Anda harus membuat lima DNS catatan. Kami menyarankan Anda menggunakan DNS validasi jika memungkinkan.

## Memilih keluar dari pencatatan transparansi sertifikat

### Important

Terlepas dari tindakan yang Anda ambil untuk memilih keluar dari pencatatan transparansi sertifikat, sertifikat Anda mungkin masih dicatat oleh klien atau individu mana pun yang memiliki akses ke titik akhir publik atau pribadi tempat Anda mengikat sertifikat. Namun, sertifikat tidak akan berisi cap waktu sertifikat yang ditandatangani (SCT). Hanya CA penerbit yang dapat menanamkan SCT sertifikat.

Mulai 30 April 2018, Google Chrome tidak lagi mempercayai SSL TLS publik/sertifikat yang tidak dicatat dalam log transparansi sertifikat. Oleh karena itu, mulai 24 April 2018, Amazon CA mulai menerbitkan semua sertifikat dan pembaruan baru ke setidaknya dua log publik. Setelah sertifikat dicatat, sertifikat tidak dapat dihapus. Untuk informasi selengkapnya, lihat [Pencatatan Transparansi Sertifikat](#).

Logging dilakukan secara otomatis ketika Anda meminta sertifikat atau ketika sertifikat diperbarui, tetapi Anda dapat memilih untuk memilih keluar. Alasan umum untuk melakukannya termasuk kekhawatiran tentang keamanan dan privasi. Misalnya, mencatat nama domain host internal memberikan informasi penyerang potensial tentang jaringan internal yang seharusnya tidak bersifat publik. Selain itu, logging dapat membocorkan nama-nama produk dan situs web baru atau yang belum dirilis.

[Untuk memilih keluar dari pencatatan transparansi saat Anda meminta sertifikat, gunakan options parameter sertifikat permintaan](#) AWS CLI perintah atau [RequestCertificateAPI](#) operasi. Jika sertifikat Anda dikeluarkan sebelum 24 April 2018, dan Anda ingin memastikan bahwa sertifikat tersebut tidak dicatat selama perpanjangan, Anda dapat menggunakan [update-certificate-options](#) perintah atau [UpdateCertificateOptionsAPI](#) operasi untuk memilih keluar.

### Batasan

- Anda tidak dapat menggunakan konsol untuk mengaktifkan atau menonaktifkan pencatatan transparansi.



- Anda tidak dapat mengubah status pencatatan setelah sertifikat memasuki periode perpanjangan, biasanya 60 hari sebelum sertifikat kedaluwarsa. Tidak ada pesan kesalahan yang dihasilkan jika perubahan status gagal.

Setelah sertifikat dicatat, sertifikat tidak dapat dihapus dari log. Memilih keluar pada saat itu tidak akan berpengaruh. Jika Anda memilih keluar dari logging ketika Anda meminta sertifikat dan kemudian memilih nanti untuk memilih kembali, sertifikat Anda tidak akan dicatat sampai diperpanjang. Jika Anda ingin sertifikat segera dicatat, kami sarankan Anda mengeluarkan yang baru.

Contoh berikut menunjukkan cara menggunakan perintah [request-certificate](#) untuk menonaktifkan transparansi sertifikat saat Anda meminta sertifikat baru.

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

```

Perintah sebelumnya menampilkan sertifikat baru Anda. ARN

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

Jika Anda sudah memiliki sertifikat, dan Anda tidak ingin itu dicatat ketika diperbarui, gunakan [update-certificate-options](#) perintah. Perintah ini tidak mengembalikan nilai.

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

## Nyalakan AWS CloudTrail

Aktifkan CloudTrail logging sebelum Anda mulai menggunakan ACM. CloudTrail Memungkinkan Anda untuk memantau AWS penerapan dengan mengambil riwayat AWS API panggilan untuk akun Anda, termasuk API panggilan yang dilakukan melalui AWS Konsol Manajemen, AWS SDKs, AWS Command Line Interface, dan Amazon Web Services tingkat yang lebih tinggi. Anda juga dapat mengidentifikasi pengguna dan akun mana yang disebut ACM APIs, alamat IP sumber tempat

panggilan dibuat, dan kapan panggilan terjadi. Anda dapat mengintegrasikan CloudTrail ke dalam aplikasi menggunakan API, mengotomatiskan pembuatan jejak untuk organisasi Anda, memeriksa status jejak Anda, dan mengontrol cara administrator mengaktifkan dan menonaktifkan CloudTrail log. Untuk informasi lebih lanjut, lihat [Membuat Jejak](#). Pergi ke [Menggunakan CloudTrail dengan AWS Certificate Manager](#) untuk melihat contoh jejak untuk ACM tindakan.

# Monitor dan log AWS Certificate Manager

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Certificate Manager dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi.

Topik berikut menjelaskan alat AWS pemantauan cloud yang tersedia untuk digunakan. ACM

Topik

- [Menggunakan Amazon EventBridge](#)
- [Menggunakan CloudTrail dengan AWS Certificate Manager](#)
- [CloudWatch Metrik yang didukung](#)

## Menggunakan Amazon EventBridge

Anda dapat menggunakan [Amazon EventBridge](#) (sebelumnya CloudWatch Acara) untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan, termasuk ACM, dikirimkan ke Amazon EventBridge dalam waktu hampir nyata. Anda dapat menggunakan peristiwa untuk memicu target termasuk AWS Lambda fungsi, AWS Batch pekerjaan, SNS topik Amazon, dan banyak lainnya. Untuk informasi selengkapnya, lihat [Apa itu Amazon EventBridge?](#)

Topik

- [EventBridge Dukungan Amazon untuk ACM](#)
- [Memicu tindakan dengan Amazon di EventBridge ACM](#)

## EventBridge Dukungan Amazon untuk ACM

Topik ini mencantumkan dan menjelaskan peristiwa ACM terkait yang didukung oleh Amazon EventBridge.

## ACMSertifikat Mendekati Acara Kedaluwarsa

ACM mengirimkan acara kedaluwarsa harian untuk semua sertifikat aktif (publik, swasta dan impor) mulai 45 hari sebelum kedaluwarsa. Waktu ini dapat diubah menggunakan [PutAccountConfiguration](#) aksi ACM API.

ACM secara otomatis memulai perpanjangan sertifikat yang memenuhi syarat yang diterbitkan, tetapi sertifikat yang diimpor harus diterbitkan kembali dan diimpor kembali sebelum kedaluwarsa untuk menghindari pemadaman. Untuk informasi selengkapnya, lihat [Mengimpor ulang sertifikat](#). Anda dapat menggunakan peristiwa kedaluwarsa untuk mengatur otomatisasi untuk mengimpor ulang sertifikat ke dalam ACM. Untuk contoh penggunaan otomatisasi AWS Lambda, lihat [Memicu tindakan dengan Amazon di EventBridge ACM](#).

ACMSertifikat Mendekati Acara Kedaluwarsa memiliki struktur sebagai berikut.

```
{
  "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"
  }
}
```

## ACMSertifikat Acara kedaluwarsa

Pelanggan dapat mendengarkan acara ini untuk memberi tahu mereka jika sertifikat publik atau pribadi yang ACM dikeluarkan di akun mereka kedaluwarsa. Acara kedaluwarsa Sertifikat tidak tersedia untuk [sertifikat yang diimpor](#), atau untuk sertifikat terkelola yang [tidak memenuhi syarat untuk perpanjangan](#).

ACMSertifikat Acara kedaluwarsa memiliki struktur berikut.

```
{
```

```

"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
}
}

```

## ACMSertifikat Acara yang tersedia

Pelanggan dapat mendengarkan acara ini untuk diberitahu ketika sertifikat publik atau pribadi yang dikelola siap digunakan. Acara ini dipublikasikan pada penerbitan, pembaruan, dan impor. Untuk sertifikat pribadi, setelah tersedia, tindakan pelanggan masih diperlukan untuk menyebarkannya ke host.

ACMSertifikat Acara yang tersedia memiliki struktur sebagai berikut.

```

{
  "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
  }
}

```

## ACMTindakan Perpanjangan Sertifikat Acara yang diperlukan

### Note

Tindakan Perpanjangan Sertifikat Peristiwa yang diperlukan tidak tersedia untuk [sertifikat yang diimpor](#).

Pelanggan dapat mendengarkan acara ini untuk diperingatkan ketika tindakan pelanggan harus diambil sebelum sertifikat dapat diperpanjang. Misalnya, jika pelanggan menambahkan CAA catatan yang ACM mencegah perpanjangan sertifikat, ACM menerbitkan acara ini ketika perpanjangan otomatis gagal pada 45 hari sebelum kedaluwarsa. Jika tidak ada tindakan pelanggan yang diambil, ACM lakukan upaya perpanjangan lebih lanjut pada 30 hari, 15 hari, 3 hari, dan 1 hari, atau sampai tindakan pelanggan diambil, sertifikat berakhir, atau sertifikat tidak lagi memenuhi syarat untuk perpanjangan. Sebuah acara diterbitkan untuk setiap upaya pembaruan ini.

ACMTindakan Perpanjangan Sertifikat Acara yang diperlukan memiliki struktur berikut.

```

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

```

```

    "CertificateType" : "AMAZON_ISSUED" | "PRIVATE",
    "CommonName": "example.com",
    "DomainValidationMethod" : "EMAIL" | "DNS",
    "RenewalStatusReason" : "CAA_ERROR" | "PENDING_DOMAIN_VALIDATION" |
"NO_AVAILABLE_CONTACTS" | "ADDITIONAL_VERIFICATION_REQUIRED" | "DOMAIN_NOT_ALLOWED"
| "INVALID_PUBLIC_DOMAIN" | "DOMAIN_VALIDATION_DENIED" | "PCA_LIMIT_EXCEEDED"
| "PCA_INVALID_ARN" | "PCA_INVALID_STATE" | "PCA_REQUEST_FAILED" |
"PCA_NAME_CONSTRAINTS_VALIDATION" | "PCA_RESOURCE_NOT_FOUND" | "PCA_INVALID_ARGS" |
"PCA_INVALID_DURATION" | "PCA_ACCESS_DENIED" | "SLR_NOT_FOUND" | "OTHER",
    "DaysToExpiry": 30,
    "CertificateExpirationDate" : "2019-12-22T18:43:48Z",
    "InUse" : TRUE | FALSE,
    "Exported" : TRUE | FALSE
  }
}

```

## AWS acara kesehatan

AWS acara kesehatan dihasilkan untuk ACM sertifikat yang memenuhi syarat untuk pembaruan. Untuk informasi tentang kelayakan pembaruan, lihat [Perpanjangan sertifikat dikelola di AWS Certificate Manager](#)

Peristiwa Kesehatan dihasilkan dalam dua skenario:

- Tentang keberhasilan pembaruan sertifikat publik atau swasta.
- Ketika pelanggan harus mengambil tindakan agar pembaruan terjadi. Ini mungkin berarti mengklik tautan dalam pesan email (untuk sertifikat yang divalidasi email), atau menyelesaikan kesalahan. Salah satu kode acara berikut disertakan dengan setiap acara. Kode diekspos sebagai variabel yang dapat Anda gunakan untuk pemfilteran.
  - AWS\_ACM\_RENEWAL\_STATE\_CHANGE(sertifikat telah diperpanjang, telah kedaluwarsa, atau akan kedaluwarsa)
  - CAA\_CHECK\_FAILURE(CAAcek gagal)
  - AWS\_ACM\_RENEWAL\_FAILURE(unter sertifikat yang ditandatangani oleh CA pribadi)

Peristiwa kesehatan memiliki struktur sebagai berikut. Dalam contoh ini, sebuah AWS\_ACM\_RENEWAL\_STATE\_CHANGE peristiwa telah dihasilkan.

