



Benutzerhandbuch

AWS Certificate Manager



Version 1.0

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

AWS Certificate Manager: Benutzerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Certificate Manager?	1
Unterstützte Regionen	1
Preisgestaltung	2
Konzepte	2
ACMZertifikat	3
ACMRoot CAs	5
Apex-Domain	5
Verschlüsselung mit asymmetrischem Schlüssel	5
Zertifizierungsstelle	6
Protokollierung der Zertifikatstransparenz	6
Domain Name System	7
Domainnamen	7
Ver- und Entschlüsselung	9
Vollqualifizierter Domainname () FQDN	9
Public Key Infrastructure	9
Stammzertifikat	9
Secure Sockets Layer () SSL	9
Sicher HTTPS	10
SSLServerzertifikate	10
Symmetrische Schlüssel-Kryptografie	10
Sicherheit auf Transportschicht (TLS)	10
Vertrauensstellung	10
Was ist das Richtige AWS Zertifikatsservice für meine Bedürfnisse?	11
Zertifikate	12
Einrichten	13
Melden Sie sich an für eine AWS-Konto	13
Erstellen eines Benutzers mit Administratorzugriff	14
Registrieren eines Domainnamens	15
(Optional) Konfigurieren Sie einen CAA Datensatz	16
Öffentliche Zertifikate	18
Merkmale und Einschränkungen	19
Fordern Sie ein öffentliches Zertifikat an	25
Prüfen des Domainbesitzes	28
Private Zertifikate	42

Bedingungen für die Nutzung	43
Fordern Sie ein privates Zertifikat an	44
Zertifikat exportieren	48
Importierte Zertifikate	51
Voraussetzungen	52
Zertifikatformat	53
Importieren des Zertifikats	55
Erneutes Importieren eines Zertifikats	57
Zertifikate auflisten	59
Zertifikatsdetails anzeigen	62
Zertifikate löschen	66
Verwaltete Zertifikatserneuerung	68
Öffentliche Zertifikate	70
Verlängerung für DNS -validierte Domains	70
E-Mail-Validierung	70
Private Zertifikate	72
Automatisieren Sie den Export erneuerter Zertifikate	73
Testen der verwalteten Erneuerung	74
Prüfen des Erneuerungsstatus	76
Überprüfen des Status (Konsole)	77
Überprüfen Sie den Status (API)	77
Überprüfen Sie den Status (CLI)	77
Überprüfen Sie den Status mit dem Personal Health Dashboard (PHD)	78
Markieren von Ressourcen	79
Tag-Einschränkungen	79
Verwalten von Tags	80
Verwalten von Tags (Konsole)	80
Tags verwalten (CLI)	82
Verwalten von Tags	82
Integrierte Services	83
Sicherheit	89
Datenschutz	90
Sicherheit für private Zertifikatsschlüssel	91
Identitäts- und Zugriffsverwaltung	92
Zielgruppe	92
Authentifizierung mit Identitäten	93

Verwalten des Zugriffs mit Richtlinien	97
Wie AWS Certificate Manager funktioniert mit IAM	100
Beispiele für identitätsbasierte Richtlinien	107
Referenztable für ACM-API-Berechtigungen	112
Von AWS verwaltete Richtlinien	114
Verwenden Sie Bedingungsschlüssel	117
Serviceverknüpfte Rollen verwenden	123
Fehlerbehebung	126
Ausfallsicherheit	129
Sicherheit der Infrastruktur	129
Gewährung des programmatischen Zugriffs auf ACM	130
Bewährte Methoden	132
Trennung auf Kontoebene	132
AWS CloudFormation	133
Zertifikat-Pinning	133
Domainvalidierung	134
Hinzufügen oder Löschen von Domainnamen	134
Abmelden von der Protokollierung für Zertifikatstransparenz	135
Einschalten AWS CloudTrail	137
Überwachen und protokollieren	138
Amazon EventBridge	138
Unterstützte Ereignisse	138
Beispielaktionen	143
CloudTrail	153
Unterstützte API Aktionen	154
APIAufrufe für integrierte Dienste	168
CloudWatch Metriken	173
Verwenden Sie AWS Certificate Manager mit dem SDK für Java	175
AddTagsToCertificate	175
DeleteCertificate	177
DescribeCertificate	179
ExportCertificate	182
GetCertificate	185
ImportCertificate	187
ListCertificates	191
RenewCertificate	193