```

{
  "source": [

```

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

## Memicu tindakan dengan Amazon di EventBridge ACM

Anda dapat membuat EventBridge aturan Amazon berdasarkan peristiwa ini dan menggunakan EventBridge konsol Amazon untuk mengonfigurasi tindakan yang terjadi saat peristiwa terdeteksi. Bagian ini menyediakan contoh prosedur untuk mengonfigurasi EventBridge aturan Amazon dan tindakan yang dihasilkan.

Topik

- [Menanggapi acara dengan Amazon SNS](#)
- [Menanggapi acara dengan fungsi Lambda](#)

### Menanggapi acara dengan Amazon SNS

Bagian ini menunjukkan cara mengonfigurasi Amazon SNS untuk mengirim pemberitahuan teks setiap kali ACM menghasilkan acara kesehatan.

Selesaikan prosedur berikut untuk mengonfigurasi respons.

Untuk membuat EventBridge aturan Amazon dan memicu tindakan

1. Buat EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat [Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa](#).



- a. Di EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>, navigasikan ke halaman Acara > Aturan dan pilih Buat aturan.
- b. Pada halaman Create rule, pilih Event Pattern.
- c. Untuk Nama Layanan, pilih Health dari menu.
- d. Untuk Jenis peristiwa, pilih Peristiwa Kondisi Spesifik.
- e. Pilih Layanan khusus dan pilih ACM dari menu.
- f. Pilih Kategori jenis acara tertentu dan pilih accountNotification.
- g. Pilih kode jenis acara apa pun.
- h. Pilih Sumber daya apa pun.
- i. Di editor pratinjau pola acara, tempel JSON pola yang dipancarkan oleh acara tersebut. Contoh ini menggunakan pola dari [AWS acara kesehatan](#) bagian.

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

## 2. Konfigurasi tindakan.

Di bagian Target, Anda dapat memilih di antara banyak layanan yang dapat langsung menggunakan acara Anda, seperti Amazon Simple Notification Service (SNS), atau Anda dapat

memilih fungsi Lambda untuk meneruskan acara ke kode eksekusi yang disesuaikan. Untuk contoh AWS Lambda implementasi, lihat [Menanggapi acara dengan fungsi Lambda](#).

## Menanggapi acara dengan fungsi Lambda

Prosedur ini menunjukkan cara menggunakan AWS Lambda untuk mendengarkan di Amazon EventBridge, membuat notifikasi dengan Amazon Simple Notification Service (SNS), dan mempublikasikan temuan ke AWS Security Hub, memberikan visibilitas kepada administrator dan tim keamanan.

Untuk mengatur fungsi dan peran Lambda IAM

1. Pertama konfigurasi peran AWS Identity and Access Management (IAM) dan tentukan izin yang diperlukan oleh fungsi Lambda. Praktik terbaik keamanan ini memberi Anda fleksibilitas dalam menentukan siapa yang memiliki otorisasi untuk memanggil fungsi, dan dalam membatasi izin yang diberikan kepada orang tersebut. Tidak disarankan untuk menjalankan sebagian besar AWS operasi langsung di bawah akun pengguna dan terutama tidak di bawah akun administrator.

Buka IAM konsol di <https://console.aws.amazon.com/iam/>.

2. Gunakan editor JSON kebijakan untuk membuat kebijakan yang ditentukan dalam templat di bawah ini. Berikan Wilayah dan detail AWS akun Anda sendiri. Untuk informasi selengkapnya, lihat [Membuat kebijakan di JSON tab](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LambdaCertificateExpiryPolicy1",
      "Effect": "Allow",
      "Action": "logs:CreateLogGroup",
      "Resource": "arn:aws:logs:<region>:<AWS-ACCT-NUMBER>:*"
    },
    {
      "Sid": "LambdaCertificateExpiryPolicy2",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```

```

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

```

3. Buat IAM peran dan lampirkan kebijakan baru padanya. Untuk informasi tentang membuat IAM peran dan melampirkan kebijakan, lihat [Membuat peran untuk AWS layanan \(konsol\)](#).

4. Buka AWS Lambda konsol di <https://console.aws.amazon.com/lambda/>.
5. Buat fungsi Lambda. Untuk informasi selengkapnya, lihat [Membuat fungsi Lambda dengan konsol](#). Selesaikan langkah-langkah berikut:
  - a. Pada halaman Create function, pilih opsi Author from scratch untuk membuat fungsi.
  - b. Tentukan nama seperti "handle-expiring-certificates" di bidang Nama fungsi.
  - c. Pilih Python 3.8 dari daftar Runtime.
  - d. Perluas Ubah peran eksekusi default dan pilih Gunakan peran yang ada.
  - e. Pilih peran yang sebelumnya Anda buat dari daftar peran yang ada.
  - f. Pilih Buat fungsi.
  - g. Di bawah kode Fungsi, masukkan kode berikut:

```
# 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. Di bawah variabel Lingkungan, pilih Edit dan opsional tambahkan variabel berikut.

- (Opsional) EXPIRY \_ DAYS

Menentukan berapa banyak lead time, dalam beberapa hari, sebelum pemberitahuan kedaluwarsa sertifikat dikirim. Fungsi default ke 45 hari, tetapi Anda dapat menentukan nilai kustom.

- (Opsional) SNS \_ TOPIC \_ ARN

Menentukan ARN untuk AmazonSNS. Berikan lengkap ARN dalam format `arn:aws:sns:<region>:<account-number>:<topic-name>`.

- (Opsional) SECURITY \_ HUB \_ REGION

Menentukan AWS Security Hub di Wilayah yang berbeda. Jika ini tidak ditentukan, Wilayah fungsi Lambda yang sedang berjalan digunakan. Jika fungsi dijalankan di beberapa Wilayah, mungkin diinginkan agar semua pesan sertifikat masuk ke Security Hub di satu Wilayah.

- i. Di bawah Pengaturan dasar, atur Timeout menjadi 30 detik.
- j. Di bagian atas halaman, pilih Deploy.

Selesaikan tugas dalam prosedur berikut untuk mulai menggunakan solusi ini.

Untuk mengotomatiskan pemberitahuan kedaluwarsa email

Dalam contoh ini, kami memberikan satu email untuk setiap sertifikat yang kedaluwarsa pada saat acara dimunculkan melalui Amazon EventBridge. Secara default, ACM memunculkan acara setiap hari untuk sertifikat yang 45 hari atau kurang dari kedaluwarsa. (Periode ini dapat disesuaikan menggunakan [PutAccountConfiguration](#) pengoperasian ACM API.) Masing-masing peristiwa ini memicu kaskade tindakan otomatis berikut:

```
ACM raises Amazon EventBridge event #
>>>>>> events

    Event matches Amazon EventBridge rule #

        Rule calls Lambda function #

            Function sends SNS email and logs a Finding in Security
Hub
```

1. Buat fungsi Lambda dan konfigurasi izin. (Sudah selesai — lihat [Untuk mengatur fungsi dan peran Lambda IAM](#)).



2. Buat SNS topik standar untuk fungsi Lambda yang akan digunakan untuk mengirim notifikasi. Untuk informasi selengkapnya, lihat [Membuat SNS topik Amazon](#).
3. Berlangganan pihak yang berkepentingan ke SNS topik baru. Untuk informasi selengkapnya, lihat [Berlangganan SNS topik Amazon](#).
4. Buat EventBridge aturan Amazon untuk memicu fungsi Lambda. Untuk informasi selengkapnya, lihat [Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa](#).

Di EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>, navigasikan ke halaman Acara > Aturan dan pilih Buat aturan. Tentukan Nama Layanan, Jenis Acara, dan fungsi Lambda. Di editor pratinjau Pola Acara, tempel kode berikut:

```
{
  "source": [
    "aws.acm"
  ],
  "detail-type": [
    "ACM Certificate Approaching Expiration"
  ]
}
```

Peristiwa seperti yang diterima Lambda ditampilkan di bawah Tampilkan contoh acara:

```
{
  "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"
  }
}
```

## Untuk membersihkan

Setelah Anda tidak lagi memerlukan konfigurasi contoh, atau konfigurasi apa pun, itu adalah praktik terbaik untuk menghapus semua jejaknya untuk menghindari masalah keamanan dan biaya masa depan yang tidak terduga:

- IAMkebijakan dan peran
- Fungsi Lambda
- CloudWatch Aturan acara
- CloudWatch Log yang terkait dengan Lambda
- SNSTopik

## Menggunakan CloudTrail dengan AWS Certificate Manager

AWS Certificate Manager terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan diACM. CloudTrail diaktifkan secara default di AWS akun Anda. CloudTrail menangkap API panggilan untuk ACM sebagai acara, termasuk panggilan dari ACM konsol dan panggilan kode ke ACM API operasi. Jika mengonfigurasi jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk ACM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatACM, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#). Ketika aktivitas acara yang didukung terjadi diACM, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS .

Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log.

Untuk informasi lebih lanjut tentang CloudTrail, lihat dokumentasi berikut:

- [AWS CloudTrail Panduan Pengguna](#).
- [Gambaran Umum untuk Membuat Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)

- [Mengkonfigurasi SNS Pemberitahuan Amazon untuk CloudTrail](#)
- [Menerima File CloudTrail Log dari Beberapa Wilayah](#) dan [Menerima File CloudTrail Log dari Beberapa Akun](#)

## Topik

- [ACMAPItindakan yang didukung dalam CloudTrail pencatatan](#)
- [API Panggilan log untuk layanan terintegrasi](#)

## ACMAPItindakan yang didukung dalam CloudTrail pencatatan

ACM mendukung pencatatan tindakan berikut sebagai peristiwa dalam file CloudTrail log:

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan Pengguna root akun AWS atau AWS Identity and Access Management (IAM) kredensial pengguna.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat [CloudTrail userIdentity Elemen](#).

Bagian berikut memberikan contoh log untuk API operasi yang didukung.

- [Menambahkan tag ke sertifikat \(AddTagsToCertificate\)](#)
- [Menghapus sertifikat \(\) DeleteCertificate](#)
- [Menjelaskan sertifikat \(\) DescribeCertificate](#)
- [Mengekspor sertifikat \(\) ExportCertificate](#)
- [Impor sertifikat \(ImportCertificate\)](#)
- [Sertifikat daftar \(ListCertificates\)](#)
- [Listing tag untuk sertifikat \(ListTagsForCertificate\)](#)
- [Menghapus tag dari sertifikat \(RemoveTagsFromCertificate\)](#)

- [Meminta sertifikat \(\) RequestCertificate](#)
- [Mengirim ulang email validasi \(\) ResendValidationEmail](#)
- [Mengambil sertifikat \(\) GetCertificate](#)

## Menambahkan tag ke sertifikat ([AddTagsToCertificate](#))

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [AddTagsToCertificate](#) API.

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-04-06T13:53:53Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "AddTagsToCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.10.16",
      "requestParameters": {
        "tags": [
          {
            "value": "Alice",
            "key": "Admin"
          }
        ]
      },
      "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/fedcba98-7654-3210-fedc-ba9876543210"
    },
    {
      "responseElements": null,
      "requestID": "fedcba98-7654-3210-fedc-ba9876543210",
      "eventID": "fedcba98-7654-3210-fedc-ba9876543210",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```

```

    }
  ]
}

```

## Menghapus sertifikat () [DeleteCertificate](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [DeleteCertificate](#) API.

```

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

```

## Menjelaskan sertifikat () [DescribeCertificate](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [DescribeCertificate](#) API.

**Note**

CloudTrail Log untuk DescribeCertificate operasi tidak menampilkan informasi tentang ACM sertifikat yang Anda tentukan. Anda dapat melihat informasi tentang sertifikat dengan menggunakan konsol, AWS Command Line Interface, atau [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"
    }
  ]
}
```

## Mengekspor sertifikat () [ExportCertificate](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [ExportCertificateAPI](#).

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

    ],
    "detail": {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2018-05-24T15:28:11Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "ExportCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4",
      "requestParameters": {
        "passphrase": {
          "hb": [
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42,
            42
          ]
        }
      }
    },
  ],
}
```

```

        "offset":0,
        "isReadOnly":false,
        "bigEndian":true,
        "nativeByteOrder":false,
        "mark":-1,
        "position":0,
        "limit":10,
        "capacity":10,
        "address":0
    },
    "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
},
"responseElements":{
  "certificateChain":
  "-----BEGIN CERTIFICATE-----
base64 certificate
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  base64 certificate
  -----END CERTIFICATE-----",
  "privateKey":"*****",
  "certificate":
  "-----BEGIN CERTIFICATE-----
  base64 certificate
  -----END CERTIFICATE-----"
},
"requestID":"01234567-89ab-cdef-0123-456789abcdef",
"eventID":"fedcba98-7654-3210-fedc-ba9876543210",
"eventType":"AwsApiCall"
}
}
]
}

```

## Impor sertifikat ([ImportCertificate](#))

Contoh berikut menunjukkan entri CloudTrail log yang merekam panggilan ke ACM [ImportCertificate](#) API operasi.

```

{
  "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"
}

```

## Sertifikat daftar ([ListCertificates](#))

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [ListCertificates](#) API.

### Note

CloudTrail Log untuk `ListCertificates` operasi tidak menampilkan ACM sertifikat Anda. Anda dapat melihat daftar sertifikat dengan menggunakan konsol, AWS Command Line Interface, atau file [ListCertificatesAPI](#).

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:43Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "ListCertificates",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "maxItems": 1000,
        "certificateStatuses": [
          "ISSUED"
        ]
      },
      "responseElements": null,
      "requestID": "74c99844-ec9c-11e5-ac34-d1e4dfe1a11b",
      "eventID": "cdfef1051-88aa-4aa3-8c33-a325270bff21",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```

## Listing tag untuk sertifikat ([ListTagsForCertificate](#))

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [ListTagsForCertificate](#) API.

**Note**

CloudTrail Log untuk `ListTagsForCertificate` operasi tidak menampilkan tag Anda. Anda dapat melihat daftar tag dengan menggunakan konsol, konsol AWS Command Line Interface, atau [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"
    }
  ]
}
```

## Menghapus tag dari sertifikat ([RemoveTagsFromCertificate](#))

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [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"
    }
  ]
}
```

## Meminta sertifikat () [RequestCertificate](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [RequestCertificate](#) API.

```
{
  "Records": [
```

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-03-18T00:00:49Z",
  "eventSource": "acm.amazonaws.com",
  "eventName": "RequestCertificate",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.9.15",
  "requestParameters": {
    "subjectAlternativeNames": [
      "example.net"
    ],
    "domainName": "example.com",
    "domainValidationOptions": [
      {
        "domainName": "example.com",
        "validationDomain": "example.com"
      },
      {
        "domainName": "example.net",
        "validationDomain": "example.net"
      }
    ]
  },
  "idempotencyToken": "8186023d89681c3ad5"
},
"responseElements": {
  "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
},
"requestID": "77dacef3-ec9c-11e5-ac34-d1e4dfe1a11b",
"eventID": "a4954cdb-8f38-44c7-8927-a38ad4be3ac8",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
```

```
}
```

## Mengirim ulang email validasi () [ResendValidationEmail](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [ResendValidationEmail](#) API.

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

## Mengambil sertifikat () [GetCertificate](#)

CloudTrail Contoh berikut menunjukkan hasil panggilan ke [GetCertificate](#) API.

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:41Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "GetCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.9.15",
      "requestParameters": {
        "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012"
      },
      "responseElements": {
        "certificateChain":
          "-----BEGIN CERTIFICATE-----
          Base64-encoded certificate chain
          -----END CERTIFICATE-----",
        "certificate":
          "-----BEGIN CERTIFICATE-----
          Base64-encoded certificate
          -----END CERTIFICATE-----"
      },
      "requestID": "744dd891-ec9c-11e5-ac34-d1e4dfe1a11b",
      "eventID": "7aa4f909-00dd-478a-9a00-b2709bcad2bb",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```



## API Panggilan log untuk layanan terintegrasi

Anda dapat menggunakan CloudTrail untuk mengaudit API panggilan yang dilakukan oleh layanan yang terintegrasi dengan ACM. Untuk informasi selengkapnya tentang penggunaan CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#). Contoh berikut menunjukkan jenis log yang dapat dihasilkan tergantung pada AWS sumber daya tempat Anda memberikan ACM sertifikat.

### Topik

- [Membuat penyeimbang beban](#)

## Membuat penyeimbang beban

Anda dapat menggunakan CloudTrail untuk mengaudit API panggilan yang dilakukan oleh layanan yang terintegrasi dengan ACM. Untuk informasi selengkapnya tentang penggunaan CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#). Contoh berikut menunjukkan jenis log yang dapat dihasilkan tergantung pada AWS sumber daya tempat Anda memberikan ACM sertifikat.

### Topik

- [Membuat Load Balancer](#)
- [Mendaftarkan EC2 Instans Amazon dengan Load Balancer](#)
- [Mengkripsi Kunci Pribadi](#)
- [Mendekripsi Kunci Pribadi](#)

## Membuat Load Balancer

Contoh berikut menunjukkan panggilan ke `CreateLoadBalancer` fungsi oleh IAM pengguna bernama Alice. Nama penyeimbang beban adalah `TestLinuxDefault`, dan pendengar dibuat menggunakan sertifikat 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"
}

```

## Mendaftarkan EC2 Instans Amazon dengan Load Balancer

Saat Anda menyediakan situs web atau aplikasi Anda di instans Amazon Elastic Compute Cloud (AmazonEC2), penyeimbang beban harus mengetahui instans tersebut. Hal ini dapat dicapai melalui konsol Elastic Load Balancing atau AWS Command Line Interface. Contoh berikut menunjukkan panggilan ke `RegisterInstancesWithLoadBalancer` penyeimbang beban bernama `LinuxTest` pada AWS akun `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"
}
```

## Mengenkripsi Kunci Pribadi

Contoh berikut menunjukkan Encrypt panggilan yang mengenkripsi kunci pribadi yang terkait dengan sertifikat ACM. Enkripsi dilakukan di dalam 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"
    }
  ]
}
```

```
]
}
```

## Mendekripsi Kunci Pribadi

Contoh berikut menunjukkan Decrypt panggilan yang mendekripsi kunci pribadi yang terkait dengan sertifikat ACM. Dekripsi dilakukan di dalam AWS, dan kunci yang didekripsi tidak pernah pergi. 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 Metrik yang didukung

Amazon CloudWatch adalah layanan pemantauan untuk AWS sumber daya. Anda dapat menggunakan CloudWatch untuk mengumpulkan dan melacak metrik, mengatur alarm, dan secara otomatis bereaksi terhadap perubahan sumber daya Anda AWS . ACM menerbitkan metrik sekali per hari untuk setiap sertifikat di akun hingga kedaluwarsa.

AWS/CertificateManagerNamespace mencakup metrik berikut.

Metrik	Deskripsi	Unit	Dimensi
DaysToExpiry	Jumlah hari sampai sertifikat berakhir. ACM berhenti menerbitkan metrik ini setelah sertifikat kedaluwarsa.	Bilangan Bulat	CertificateArn <ul style="list-style-type: none"> <li>• Nilai: ARN dari sertifikat</li> </ul>

Untuk informasi selengkapnya tentang CloudWatch metrik, lihat topik berikut:

- [Menggunakan CloudWatch Metrik Amazon](#)
- [Membuat CloudWatch Alarm Amazon](#)

# Gunakan AWS Certificate Manager dengan SDK untuk Java

Anda dapat menggunakan AWS Certificate Manager API untuk berinteraksi dengan layanan secara terprogram dengan mengirimkan HTTP permintaan. Untuk informasi lebih lanjut, lihat [AWS Certificate Manager API Referensi](#).

Selain web API (atau HTTP API), Anda dapat menggunakan AWS SDK dan alat baris perintah untuk berinteraksi dengan ACM dan layanan lainnya. Untuk informasi lebih lanjut, lihat [Alat untuk Amazon Web Services](#).

Topik berikut menunjukkan cara menggunakan salah satu AWS SDKs, [AWS SDK for Java](#) untuk melakukan beberapa operasi yang tersedia di AWS Certificate Manager API.