ListTagsForCertificate	195
RemoveTagsFromCertificate	197
RequestCertificate	199
ResendValidationEmail	202
Fehlerbehebung	205
Zertifikatsanforderungen	205
Zeitüberschreitung bei der Anforderung	205
Anforderung schlägt fehl	206
Zertifikatsvalidierung	207
DNSValidierung	208
E-Mail-Validierung	211
Zertifikatserneuerung	213
Vorbereitung auf die automatische Domaininvalidierung	214
Behandlung von Fehlern bei der Erneuerung verwalteter Zertifikate	214
Weitere Probleme	216
CAAaufzeichnungen	217
Zertifikatsimport	218
Zertifikat-Pinning	219
APIGateway	219
Unerwarteter Fehler	219
Probleme mit der ACM serviceverknüpften Rolle () SLR	220
Umgang mit Ausnahmen	221
Umgang mit Ausnahmen bei privaten Zertifikaten	221
Kontingente	225
Allgemeine Kontingente	225
APIKontingente bewerten	228
Dokumentverlauf	231
.....	ccxxxix

Was ist AWS Certificate Manager?

AWS Certificate Manager (ACM) bewältigt die Komplexität der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS Websites und Anwendungen. Sie können Zertifikate für Ihre [integrierten Geräte bereitstellen AWS Dienste, indem Sie sie](#) entweder direkt zusammen mit Zertifikaten von Drittanbietern ausstellen ACM oder indem Sie Zertifikate von Drittanbietern in das ACM Verwaltungssystem [importieren](#). ACM Zertifikate können einzelne Domainnamen, mehrere spezifische Domainnamen, Wildcard-Domains oder Kombinationen davon schützen. ACM Wildcard-Zertifikate können eine unbegrenzte Anzahl von Subdomains schützen. Sie können auch ACM Zertifikate [exportieren](#), die signiert sind von AWS Private CA zur Verwendung überall in Ihrem internen Bereich PKI.

Note

ACM ist nicht für die Verwendung mit einem eigenständigen Webserver vorgesehen. Wenn Sie einen eigenständigen sicheren Server auf einer EC2 Amazon-Instance einrichten möchten, finden Sie im folgenden Tutorial Anweisungen: [Configure SSL/TLS on Amazon Linux 2023](#).

Themen

- [Unterstützte Regionen](#)
- [Preisgestaltung für AWS Certificate Manager](#)
- [AWS Certificate Manager Konzepte](#)
- [Was ist das Richtige AWS Zertifikatsservice für meine Bedürfnisse?](#)

Unterstützte Regionen

Besuch [AWS Regionen und Endpunkte](#) in der Allgemeine AWS-Referenz oder die [AWS Regionentabelle](#), um die regionale Verfügbarkeit für zu sehen ACM.

Zertifikate in ACM sind regionale Ressourcen. Um ein Zertifikat mit Elastic Load Balancing für denselben vollqualifizierten Domainnamen (FQDN) oder für mehrere Domainnamen zu verwenden FQDNs AWS Sie müssen für jede Region ein Zertifikat anfordern oder importieren. Für Zertifikate, die von bereitgestellt werden ACM, bedeutet dies, dass Sie jeden Domainnamen im Zertifikat für jede Region erneut validieren müssen. Sie können keine Zertifikate zwischen Regionen kopieren.

Um ein ACM Zertifikat bei Amazon verwenden zu können CloudFront, müssen Sie das Zertifikat in der Region USA Ost (Nord-Virginia) anfordern oder importieren. ACMZertifikate in dieser Region, die einer CloudFront Verteilung zugeordnet sind, werden an alle für diese Verteilung konfigurierten geografischen Standorte verteilt.

Preisgestaltung für AWS Certificate Manager

Für SSL TLS /-Zertifikate, mit denen Sie verwalten, fallen keine zusätzlichen Gebühren an AWS Certificate Manager. Sie zahlen nur für AWS Ressourcen, die Sie für den Betrieb Ihrer Website oder Anwendung erstellen. Die neuesten ACM Preisinformationen finden Sie auf der [AWS Certificate Manager](#) Seite mit Servicepreisen auf der AWS Webseite.