## Topik

- [Menambahkan tag ke sertifikat](#)
- [Menghapus sertifikat](#)
- [Menjelaskan sertifikat](#)
- [Mengekspor sertifikat](#)
- [Mengambil sertifikat dan rantai sertifikat](#)
- [Mengimpor sertifikat](#)
- [Sertifikat daftar](#)
- [Memperbarui sertifikat](#)
- [Listing tag sertifikat](#)
- [Menghapus tag dari sertifikat](#)
- [Meminta sertifikat](#)
- [Mengirim ulang email validasi](#)

## Menambahkan tag ke sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [AddTagsToCertificate](#) fungsi.

```
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);
}
}
```

## Menghapus sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [DeleteCertificate](#) fungsi. Jika berhasil, fungsi mengembalikan set kosong {}.

```
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);

}
}
```

## Menjelaskan sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [DescribeCertificate](#) fungsi.

```
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);  
  
}  
}
```

Jika berhasil, contoh sebelumnya menampilkan informasi yang mirip dengan berikut ini.

```
{  
  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,  
  }  
}
```

## Mengekspor sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [ExportCertificate](#) fungsi. Fungsi ini mengekspor sertifikat pribadi yang dikeluarkan oleh otoritas sertifikat swasta (CA) dalam format PKCS #8. (Tidak mungkin mengekspor sertifikat publik apakah itu ACM diterbitkan atau diimpor.) Ini juga mengekspor rantai sertifikat dan kunci pribadi. Dalam contoh, frasa sandi untuk kunci disimpan dalam file lokal.

```
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();
}
}
```

## Mengambil sertifikat dan rantai sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [GetCertificate](#) fungsi.

```
package com.amazonaws.samples;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.GetCertificateRequest;
import com.amazonaws.services.certificatemanager.model.GetCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.RequestInProgressException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the GetCertificate function in the AWS
 * Certificate
 * Manager service.
 */
```

```
* Input parameter:
*   CertificateArn - The ARN of the certificate to retrieve.
*
* Output parameters:
*   Certificate - A base64-encoded certificate in PEM format.
*   CertificateChain - The base64-encoded certificate chain in PEM format.
*
*/
```

```
public class AWSCertificateManagerExample {

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

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load the credentials from the
            credential profiles file.", ex);
        }

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

        // Create a request object and set the ARN of the certificate to be described.
        GetCertificateRequest req = new GetCertificateRequest();

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

        // Retrieve the certificate and certificate chain.
        // If you recently requested the certificate, loop until it has been created.
        GetCertificateResult result = null;
        long totalTimeout = 1200001;
        long timeSlept = 01;
        long sleepInterval = 100001;
        while (result == null && timeSlept < totalTimeout) {
```

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

    timeSlept += sleepInterval;
}

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

Contoh sebelumnya menciptakan output yang mirip dengan berikut ini.

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

## Mengimpor sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [ImportCertificate](#) fungsi.

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 * Certificate Manager
 * service.
 *
 * Input parameters:
 * Certificate - PEM file that contains the certificate to import.
 * CertificateArn - Use to reimport a certificate (not included in this example).
 * CertificateChain - The certificate chain, not including the end-entity
 * certificate.
 * PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 * CertificateArn - The ARN of the imported certificate.
 */
public class AWSCertificateManagerSample {

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Sertifikat daftar

Contoh berikut menunjukkan bagaimana menggunakan [ListCertificates](#) fungsi.

```
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);
    }
}
```



```
}
```

Sampel sebelumnya menciptakan output yang mirip dengan berikut ini.

```
{
  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
  }]
}
```

## Memperbarui sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [RenewCertificate](#) fungsi. Fungsi ini memperbarui sertifikat pribadi yang dikeluarkan oleh otoritas sertifikat swasta (CA) dan diekspor dengan fungsi tersebut [ExportCertificate](#). Saat ini, hanya sertifikat pribadi yang diekspor yang dapat diperbarui dengan fungsi ini. Untuk memperbaharui AWS Private CA sertifikat dengan ACM, Anda harus terlebih dahulu memberikan izin utama ACM layanan untuk melakukannya. Untuk informasi selengkapnya, lihat [Menetapkan Izin Perpanjangan Sertifikat](#) ke. 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);
}
}
```

## Listing tag sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [ListTagsForCertificate](#) fungsi.

```
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);

}
}
```

Sampel sebelumnya menciptakan output yang mirip dengan berikut ini.

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

## Menghapus tag dari sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [RemoveTagsFromCertificate](#) fungsi.

```
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);
}
}
```

## Meminta sertifikat

Contoh berikut menunjukkan bagaimana menggunakan [RequestCertificate](#) fungsi.

```
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);
}
}
```

Sampel sebelumnya menciptakan output yang mirip dengan berikut ini.

```
{CertificateArn:  
  arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

## Mengirim ulang email validasi

Contoh berikut menunjukkan cara menggunakan [ResendValidationEmail](#) fungsi.

```
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());  
  
    }  
}
```

Sampel sebelumnya mengirim ulang email validasi Anda dan menampilkan set kosong.

# Memecahkan masalah dengan AWS Certificate Manager

Konsultasikan topik berikut jika Anda mengalami masalah dalam menggunakan AWS Certificate Manager.

## Note

Jika Anda tidak melihat masalah Anda ditangani di bagian ini, kami sarankan untuk mengunjungi [AWS Pusat Pengetahuan](#).

## Topik

- [Memecahkan masalah permintaan sertifikat](#)
- [Memecahkan masalah validasi sertifikat](#)
- [Memecahkan masalah perpanjangan sertifikat terkelola](#)
- [Memecahkan masalah lain](#)
- [Menangani pengecualian](#)

## Memecahkan masalah permintaan sertifikat

Konsultasikan topik berikut jika Anda mengalami masalah saat meminta ACM sertifikat.

## Topik

- [Waktu permintaan sertifikat habis](#)
- [Permintaan sertifikat gagal](#)

## Waktu permintaan sertifikat habis

Permintaan waktu ACM sertifikat habis jika tidak divalidasi dalam waktu 72 jam. Untuk memperbaiki kondisi ini, buka konsol, temukan catatan untuk sertifikat, klik kotak centang untuk itu, pilih Tindakan, dan pilih Hapus. Kemudian pilih Tindakan dan Minta sertifikat untuk memulai lagi. Untuk informasi selengkapnya, lihat [AWS Certificate Manager DNSvalidasi](#) atau [AWS Certificate Manager validasi email](#). Kami menyarankan Anda menggunakan DNS validasi jika memungkinkan.

## Permintaan sertifikat gagal

Jika permintaan Anda gagal ACM dan Anda menerima salah satu pesan galat berikut, ikuti langkah-langkah yang disarankan untuk memperbaiki masalah. Anda tidak dapat mengirimkan kembali permintaan sertifikat yang gagal — setelah menyelesaikan masalah, kirimkan permintaan baru.

### Topik

- [Pesan galat: Tidak Ada Kontak yang Tersedia](#)
- [Pesan galat: Diperlukan Verifikasi Tambahan](#)
- [Pesan galat: Domain Publik Tidak Valid](#)
- [Pesan galat: Lainnya](#)

### Pesan galat: Tidak Ada Kontak yang Tersedia

Anda memilih validasi email saat meminta sertifikat, tetapi tidak ACM dapat menemukan alamat email yang akan digunakan untuk memvalidasi satu atau beberapa nama domain dalam permintaan. Untuk memperbaiki masalah ini, Anda dapat melakukan salah satu hal berikut:

- Pastikan domain Anda dikonfigurasi untuk menerima email. Server nama domain Anda harus memiliki catatan penukar surat (catatan MX) sehingga ACM server email tahu ke mana harus mengirim email [validasi domain](#).

Menyelesaikan salah satu tugas sebelumnya sudah cukup untuk memperbaiki masalah ini; Anda tidak perlu melakukan keduanya. Setelah Anda memperbaiki masalah, minta sertifikat baru.

Untuk informasi selengkapnya tentang cara memastikan bahwa Anda menerima email validasi domain dari ACM, lihat [AWS Certificate Manager validasi email](#) atau [Tidak menerima email validasi](#). Jika Anda mengikuti langkah-langkah ini dan terus mendapatkan pesan Tidak Ada Kontak yang Tersedia, [laporkan ke AWS](#) sehingga kita bisa menyelidikinya.

### Pesan galat: Diperlukan Verifikasi Tambahan

ACM memerlukan informasi tambahan untuk memproses permintaan sertifikat ini. Ini terjadi sebagai tindakan perlindungan penipuan jika domain Anda berada di peringkat 1000 situs web [Alexa teratas](#). Untuk memberikan informasi yang diperlukan, gunakan [Support Center](#) untuk menghubungi Support. Jika Anda tidak memiliki rencana dukungan, posting thread baru di [Forum ACM Diskusi](#).

**Note**

Anda tidak dapat meminta sertifikat untuk nama domain milik Amazon seperti yang diakhiri dengan [amazonaws.com](https://amazonaws.com), [cloudfront.net](https://cloudfront.net), atau [elasticbeanstalk.com](https://elasticbeanstalk.com).

## Pesan galat: Domain Publik Tidak Valid

Satu atau lebih nama domain dalam permintaan sertifikat tidak valid. Biasanya, ini karena nama domain dalam permintaan bukan domain tingkat atas yang valid. Coba lagi untuk meminta sertifikat, memperbaiki kesalahan ejaan atau kesalahan ketik yang ada dalam permintaan gagal, dan pastikan bahwa semua nama domain dalam permintaan adalah untuk domain tingkat atas yang valid. Misalnya, Anda tidak dapat meminta ACM sertifikat untuk `example.invalidpublicdomain` karena “invalidpublicdomain” bukan domain tingkat atas yang valid. Jika Anda terus menerima alasan kegagalan ini, hubungi [Pusat Dukungan](#). Jika Anda tidak memiliki rencana dukungan, posting thread baru di [Forum ACM Diskusi](#).

## Pesan galat: Lainnya

Biasanya, kegagalan ini terjadi ketika ada kesalahan ketik pada satu atau lebih nama domain dalam permintaan sertifikat. Coba lagi untuk meminta sertifikat, memperbaiki kesalahan ejaan atau kesalahan ketik yang ada dalam permintaan gagal. Jika Anda terus menerima pesan kegagalan ini, gunakan [Pusat Dukungan](#) untuk menghubungi Support. Jika Anda tidak memiliki rencana dukungan, posting thread baru di [Forum ACM Diskusi](#).

## Memecahkan masalah validasi sertifikat

Jika status permintaan ACM sertifikat adalah Validasi Tertunda, permintaan sedang menunggu tindakan dari Anda. Jika Anda memilih validasi email saat mengajukan permintaan, Anda atau perwakilan resmi harus menanggapi pesan email validasi. Pesan-pesan ini dikirim ke alamat email umum untuk domain yang diminta. Untuk informasi selengkapnya, lihat [AWS Certificate Manager validasi email](#). Jika Anda memilih DNS validasi, Anda harus menulis CNAME catatan yang ACM dibuat untuk Anda ke DNS database Anda. Untuk informasi selengkapnya, lihat [AWS Certificate Manager DNSvalidasi](#).

**⚠ Important**

Anda harus memvalidasi bahwa Anda memiliki atau mengontrol setiap nama domain yang Anda sertakan dalam permintaan sertifikat Anda. Jika Anda memilih validasi email, Anda akan menerima pesan email validasi untuk setiap domain. Jika tidak, maka lihatlah [Tidak menerima email validasi](#). Jika Anda memilih DNS validasi, Anda harus membuat satu CNAME catatan untuk setiap domain.

**ℹ Note**

ACMSertifikat publik dapat diinstal pada EC2 instans Amazon yang terhubung ke [Enclave Nitro](#), tetapi tidak ke instans Amazon lainnya. Untuk informasi tentang pengaturan server web mandiri pada EC2 instans Amazon yang tidak terhubung ke Enclave Nitro, lihat [Tutorial: Menginstal LAMP server web di Amazon Linux 2](#) atau [Tutorial: Menginstal server LAMP web dengan Amazon Linux. AMI](#)

Kami menyarankan Anda menggunakan DNS validasi daripada validasi email.

Konsultasikan topik berikut jika Anda mengalami masalah validasi.

Topik

- [Memecahkan masalah validasi DNS](#)
- [Memecahkan masalah validasi email](#)

## Memecahkan masalah validasi DNS

Konsultasikan panduan berikut jika Anda mengalami masalah dalam memvalidasi sertifikat. DNS

Langkah pertama dalam DNS pemecahan masalah adalah memeriksa status domain Anda saat ini dengan alat seperti berikut:

- menggali — [Linux](#), [Windows](#)
- nslookup - [Linux](#), [Windows](#)
- Whois - [Linux](#), [Windows](#)



## Topik

- [Garis bawah dilarang oleh penyedia DNS](#)
- [Periode trailing default ditambahkan oleh penyedia DNS](#)
- [DNSvalidasi gagal GoDaddy](#)
- [ACMKonsol tidak menampilkan tombol "Buat catatan di Rute 53"](#)
- [Validasi Route 53 gagal pada domain pribadi \(tidak tepercaya\)](#)
- [Validasi berhasil tetapi penerbitan atau pembaruan gagal](#)
- [Validasi gagal untuk DNS server di VPN](#)

## Garis bawah dilarang oleh penyedia DNS

Jika DNS penyedia Anda melarang garis bawah utama dalam CNAME nilai, Anda dapat menghapus garis bawah dari nilai yang ACM disediakan dan memvalidasi domain Anda tanpanya. Misalnya, CNAME nilai `_x2.acm-validations.aws` dapat diubah `x2.acm-validations.aws` untuk tujuan validasi. Namun, parameter CNAME nama harus selalu dimulai dengan garis bawah utama.

Anda dapat menggunakan salah satu nilai di sisi kanan tabel di bawah ini untuk memvalidasi domain.

Nama	Tipe	Nilai
<code>_&lt;random value&gt;.example.com.</code>	CNAME	<code>&lt;random value&gt;.acm-validations.aws.</code>
<code>&lt;random value&gt;.example.com.</code>	CNAME	<code>&lt;random value&gt;.acm-validations.aws.</code>

## Periode trailing default ditambahkan oleh penyedia DNS

Beberapa DNS penyedia menambahkan secara default periode tambahan ke CNAME nilai yang Anda berikan. Akibatnya, menambahkan periode sendiri menyebabkan kesalahan. Misalnya, "`<random_value>.acm-validations.aws.`" ditolak sementara "`<random_value>.acm-validations.aws`" diterima.

## DNSvalidasi gagal GoDaddy

DNSvalidasi untuk domain yang terdaftar di Godaddy dan pendaftar lainnya mungkin gagal kecuali Anda mengubah nilai yang diberikan oleh. CNAME ACM Mengambil example.com sebagai nama domain, CNAME catatan yang dikeluarkan memiliki bentuk berikut:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:
_cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

Anda dapat membuat CNAME rekaman yang kompatibel GoDaddy dengan memotong domain apex (termasuk periode) di akhir NAME bidang, sebagai berikut:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:
_cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

## ACMKonsol tidak menampilkan tombol "Buat catatan di Rute 53"

Jika Anda memilih Amazon Route 53 sebagai DNS penyedia Anda, AWS Certificate Manager dapat berinteraksi langsung dengannya untuk memvalidasi kepemilikan domain Anda. Dalam beberapa keadaan, tombol Buat catatan di Route 53 konsol mungkin tidak tersedia saat Anda mengharapkannya. Jika ini terjadi, periksa kemungkinan penyebab berikut.

- Anda tidak menggunakan Route 53 sebagai DNS penyedia Anda.
- Anda masuk ACM dan Route 53 melalui akun yang berbeda.
- Anda tidak memiliki IAM izin untuk membuat catatan di zona yang dihosting oleh Route 53.
- Anda atau orang lain telah memvalidasi domain tersebut.
- Domain tidak dapat dialamatkan secara publik.

## Validasi Route 53 gagal pada domain pribadi (tidak tepercaya)

Selama DNS validasi, ACM mencari CNAME di zona yang dihosting publik. Ketika tidak menemukannya, waktu habis setelah 72 jam dengan status Validasi habis waktu. Anda tidak dapat menggunakannya untuk meng-host DNS catatan untuk domain pribadi, termasuk sumber daya di [zona host VPC pribadi](#) Amazon, domain tidak tepercaya di privatPKI, dan sertifikat yang ditandatangani sendiri.

AWS memberikan dukungan untuk domain yang tidak dipercaya secara publik melalui [AWS Private CA](#) layanan.

## Validasi berhasil tetapi penerbitan atau pembaruan gagal

Jika penerbitan sertifikat gagal dengan “Validasi tertunda” meskipun DNS benar, periksa apakah penerbitan tidak diblokir oleh catatan Otorisasi Otorisasi () Otoritas Sertifikasi. CAA Untuk informasi selengkapnya, lihat [\(Opsional\) Konfigurasi CAA catatan](#).

## Validasi gagal untuk DNS server di VPN

Jika Anda menemukan DNS server di VPN dan ACM gagal memvalidasi sertifikat terhadapnya, periksa apakah server dapat diakses publik. Penerbitan sertifikat publik menggunakan ACM DNS validasi mengharuskan catatan domain dapat diselesaikan melalui internet publik.

## Memecahkan masalah validasi email

Konsultasikan panduan berikut jika Anda mengalami masalah dalam memvalidasi domain sertifikat dengan email.

### Topik

- [Tidak menerima email validasi](#)
- [Stempel waktu awal yang persisten untuk validasi email](#)
- [Saya tidak dapat beralih ke DNS validasi](#)

## Tidak menerima email validasi

Ketika Anda meminta sertifikat dari ACM dan memilih validasi email, email validasi domain dikirim ke lima alamat administratif umum. Untuk informasi selengkapnya, lihat [AWS Certificate Manager validasi email](#). Jika Anda mengalami masalah dalam menerima email validasi, tinjau saran berikut.

### Di mana mencari email

ACM mengirimkan pesan email validasi ke nama domain yang Anda minta. Anda juga dapat menentukan superdomain sebagai domain validasi jika Anda ingin menerima email ini di domain tersebut. Subdomain apa pun hingga alamat situs web minimal valid, dan digunakan sebagai domain untuk alamat email sebagai akhiran setelah @. Misalnya, Anda dapat menerima email ke admin@example.com jika Anda menentukan example.com sebagai domain validasi untuk subdomain.example.com. Tinjau daftar alamat email yang ditampilkan di ACM konsol (atau dikembalikan dari CLI atau API) untuk menentukan di mana Anda harus mencari email validasi. Untuk melihat daftar, klik ikon di sebelah nama domain di kotak berlabel Validasi tidak lengkap.

## Email ditandai sebagai spam

Periksa folder spam Anda untuk email validasi.

## GMail secara otomatis mengurutkan email Anda

Jika Anda menggunakan GMail, email validasi mungkin telah secara otomatis diurutkan ke dalam tab Pembaruan atau Promosi.

## Registrar domain tidak menampilkan informasi kontak atau perlindungan privasi diaktifkan

Untuk domain yang dibeli dari Route 53, perlindungan privasi diaktifkan secara default dan alamat email Anda dipetakan ke `whoisprivacyservice.org`, `contact.gandi.net`, atau alamat `identity-protect.org` email. Pastikan bahwa alamat email pendaftar Anda pada file dengan registrar domain Anda up to date sehingga email yang dikirim ke alamat email yang dikaburkan ini dapat diteruskan ke alamat email yang Anda kontrol.

### Note

Perlindungan privasi untuk beberapa domain yang pembelian Anda dengan Route 53 akan diaktifkan bahkan jika Anda memilih untuk membuat informasi kontak Anda publik. Misalnya, perlindungan privasi untuk domain tingkat atas `.ca` tidak dapat dinonaktifkan secara terprogram oleh Route 53. Anda harus menghubungi [AWS Support Center](#) dan minta agar perlindungan privasi dinonaktifkan.

Setelah menyediakan setidaknya satu dari delapan alamat email yang AWS mengirim email validasi dan mengonfirmasi bahwa Anda dapat menerima email untuk alamat itu, Anda siap untuk meminta sertifikat melalui ACM. Setelah Anda membuat permintaan sertifikat, pastikan alamat email yang dimaksud muncul di daftar alamat email di AWS Management Console. Saat sertifikat berada dalam status validasi Tertunda, Anda dapat memperluas daftar untuk melihatnya dengan mengklik ikon di sebelah nama domain di kotak berlabel Validasi tidak lengkap. Anda juga dapat melihat daftar di Langkah 3: Validasi wizard ACM Minta Sertifikat. Alamat email yang terdaftar adalah alamat email yang dikirim.

## Hubungi Support Center

Jika, setelah meninjau panduan sebelumnya, Anda masih belum menerima email validasi domain, silakan kunjungi [Support Pusatkan](#) dan buat kasing. Jika Anda tidak memiliki perjanjian dukungan, kirimkan pesan ke [Forum ACM Diskusi](#).

## Stempel waktu awal yang persisten untuk validasi email

Stempel waktu permintaan validasi email pertama sertifikat tetap ada melalui permintaan perpanjangan validasi selanjutnya. Ini bukan bukti kesalahan dalam ACM operasi.

## Saya tidak dapat beralih ke DNS validasi

Setelah Anda membuat sertifikat dengan validasi email, Anda tidak dapat beralih untuk memvalidasinya dengan DNS. Untuk menggunakan DNS validasi, hapus sertifikat dan kemudian buat yang baru yang menggunakan DNS validasi.

## Memecahkan masalah perpanjangan sertifikat terkelola

ACM mencoba memperbarui ACM sertifikat Anda secara otomatis sebelum kedaluwarsa sehingga tidak ada tindakan yang diperlukan dari Anda. Konsultasikan topik berikut jika Anda memiliki masalah [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#).