AWS Certificate Manager Konzepte

Dieser Abschnitt enthält Definitionen der Konzepte, die verwendet werden von AWS Certificate Manager.

Themen

- [ACMZertifikat](#)
- [ACMRoot CAs](#)
- [Apex-Domain](#)
- [Verschlüsselung mit asymmetrischem Schlüssel](#)
- [Zertifizierungsstelle](#)
- [Protokollierung der Zertifikatstransparenz](#)
- [Domain Name System](#)
- [Domainnamen](#)
- [Ver- und Entschlüsselung](#)
- [Vollqualifizierter Domainname \(\) FQDN](#)
- [Public Key Infrastructure](#)
- [Stammzertifikat](#)
- [Secure Sockets Layer \(\) SSL](#)
- [Sicher HTTPS](#)
- [SSLServerzertifikate](#)
- [Symmetrische Schlüssel-Kryptografie](#)

- [Sicherheit auf Transportschicht \(TLS\)](#)
- [Vertrauensstellung](#)

ACMZertifikat

ACM generiert X.509-Zertifikate der Version 3. Jedes Zertifikat ist 13 Monate (395 Tage) gültig und enthält die folgenden Erweiterungen.

- Basic Constraints– gibt an, ob das Subject des Zertifikats eine Zertifizierungsstelle (CA) ist
- Authority Key Identifier– ermöglicht die Identifizierung des öffentlichen Schlüssels, der dem privaten Schlüssel entspricht, mit dem das Zertifikat signiert wurde.
- Subject Key Identifier– ermöglicht die Identifizierung von Zertifikaten, die einen bestimmten öffentlichen Schlüssel enthalten.
- Key Usage– definiert den Zweck des im Zertifikat eingebetteten öffentlichen Schlüssels.
- Extended Key Usage– gibt einen oder mehrere Zwecke an, für die der öffentliche Schlüssel zusätzlich zu den von der Erweiterung Key Usage angegebenen Zwecken verwendet werden kann.
- CRL Verteilungspunkte — gibt an, wo CRL Informationen abgerufen werden können.

Der Klartext eines ACM ausgestellten Zertifikats ähnelt dem folgenden Beispiel:

```
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
```

ACMRoot CAs

Den von ausgestellten öffentlichen Entity-Zertifikaten wird ihr Vertrauen von dem folgenden Amazon-Stammverzeichnis ACM abgeleitet: CAs

Definierter Name (Distinguished Name)	Verschlüsselungsalgorithmus
CN=Amazon Root CA 1, O=Amazon, C=US	2048-Bit RSA () RSA_2048
CN=Amazon Root CA 2, O=Amazon, C=US	4096-Bit RSA () RSA_4096
CN=Amazon Root CA 3, O=Amazon, C=US	Elliptic Prime Curve 256 Bit (EC_prime256v1)
CN=Amazon Root CA 4, O=Amazon, C=US	Elliptic Prime Curve 384 Bit (EC_secp384r1)

Die standardmäßige Vertrauensbasis für von ACM -ausgestellte Zertifikate ist CN=Amazon Root CA 1, O=Amazon, C=US, was 2048-Bit-Sicherheit bietet. RSA Die anderen Roots sind für die zukünftige Verwendung reserviert. Alle Roots werden durch das Starfield Services Root Certificate Authority-Zertifikat gegensigniert.

Weitere Informationen finden Sie unter [Amazon Trust Services](#).

Apex-Domain

Siehe [Domainnamen](#).

Verschlüsselung mit asymmetrischem Schlüssel

Im Gegensatz zu [Symmetrische Schlüssel-Kryptografie](#) verwendet die asymmetrische Verschlüsselung unterschiedliche, aber mathematisch zusammenhängende Schlüssel für die Ver- und Entschlüsselung von Inhalten. Einer der Schlüssel ist öffentlich und wird in der Regel in einem

X.509 v3-Zertifikat bereitgestellt. Der andere Schlüssel ist privat und sicher gespeichert. Das X.509-Zertifikat bindet die Identität eines Benutzers, Computers oder einer anderen Ressource (das Zertifikatssubjekt) an den öffentlichen Schlüssel.