## Mempersiapkan validasi domain otomatis

Sebelum ACM dapat memperbarui sertifikat Anda secara otomatis, berikut ini harus benar:

- Sertifikat Anda harus dikaitkan dengan AWS Layanan yang terintegrasi dengan ACM Untuk informasi tentang sumber daya yang ACM mendukung, lihat [Layanan terintegrasi dengan ACM](#).
- Untuk sertifikat yang divalidasi email, ACM harus dapat menghubungi Anda di alamat email administrator untuk setiap domain yang tercantum dalam sertifikat Anda. Alamat email yang akan dicoba tercantum di [AWS Certificate Manager validasi email](#).
- Untuk sertifikat DNS -validated, pastikan DNS konfigurasi Anda berisi CNAME catatan yang benar seperti yang dijelaskan dalam [AWS Certificate Manager DNS validasi](#)

## Menangani kegagalan dalam perpanjangan sertifikat terkelola

[Ketika sertifikat mendekati kedaluwarsa \(60 hari untuk DNS, 45 untuk EMAIL dan 60 hari untuk Private\), ACM upaya untuk memperbarui sertifikat jika memenuhi kriteria kelayakan.](#) Anda mungkin harus mengambil tindakan agar pembaruan berhasil. Untuk informasi selengkapnya, lihat [Perpanjangan sertifikat terkelola di AWS Certificate Manager](#).

## Perpanjangan sertifikat terkelola untuk sertifikat yang divalidasi email

ACMsertifikat berlaku selama 13 bulan (395 hari). Memperpanjang sertifikat memerlukan tindakan oleh pemilik domain. ACMmulai mengirimkan pemberitahuan perpanjangan ke alamat email yang terkait dengan domain 45 hari sebelum kedaluwarsa. Notifikasi berisi tautan yang dapat diklik pemilik domain untuk perpanjangan. Setelah semua domain yang terdaftar divalidasi, ACM mengeluarkan sertifikat yang diperbarui dengan hal yang sama. ARN

Lihat [Memvalidasi dengan Email](#) untuk petunjuk tentang mengidentifikasi domain mana yang berada dalam PENDING\_VALIDATION status dan mengulangi proses validasi untuk domain tersebut.

## Perpanjangan sertifikat terkelola untuk sertifikat yang DNS divalidasi

ACMtidak mencoba TLS validasi untuk sertifikat yang DNS divalidasi. Jika ACM gagal memperbarui sertifikat yang Anda validasi dengan DNS validasi, kemungkinan besar karena CNAME catatan yang hilang atau tidak akurat dalam konfigurasi Anda. DNS Jika ini terjadi, ACM memberi tahu Anda bahwa sertifikat tidak dapat diperpanjang secara otomatis.

### Important

Anda harus memasukkan CNAME catatan yang benar ke dalam DNS database Anda. Konsultasikan registrar domain Anda tentang cara melakukannya.

Anda dapat menemukan CNAME catatan untuk domain Anda dengan memperluas sertifikat dan entri domainnya di ACM konsol. Lihat gambar di bawah ini untuk detailnya. Anda juga dapat mengambil CNAME catatan dengan menggunakan [DescribeCertificate](#) operasi dalam ACM API atau [perintah deskripsi-sertifikat](#) di ACM CLI Untuk informasi selengkapnya, lihat [AWS Certificate Manager DNSvalidasi](#).

« < Viewing 1 to 3 of 3 certificates > »

<input type="checkbox"/>	Name ▾	Domain name ▾	Additional names	Status ▾	Type ▾	In use? ▾	Renewal eligibility ▾
<input type="checkbox"/>	▶	amzn1.example.biz		Issued	Amazon Issued	No	Ineligible
<input type="checkbox"/>	▶	amzn2.example.biz		Validation timed out	Amazon Issued	No	Ineligible
<input type="checkbox"/>	▼	amzn3.example.biz		Issued	Amazon Issued	No	Ineligible

**Status**

**Status** Issued  
**Detailed status** The certificate was issued at 2018-03-22T22:42:12UTC

Domain	Validation status
▶ amzn3.example.biz	Success

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

**Details**

<b>Type</b>	Amazon Issued	<b>Requested at</b>	2018-03-22T22:38:52UTC
<b>In use?</b>	No	<b>Issued at</b>	2018-03-22T22:42:12UTC
<b>Domain name</b>	amzn3.example.biz	<b>Not before</b>	2018-03-22T00:00:00UTC
<b>Number of additional names</b>	0	<b>Not after</b>	2019-04-22T12:00:00UTC
<b>Identifier</b>	1fae4ec1-6db6-4d3d-967a-ee5e53ecd45	<b>Public key info</b>	RSA 2048-bit
<b>Serial number</b>	0e:10:30:f3:1c:b4:1e:b7:54:bb:f3:99:62:5b:7f:fb	<b>Signature algorithm</b>	SHA256WITHRSA
		<b>ARN</b>	arn:aws:acm:us-west-2:140948901414:certificate/1fae4ec1-6db6-4d3d-967a-ee5e53ecd45
		<b>Validation state</b>	None

**Tags**

Name

« < Viewing 1 to 3 of 3 certificates > »

Pilih sertifikat target dari konsol.

Domain	Validation status
amzn3.example.biz	Success

Add the following CNAME record to the DNS configuration for your domain. The procedure for adding CNAME records depends on your DNS service Provider. [Learn more.](#)

Name	Type	Value
_dc8d107e33e2a83816b6a2a395a5cf5d.amzn.example.biz.	CNAME	_dadbc0aaa5530cf8b0964967cf1d4ed8.acm-validations.aws.

**Note:** Changing the DNS configuration allows ACM to issue certificates for this domain name for as long as the DNS record exists. You can revoke permission at any time by removing the record. [Learn more.](#)

[Create record in Route 53](#) **Amazon Route 53 DNS Customers** ACM can update your DNS configuration for you. [Learn more.](#)

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

Perluas jendela sertifikat untuk menemukan CNAME informasi sertifikat.

Jika masalah berlanjut, hubungi [Support Center](#).

## Memahami waktu pembaruan

[Perpanjangan sertifikat terkelola di AWS Certificate Manager](#) adalah proses asinkron. Ini berarti bahwa langkah-langkah tidak terjadi secara berurutan. Setelah semua nama domain dalam ACM sertifikat telah divalidasi, mungkin ada penundaan sebelum ACM memperoleh sertifikat baru. Penundaan tambahan dapat terjadi antara waktu ketika ACM memperoleh sertifikat yang diperbarui dan waktu ketika sertifikat tersebut dikerahkan ke AWS sumber daya yang menggunakannya. Oleh karena itu, perubahan status sertifikat dapat memakan waktu hingga beberapa jam untuk muncul di konsol.



# Memecahkan masalah lain

Bagian ini mencakup panduan untuk masalah yang tidak terkait dengan penerbitan atau validasi sertifikat ACM.

## Topik

- [Otoritas Sertifikasi Otorisasi \(CAA\) masalah](#)
- [Masalah impor sertifikat](#)
- [Masalah penyematan sertifikat](#)
- [API Masalah gateway](#)
- [Apa yang harus dilakukan ketika sertifikat kerja gagal secara tak terduga](#)
- [Masalah dengan peran ACM terkait layanan \(\) SLR](#)

## Otoritas Sertifikasi Otorisasi (CAA) masalah

Anda dapat menggunakan CAA DNS catatan untuk menentukan bahwa otoritas sertifikat Amazon (CA) dapat menerbitkan ACM sertifikat untuk domain atau subdomain Anda. Jika Anda menerima kesalahan selama penerbitan sertifikat yang mengatakan Satu atau beberapa nama domain gagal validasi karena kesalahan Otorisasi Otorisasi (CAA) Otoritas Sertifikasi, periksa catatan Anda. CAA DNS Jika Anda menerima kesalahan ini setelah permintaan ACM sertifikat berhasil divalidasi, Anda harus memperbarui CAA catatan Anda dan meminta sertifikat lagi. Bidang nilai dalam CAA catatan Anda harus berisi salah satu nama domain berikut:

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

Untuk informasi selengkapnya tentang membuat CAA rekaman, lihat [\(Opsional\) Konfigurasi CAA catatan](#).

### Note

Anda dapat memilih untuk tidak mengonfigurasi CAA catatan untuk domain Anda jika Anda tidak ingin mengaktifkan CAA pemeriksaan.

## Masalah impor sertifikat

Anda dapat mengimpor sertifikat pihak ketiga ke dalam ACM dan mengaitkannya dengan [layanan terintegrasi](#). [Jika Anda mengalami masalah, tinjau prasyarat dan topik format sertifikat](#). Secara khusus, perhatikan hal berikut:

- Anda hanya dapat mengimpor X.509 versi SSL 3/sertifikat. TLS
- Sertifikat Anda dapat ditandatangani sendiri atau dapat ditandatangani oleh otoritas sertifikat (CA).
- Jika sertifikat Anda ditandatangani oleh CA, Anda harus menyertakan rantai sertifikat perantara yang menyediakan jalur ke akar otoritas.
- Jika sertifikat Anda ditandatangani sendiri, Anda harus menyertakan kunci pribadi dalam teks biasa.
- Setiap sertifikat dalam rantai harus secara langsung mengesahkan yang sebelumnya.
- Jangan sertakan sertifikat entitas akhir Anda dalam rantai sertifikat perantara.
- Sertifikat, rantai sertifikat, dan kunci pribadi Anda (jika ada) harus PEM —dikodekan. Secara umum, PEM pengkodean terdiri dari blok teks yang dikodekan Base64 yang dimulai dan diakhiri dengan header ASCII teks biasa dan garis footer. Anda tidak boleh menambahkan baris atau spasi atau membuat perubahan lain pada PEM file saat menyalin atau mengunggahnya. Anda dapat memverifikasi rantai sertifikat menggunakan [utilitas Open SSL Verify](#).
- Kunci pribadi Anda (jika ada) tidak boleh dienkripsi. (Tip: jika memiliki frasa sandi, itu dienkripsi.)
- Layanan yang [terintegrasi](#) dengan ACM harus menggunakan ACM algoritme dan ukuran kunci yang didukung. Lihat AWS Certificate Manager Panduan Pengguna dan dokumentasi untuk setiap layanan untuk memastikan bahwa sertifikat Anda akan berfungsi.
- Dukungan sertifikat oleh layanan terintegrasi mungkin berbeda tergantung pada apakah sertifikat diimpor ke IAM atau ke dalam ACM.
- Sertifikat harus valid ketika diimpor.
- Informasi detail untuk semua sertifikat Anda ditampilkan di konsol. Namun, secara default, jika Anda memanggil [ListCertificates](#) API atau [daftar-sertifikat](#) AWS CLI perintah tanpa menentukan keyTypes filter, hanya RSA\_1024 atau RSA\_2048 sertifikat yang ditampilkan.

## Masalah penyematan sertifikat

Untuk memperbarui sertifikat, buat key ACM pair public-private baru. Jika aplikasi Anda menggunakan [Penyematan sertifikat](#), kadang-kadang dikenal sebagai SSL menyematkan, untuk

menyematkan ACM sertifikat, aplikasi mungkin tidak dapat terhubung ke domain Anda setelahnya. AWS memperbarui sertifikat. Untuk alasan ini, kami menyarankan Anda untuk tidak menyematkan ACM sertifikat. Jika aplikasi Anda harus menyematkan sertifikat, Anda dapat melakukan hal berikut:

- [Impor sertifikat Anda sendiri ke dalam ACM](#) dan kemudian pin aplikasi Anda ke sertifikat yang diimpor. ACM tidak menyediakan perpanjangan terkelola untuk sertifikat yang diimpor.
- Jika Anda menggunakan sertifikat publik, sematkan aplikasi Anda ke semua [sertifikat root Amazon](#) yang tersedia. Jika Anda menggunakan sertifikat pribadi, sematkan aplikasi Anda ke sertifikat root CA.

## API Masalah gateway

Saat Anda menerapkan API titik akhir yang dioptimalkan tepi, API Gateway menyiapkan distribusi untuk Anda. CloudFront CloudFront Distribusi dimiliki oleh API Gateway, bukan oleh akun Anda. Distribusi terikat pada ACM sertifikat yang Anda gunakan saat menerapkan. API Untuk menghapus pengikatan dan memungkinkan ACM untuk menghapus sertifikat Anda, Anda harus menghapus domain kustom API Gateway yang terkait dengan sertifikat.

Saat Anda menerapkan API titik akhir regional, API Gateway membuat penyeimbang beban aplikasi (ALB) atas nama Anda. Load balancer dimiliki oleh API Gateway dan tidak terlihat oleh Anda. ALB ini terikat pada ACM sertifikat yang Anda gunakan saat menerapkan. API Untuk menghapus pengikatan dan memungkinkan ACM untuk menghapus sertifikat Anda, Anda harus menghapus domain kustom API Gateway yang terkait dengan sertifikat.

## Apa yang harus dilakukan ketika sertifikat kerja gagal secara tak terduga

Jika Anda telah berhasil mengaitkan ACM sertifikat dengan layanan terintegrasi, tetapi sertifikat berhenti bekerja dan layanan terintegrasi mulai mengembalikan kesalahan, penyebabnya mungkin adalah perubahan dalam izin yang dibutuhkan layanan untuk menggunakan ACM sertifikat.

Misalnya, Elastic Load Balancing (ELB) memerlukan izin untuk mendekripsi AWS KMS key yang, pada gilirannya, mendekripsi kunci pribadi sertifikat. Izin ini diberikan oleh kebijakan berbasis sumber daya yang ACM berlaku saat Anda mengaitkan sertifikat dengan. ELB Jika ELB kehilangan hibah untuk izin itu, itu akan gagal saat berikutnya mencoba mendekripsi kunci sertifikat.

Untuk menyelidiki masalah, periksa status hibah Anda menggunakan AWS KMS konsol di <https://console.aws.amazon.com/kms>. Kemudian ambil salah satu tindakan berikut:

- Jika Anda yakin bahwa izin yang diberikan kepada layanan terintegrasi telah dicabut, kunjungi konsol layanan terintegrasi, lepaskan sertifikat dari layanan, lalu kaitkan kembali. Ini akan menerapkan kembali kebijakan berbasis sumber daya dan menerapkan hibah baru.
- Jika Anda yakin bahwa izin yang diberikan ACM telah dicabut, hubungi Support di <https://console.aws.amazon.com/support/#/>.

## Masalah dengan peran ACM terkait layanan () SLR

Saat Anda mengeluarkan sertifikat yang ditandatangani oleh CA pribadi yang telah dibagikan dengan Anda oleh akun lain, ACM mencoba penggunaan pertama untuk menyiapkan peran terkait layanan (SLR) untuk berinteraksi sebagai prinsipal dengan AWS Private CA [kebijakan akses berbasis sumber daya](#). Jika Anda mengeluarkan sertifikat pribadi dari CA bersama dan tidak SLR ada, tidak ACM akan dapat memperbarui sertifikat itu secara otomatis untuk Anda.

ACM mungkin mengingatkan Anda bahwa itu tidak dapat menentukan apakah SLR ada di akun Anda. Jika `iam:GetRole` izin yang diperlukan telah diberikan kepada akun Anda, maka peringatan tidak akan terulang kembali setelah SLR dibuat. ACM SLR Jika terulang kembali, Anda atau administrator akun Anda mungkin perlu memberikan `iam:GetRole` izin ACM, atau mengaitkan akun Anda dengan kebijakan ACM `-managed.AWSCertificateManagerFullAccess`

Untuk informasi selengkapnya, lihat [Izin Peran Tertaut Layanan](#) di Panduan Pengguna. IAM

## Menangani pengecualian

Sesi AWS Certificate Manager perintah mungkin gagal karena beberapa alasan. Untuk informasi tentang setiap pengecualian, lihat tabel di bawah ini.

### Penanganan pengecualian sertifikat pribadi

Pengecualian berikut dapat terjadi ketika Anda mencoba memperbarui PKI sertifikat pribadi yang dikeluarkan oleh AWS Private CA.

#### Note

AWS Private CA tidak didukung di Wilayah China (Beijing) dan Wilayah China (Ningxia).

ACMkode kegagalan	Komentar
PCA_ACCESS_DENIED	<p>CA pribadi belum memberikan ACM izin. Hal ini memicu a <code>AWS Private CA AccessDeniedException</code> kode kegagalan.</p> <p>Untuk mengatasi masalah tersebut, berikan izin yang diperlukan kepada prinsipal ACM layanan menggunakan AWS Private CA <a href="#">CreatePermission</a> operasi.</p>
PCA_INVALID_DURATION	<p>Masa berlaku sertifikat yang diminta melebihi masa berlaku CA swasta yang menerbitkan. Hal ini memicu a <code>AWS Private CA ValidationException</code> kode kegagalan.</p> <p>Untuk mengatasi masalah tersebut, <a href="#">instal sertifikat CA baru</a> dengan masa berlaku yang sesuai.</p>
PCA_INVALID_STATE	<p>CA pribadi yang dipanggil tidak dalam keadaan yang benar untuk melakukan ACM operasi yang diminta. Hal ini memicu a <code>AWS Private CA InvalidStateException</code> kode kegagalan.</p> <p>Selesaikan masalah sebagai berikut:</p> <ul style="list-style-type: none"><li>• Jika CA memiliki status <code>CREATING</code>, tunggu pembuatan selesai dan kemudian instal sertifikat CA.</li><li>• Jika CA memiliki status <code>PENDING_CERTIFICATE</code>, instal sertifikat CA.</li><li>• Jika CA memiliki status <code>DISABLED</code>, perbarui ke <code>ACTIVE</code> status.</li><li>• Jika CA memiliki status <code>DELETED</code>, kembalika n.</li></ul>

ACMkode kegagalan	Komentar
	<ul style="list-style-type: none"><li>• Jika CA memiliki statusEXPIRED, instal sertifikat baru</li><li>• Jika CA memiliki statusFAILED, dan Anda tidak dapat menyelesaikan masalah, hubungi <a href="#">Support</a>.</li></ul>
PCA_LIMIT_EXCEEDED	<p>CA swasta telah mencapai kuota penerbitan. Hal ini memicu a AWS Private CA LimitExceededException kode kegagalan. Coba ulangi permintaan Anda sebelum melanjutkan dengan bantuan ini.</p> <p>Jika kesalahan berlanjut, hubungi <a href="#">Support</a> untuk meminta peningkatan kuota.</p>
PCA_REQUEST_FAILED	<p>Terjadi kesalahan jaringan atau sistem. Hal ini memicu a AWS Private CA RequestFailedException kode kegagalan. Coba ulangi permintaan Anda sebelum melanjutkan dengan bantuan ini.</p> <p>Jika kesalahan berlanjut, hubungi <a href="#">Support</a>.</p>
PCA_RESOURCE_NOT_FOUND	<p>CA pribadi telah dihapus secara permanen. Hal ini memicu a AWS Private CA ResourceNotFoundException kode kegagalan. Verifikasi bahwa Anda menggunakan yang benarARN. Jika gagal, Anda tidak akan dapat menggunakan CA ini.</p> <p>Untuk mengatasi masalah tersebut, <a href="#">buat CA baru</a>.</p>

ACMkode kegagalan	Komentar
SLR_NOT_FOUND	Untuk memperbarui sertifikat yang ditandatangani oleh CA pribadi yang berada di akun lain, ACM diperlukan Service Linked Role (SLR) pada akun tempat sertifikat berada. Jika Anda perlu membuat ulang yang dihapus SLR, lihat <a href="#">Menciptakan SLR untuk ACM</a> .

# Kuota

Kuota layanan AWS Certificate Manager (ACM) berikut berlaku untuk setiap AWS wilayah per setiap AWS akun.

Untuk melihat kuota apa yang dapat disesuaikan, lihat [tabel ACM kuota](#) di Panduan Referensi AWS Umum. Untuk meminta peningkatan kuota, buat kasus di [Support Pusat](#).

## Kuota umum

Item	Kuota default
<p>Jumlah ACM sertifikat</p> <p>Sertifikat yang kedaluwarsa dan dicabut terus dihitung terhadap total ini.</p> <p>Sertifikat yang ditandatangani oleh CA dari AWS Private CA tidak dihitung terhadap total ini.</p>	2500
<p>Jumlah ACM sertifikat per tahun (365 hari terakhir)</p> <p>Anda dapat meminta hingga dua kali kuota ACM sertifikat per tahun, wilayah, dan akun. Misalnya, jika kuota Anda 2.500, Anda dapat meminta hingga 5.000 ACM sertifikat per tahun di wilayah dan akun tertentu. Anda hanya dapat memiliki 2.500 sertifikat pada waktu tertentu. Untuk meminta 5.000 sertifikat dalam setahun, Anda harus menghapus 2.500 selama setahun untuk tetap dalam kuota. Jika Anda membutuhkan lebih dari 2.500 sertifikat pada waktu tertentu, Anda harus menghubungi <a href="#">Support Pusat</a>.</p>	5.000



Item	Kuota default
Sertifikat yang ditandatangani oleh CA dari AWS Private CA tidak dihitung terhadap total ini.	
Jumlah sertifikat yang diimpor	2.500
Jumlah sertifikat impor per tahun (365 hari terakhir)	5.000
Jumlah nama domain per ACM sertifikat	10
<p>Kuota default adalah 10 nama domain untuk setiap ACM sertifikat. Kuota Anda mungkin lebih besar.</p> <p>Nama domain pertama yang Anda kirimkan disertakan sebagai nama umum subjek (CN) sertifikat. Semua nama disertakan dalam ekstensi Nama Alternatif Subjek.</p> <p>Anda dapat meminta hingga 100 nama domain. Untuk meminta peningkatan kuota Anda, buat permintaan di konsol Service Quotas untuk ACM layanan. Namun, sebelum membuat kasus, pastikan Anda memahami bagaimana menambahkan lebih banyak nama domain dapat membuat lebih banyak pekerjaan administratif untuk Anda jika Anda menggunakan validasi email. Untuk informasi selengkapnya, lihat <a href="#">Validasi domain</a>.</p> <p>Kuota untuk jumlah nama domain per ACM sertifikat hanya berlaku untuk sertifikat yang disediakan oleh ACM. Kuota ini tidak berlaku untuk sertifikat yang Anda impor ACM. Bagian berikut hanya berlaku untuk ACM sertifikat.</p>	