ACMZertifikate sind SSL TLS X.509/-Zertifikate, die die Identität Ihrer Website und die Details Ihrer Organisation an den öffentlichen Schlüssel binden, der im Zertifikat enthalten ist. ACM verwendet dein AWS KMS key um den privaten Schlüssel zu verschlüsseln. Weitere Informationen finden Sie unter [Sicherheit für private Zertifikatsschlüssel](#).

Zertifizierungsstelle

Eine Zertifizierungsstelle (Certificate Authority, CA) ist eine Entität, die digitale Zertifikate ausstellt. Kommerziell basiert der gängigste digitale Zertifikatstyp auf dem ISO X.509-Standard. Die CA stellt signierte digitale Zertifikate aus, die die Identität des Zertifikat-Subjects bestätigen und diese Identität an den öffentlichen Schlüssel binden, der im Zertifikat enthalten ist. Eine CA verwaltet in der Regel auch die Zertifikataufhebung.

Protokollierung der Zertifikatstransparenz

Zum Schutz vor TLS Zertifikaten vom TypSSL/, die versehentlich oder von einer kompromittierten Zertifizierungsstelle ausgestellt wurden, verlangen einige Browser, dass öffentliche Zertifikate, die für Ihre Domain ausgestellt wurden, in einem Transparenzprotokoll für Zertifikate aufgezeichnet werden. Der Domainname wird aufgezeichnet. der private Schlüssel nicht. Zertifikate, die nicht protokolliert werden, erzeugen typischerweise einen Fehler im Browser.

Sie können die Protokolle überwachen, um sicherzustellen, dass nur von Ihnen autorisierte Zertifikate für Ihre Domain ausgestellt wurden. Sie können einen Service wie z. B. [Certificate Search](#) nutzen, um die Protokolle zu überprüfen.

Bevor die Amazon CA ein öffentlich vertrauenswürdiges SSL TLS /-Zertifikat für Ihre Domain ausstellt, übermittelt sie das Zertifikat an mindestens drei Certificate Transparency Log-Server. Diese Server fügen das Zertifikat zu ihren öffentlichen Datenbanken hinzu und senden einen signierten Zertifikatszeitstempel (SCT) an die Amazon-Zertifizierungsstelle zurück. Die CA bettet das dann SCT in das Zertifikat ein, signiert das Zertifikat und stellt es Ihnen aus. Die Zeitstempel sind in anderen X.509-Erweiterungen enthalten.

```
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
```

Die Protokollierung der Zertifikatstransparenz erfolgt automatisch, wenn Sie ein Zertifikat anfordern oder erneuern, es sei denn, Sie entscheiden sich dafür, diesen Service nicht zu nutzen. Weitere Informationen zur Abmeldung finden Sie unter [Abmelden von der Protokollierung für Zertifikatstransparenz](#).

Domain Name System

Das Domain Name System (DNS) ist ein hierarchisch verteiltes Benennungssystem für Computer und andere Ressourcen, die mit dem Internet oder einem privaten Netzwerk verbunden sind. DNS wird hauptsächlich verwendet, um textuelle Domainnamen, z. B. `aws.amazon.com` in numerische IP-Adressen (Internet Protocol) der folgenden Form zu übersetzen: `111.122.133.144`. Die DNS-Datenbank für Ihre Domain enthält jedoch eine Reihe von Datensätzen, die für andere Zwecke verwendet werden können. Beispielsweise können ACM Sie anhand eines CNAME-Datensatzes überprüfen, ob Sie Eigentümer einer Domain sind oder diese kontrollieren, wenn Sie ein Zertifikat anfordern. Weitere Informationen finden Sie unter [AWS Certificate Manager DNS-Validierung](#).

Domainnamen

Ein Domainname ist eine Textzeichenfolge `www.example.com`, wie sie vom Domain Name System (DNS) in eine IP-Adresse übersetzt werden kann. Computernetzwerke, einschließlich des Internet, verwenden IP-Adressen statt Textnamen. Ein Domainname besteht aus unterschiedlichen Bezeichnungen, die jeweils durch einen Punkt voneinander getrennt werden:

TLD

Die Bezeichnung ganz rechts wird als Top-Level-Domain (TLD) bezeichnet. Allgemeine Beispiele sind unter anderem `.com`, `.net` und `.edu`. Außerdem ist die TLD Angabe für in einigen Ländern registrierte Unternehmen eine Abkürzung für den Ländernamen und wird als Ländercode bezeichnet. Beispiele sind unter anderem `.uk` für Großbritannien und Nordirland, `.ru` für Russland und `.fr` für Frankreich. Wenn Ländercodes verwendet werden, TLD wird häufig eine zweite Hierarchie für die eingeführt, um den Typ der registrierten Einheit zu identifizieren. Beispielsweise `.co.uk` TLD identifiziert der Handelsunternehmen im Vereinigten Königreich.

Apex-Domain

Der Apex-Domainname umfasst die Top-Level-Domain und erweitert diese. Für Domainnamen, die einen Ländercode enthalten, beinhaltet die Apex-Domain den Code und gegebenenfalls die Bezeichnungen, die den Typ der registrierten Einheit identifizieren. Die Apex-Domain beinhaltet keine Unterdomains (siehe folgender Absatz). In `www.example.com` ist der Name der Apex-Domain `example.com`. In `www.example.co.uk` ist der Name der Apex-Domain `example.co.uk`. Andere Namen, die häufig anstelle von apex verwendet werden, sind unter anderem `base`, `bare`, `root`, `root apex` oder `zone apex`.

Unterdomain

Unterdomainnamen stehen vor dem Apex-Domainnamen und werden von diesem sowie voneinander durch jeweils einen Punkt getrennt. Der gebräuchlichste Unterdomainname ist `www`, es ist jedoch auch jeder andere Name möglich. Unterdomainnamen können mehrere Ebenen haben. Beispielsweise sind in `jake.dog.animals.example.com` die Unterdomains `jake`, `dog` und `animals`.

Superdomain

Die Domain, zu der eine Subdomain gehört.

FQDN

Ein vollqualifizierter Domainname (FQDN) ist der vollständige DNS Name für einen Computer, eine Website oder eine andere Ressource, die mit einem Netzwerk oder dem Internet verbunden ist. Zum Beispiel `aws.amazon.com` der FQDN für Amazon Web Services. An FQDN umfasst alle Domains bis hin zur Top-Level-Domain. `[subdomain1].[subdomain2]. . . [subdomainn].[apex domain].[top-level domain]`Stellt beispielsweise das allgemeine Format eines dar. FQDN

PQDN

Ein Domänenname, der nicht vollständig qualifiziert ist, wird als teilqualifizierter Domänenname (PQDN) bezeichnet und ist mehrdeutig. Ein Name wie [subdomain₁.subdomain₂.] ist aPQDN, weil die Stammdomäne nicht bestimmt werden kann.

Ver- und Entschlüsselung

Die Verschlüsselung ist der Prozess, um Daten vertraulich bereitzustellen. Die Entschlüsselung kehrt den Prozess um und stellt die ursprünglichen Daten wieder her. Nicht verschlüsselte Daten werden in der Regel als Klartext bezeichnet, ob es sich um einen Text handelt oder nicht. Verschlüsselte Daten werden in der Regel Verschlüsselungstext genannt. HTTPSDie Verschlüsselung von Nachrichten zwischen Clients und Servern verwendet Algorithmen und Schlüssel. Algorithmen definieren das step-by-step Verfahren, mit dem Klartextdaten in Chiffretext (Verschlüsselung) und Chiffretext wieder in den ursprünglichen Klartext umgewandelt werden (Entschlüsselung). Schlüssel werden von Algorithmen während der Verschlüsselung und Entschlüsselung verwendet. Schlüssel können entweder privat oder öffentlich sein.

Vollqualifizierter Domainname () FQDN

Siehe [Domainnamen](#).

Public Key Infrastructure

Eine Public-Key-Infrastruktur (PKI) besteht aus Hardware, Software, Mitarbeitern, Richtlinien, Dokumenten und Verfahren, die zum Erstellen, Ausstellen, Verwalten, Verteilen, Verwenden, Speichern und Widerrufen digitaler Zertifikate erforderlich sind. PKI erleichtert die sichere Übertragung von Informationen über Computernetzwerke.