Item	Kuota default
<p>Jumlah Pribadi CAs</p> <p>ACM terintegrasi dengan AWS Private Certificate Authority (AWS Private CA). Anda dapat menggunakan ACM konsol, AWS CLI, atau ACM API meminta sertifikat pribadi dari otoritas sertifikat pribadi (CA) yang ada yang dihosting oleh AWS Private CA. Sertifikat ini dikelola dalam ACM lingkungan dan memiliki batasan yang sama dengan sertifikat publik yang dikeluarkan oleh ACM. Untuk informasi selengkapnya, lihat <a href="#">Minta sertifikat pribadi di AWS Certificate Manager</a>. Anda juga dapat mengeluarkan sertifikat pribadi dengan menggunakan AWS Private CA layanan mandiri. Untuk informasi selengkapnya, lihat <a href="#">Menerbitkan Sertifikat Entitas Akhir Pribadi</a>. CA pribadi yang telah dihapus akan dihitung terhadap kuota Anda hingga akhir periode restorasi. Untuk informasi selengkapnya, lihat <a href="#">Menghapus CA Pribadi Anda</a>.</p>	200
Jumlah Sertifikat Pribadi per CA (seumur hidup)	1.000.000

## API kuota tarif

Kuota berikut berlaku ACM API untuk setiap wilayah dan akun. ACM throttles API permintaan pada kuota yang berbeda tergantung pada operasi. API Throttling berarti ACM menolak permintaan yang valid karena permintaan melebihi kuota operasi untuk jumlah permintaan per detik. Ketika permintaan dibatasi, ACM mengembalikan kesalahan. `ThrottlingException` Tabel berikut mencantumkan setiap API operasi dan kuota di mana permintaan ACM throttles untuk operasi itu.

**Note**

Selain API tindakan yang tercantum dalam tabel di bawah ini, juga ACM dapat memanggil `IssueCertificate` tindakan eksternal dari AWS Private CA. Untuk informasi kuota up-to-date `tarifIssueCertificate`, lihat [titik akhir dan kuota](#) untuk AWS Private CA

## Requests-per-second kuota untuk setiap operasi ACM API

API panggilan	Permintaan per detik
<code>AddTagsToCertificate</code>	5
<code>DeleteCertificate</code>	10
<code>DescribeCertificate</code>	10
<code>ExportCertificate</code>	10
<code>GetAccountConfiguration</code>	1
<code>GetCertificate</code>	10
<code>ImportCertificate</code>	1
<code>ListCertificates</code>	8
<code>ListTagsForCertificate</code>	10
<code>PutAccountConfiguration</code>	1
<code>RemoveTagsFromCertificate</code>	5
<code>RenewCertificate</code>	5
<code>RequestCertificate</code>	5
<code>ResendValidationEmail</code>	1
<code>UpdateCertificateOptions</code>	5

Untuk informasi selengkapnya, lihat [AWS Certificate Manager API Referensi](#).

# Riwayat dokumen

Tabel berikut menjelaskan riwayat rilis dokumentasi AWS Certificate Manager dimulai pada tahun 2018.

Perubahan	Deskripsi	Tanggal
<a href="#">Penutupan validasi email mail exchanger (MX)</a>	ACMKonsol tidak lagi mendukung penukar surat (MX).	Juli 11, 2024
<a href="#">Menambahkan praktik terbaik seputar pemisahan tingkat akun</a>	Gunakan pemisahan tingkat akun dalam kebijakan Anda sedapat mungkin. Jika tidak memungkinkan, Anda dapat membatasi izin di tingkat akun atau melalui kunci kondisi konteks enkripsi dalam kebijakan Anda.	Juni 11, 2024
<a href="#">penghentian verifikasi email yang akan datang WHOIS</a>	Menambahkan catatan tentang penghentian verifikasi WHOIS email mulai Juni 2024.	Februari 5, 2024
<a href="#">Dukungan kunci kondisi ditambahkan</a>	Menambahkan dukungan untuk tombol IAM Kondisi saat meminta ACM sertifikat. Untuk daftar kondisi yang didukung, lihat <a href="https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported">https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported</a> .	24 Agustus 2023
<a href="#">ECDSA dukungan ditambahkan</a>	Menambahkan dukungan untuk Elliptic Curve Digital Signature Algorithm (ECDSA)	8 November 2022

saat meminta sertifikat publik. ACM Untuk daftar algoritme kunci yang didukung, lihat <https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms>.

### CloudWatch Acara Baru

Ditambahkan ACM Sertifikat Kedaluwarsa, ACM Sertifikat Tersedia, dan Tindakan Perpanjangan ACM Sertifikat Acara yang diperlukan. Untuk daftar CloudWatch Acara yang didukung, lihat <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html>.

27 Oktober 2022

### Memperbarui jenis algoritme kunci untuk impor

Sertifikat yang diimpor ke sekarang ACM mungkin memiliki kunci dengan algoritma tambahan RSA dan Elliptic Curve. Untuk daftar algoritme kunci yang saat ini didukung, lihat <https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html>.

14 Juli 2021

[Mempromosikan “Monitoring and Logging” sebagai bagian terpisah](#)

Memindahkan dokumentasi pemantauan dan pencatatan ke babnya sendiri. Perubahan ini mencakup CloudWatch Metrik, Peristiwa CloudWatch / EventBridge, dan. CloudTrail Untuk informasi selengkapnya, lihat <https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html>.

23 Maret 2021

[Menambahkan CloudWatch dukungan Metrik dan Acara](#)

Ditambahkan DaysToExpired metrik dan acara dan dukungan APIs. Untuk informasi selengkapnya, silakan lihat <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html> dan <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html>.

3 Maret 2021

[Menambahkan dukungan lintas akun](#)

Menambahkan dukungan lintas akun untuk menggunakan pribadi CAs dari AWS Private CA Untuk informasi selengkapnya, lihat <https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html>.

17 Agustus 2020

<a href="#">Ditambahkan dukungan wilayah</a>	Ditambahkan dukungan wilayah untuk AWS Wilayah China (Beijing dan Ningxia). Untuk daftar lengkap wilayah yang didukung, lihat <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region</a> .	4 Maret 2020
<a href="#">Menambahkan pengujian alur kerja pembaruan</a>	Pelanggan sekarang dapat secara manual menguji konfigurasi alur kerja pembaruan ACM terkelola mereka. Untuk informasi selengkapnya, lihat <a href="#">Menguji Konfigurasi Pembaruan ACM Terkelola</a> .	14 Maret 2019
<a href="#">Pencatatan transparansi sertifikat sekarang default</a>	Ditambahkan kemampuan untuk menerbitkan sertifikat ACM publik ke dalam log transparansi sertifikat secara default.	April 24, 2018
<a href="#">Peluncuran AWS Private CA</a>	Meluncurkan ACM Private Certificate Manager (CM), dan perpanjangan AWS Certificate Manager yang memungkinkan pengguna untuk membangun infrastruktur terkelola yang aman untuk menerbitkan dan mencabut sertifikat digital pribadi. Untuk informasi selengkapnya, silakan lihat <a href="#">AWS Otoritas Sertifikat Swasta</a> .	4 April 2018



[Pencatatan transparansi sertifikat](#)

Menambahkan pencatatan transparansi sertifikat ke Praktik Terbaik.

27 Maret 2018

Tabel berikut menjelaskan riwayat rilis dokumentasi AWS Certificate Manager sebelum 2018.

Perubahan	Deskripsi	Tanggal Rilis
Konten baru	Ditambahkan DNS validasi ke <a href="#">AWS Certificate Manager DNS validasi</a> .	21 November 2017
Konten baru	Menambahkan contoh kode Java baru ke <a href="#">Gunakan AWS Certificate Manager dengan SDK untuk Java</a> .	12 Oktober 2017
Konten baru	Menambahkan informasi tentang CAA catatan ke <a href="#">(Opsional) Konfigurasi CAA catatan</a> .	21 September 2017
Konten baru	Menambahkan informasi tentang domain.IO ke <a href="#">Memecahkan masalah dengan AWS Certificate Manager</a>	Juli 07, 2017
Konten baru	Menambahkan informasi tentang mengimpor ulang sertifikat ke <a href="#">Impor ulang sertifikat</a>	Juli 07, 2017
Konten baru	Menambahkan informasi tentang penyematan sertifikat ke <a href="#">Praktik terbaik</a> dan ke <a href="#">Memecahkan masalah</a>	Juli 07, 2017

Perubahan	Deskripsi	Tanggal Rilis
	<a href="#">dengan AWS Certificate Manager</a> .	
Konten baru	Ditambahkan AWS CloudFormation ke <a href="#">Layanan terintegrasi dengan ACM</a> .	27 Mei 2017
Perbarui	Menambahkan informasi lebih lanjut ke <a href="#">Kuota</a> .	27 Mei 2017
Konten baru	Penambahan dokumentasi tentang <a href="#">Identity and Access Management untuk AWS Certificate Manager</a> .	28 April 2017
Perbarui	Ditambahkan grafik untuk menunjukkan di mana email validasi dikirim. Lihat <a href="#">AWS Certificate Manager validasi email</a> .	April 21, 2017
Perbarui	Menambahkan informasi tentang pengaturan email untuk domain Anda. Lihat <a href="#">AWS Certificate Manager validasi email</a> .	6 April 2017
Perbarui	Menambahkan informasi tentang memeriksa status perpanjangan sertifikat di konsol. Lihat <a href="#">Periksa status perpanjangan sertifikat</a> .	28 Maret 2017
Perbarui	Memperbarui dokumentasi untuk menggunakan Elastic Load Balancing.	21 Maret 2017

Perubahan	Deskripsi	Tanggal Rilis
Konten baru	Ditambahkan dukungan untuk AWS Elastic Beanstalk dan Amazon API Gateway. Lihat <a href="#">Layanan terintegrasi dengan ACM</a> .	21 Maret 2017
Perbarui	Pembaruan dokumentasi tentang <a href="#">Perpanjangan sertifikat dikelola</a> .	20 Februari 2017
Konten baru	Penambahan dokumentasi tentang <a href="#">Sertifikat yang diimpor</a> .	13 Oktober 2016
Konten baru	Ditambahkan AWS CloudTrail dukungan untuk ACM tindakan. Lihat <a href="#">Menggunakan CloudTrail dengan AWS Certificate Manager</a> .	25 Maret 2016
Panduan baru	Rilis ini memperkenalkan AWS Certificate Manager.	21 Januari 2016

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.