Stammzertifikat

Eine Zertifizierungsstelle (CA) besteht in der Regel innerhalb einer hierarchischen Struktur, die mehrere andere CAs mit klar definierten Eltern-Kind-Beziehungen zwischen ihnen enthält. Untergeordnete oder untergeordnete Personen CAs werden von ihren Eltern zertifiziert CAs, wodurch eine Zertifikatskette entsteht. Die CA oben in der Hierarchie wird als die Stamm-CA bezeichnet und ihr Zertifikat wird Stammzertifikat genannt. Dieses Zertifikat ist in der Regel selbstsigniert.

Secure Sockets Layer () SSL

Secure Sockets Layer (SSL) und Transport Layer Security (TLS) sind kryptografische Protokolle, die Kommunikationssicherheit über ein Computernetzwerk bieten. TLS ist der Nachfolger von SSL. Beide

verwenden X.509-Zertifikate, um den Server zu authentifizieren. Beide Protokolle verhandeln einen symmetrischen Schlüssel zwischen dem Client und dem Server, der für die Verschlüsselung von Daten zwischen den beiden Entitäten verwendet wird.

Sicher HTTPS

HTTPS steht für HTTP SSL over/TLS, eine sichere Form davon HTTP, die von allen gängigen Browsern und Servern unterstützt wird. Alle HTTP Anfragen und Antworten werden verschlüsselt, bevor sie über ein Netzwerk gesendet werden. HTTPS kombiniert das HTTP Protokoll mit symmetrischen, asymmetrischen und auf X.509-Zertifikaten basierenden kryptografischen Techniken. HTTPS funktioniert, indem im Modell Open Systems Interconnection (OSI) eine kryptografische Sicherheitsschicht unterhalb der HTTP Anwendungsschicht und oberhalb der TCP Transportschicht eingefügt wird. Die Sicherheitsebene verwendet das Secure Sockets Layer (SSL) -Protokoll oder das Transport Layer Security (TLS) -Protokoll.

SSL Serverzertifikate

Für Transaktionen sind Serverzertifikate erforderlich, um einen Server zu authentifizieren. Ein Serverzertifikat ist eine X.509-v3-Datenstruktur, mit der der öffentliche Schlüssel im Zertifikat an das Subject des Zertifikats gebunden wird. Ein SSL/TLS-Zertifikat ist von einer Zertifizierungsstelle (CA) signiert und enthält den Namen des Servers, den Gültigkeitszeitraum, den öffentlichen Schlüssel, den Signaturalgorithmus und mehr.

Symmetrische Schlüssel-Kryptografie

Die symmetrische Schlüssel-Kryptografie verwendet denselben Schlüssel zur Ver- und Entschlüsselung von digitalen Daten. Siehe auch [Verschlüsselung mit asymmetrischem Schlüssel](#).

Sicherheit auf Transportschicht (TLS)

Siehe [Secure Sockets Layer \(SSL\)](#).

Vertrauensstellung

Damit ein Webbrowser der Identität einer Website vertraut, muss der Browser das Zertifikat der Website überprüfen können. Browser vertrauen jedoch nur einer kleinen Anzahl von Zertifikaten, die als CA-Stammzertifikate bekannt sind. Ein vertrauenswürdiger Dritter, als Zertifikatsstelle (Certificate Authority, CA) bezeichnet, validiert die Identität der Website und stellt ein signiertes digitales Zertifikat für den Betreiber der Website aus. Der Browser kann dann die digitale Signatur überprüfen, um

die Identität der Website zu validieren. Wenn die Validierung erfolgreich ist, zeigt der Browser ein Schlosssymbol in der Adressleiste an.

Was ist das Richtige AWS Zertifikatsservice für meine Bedürfnisse?

AWS bietet Kunden, die verwaltete X.509-Zertifikate einsetzen, zwei Optionen. Wählen Sie die beste für Ihre Bedürfnisse aus.

1. **AWS Certificate Manager (ACM)** — Dieser Service richtet sich an Unternehmenskunden, die eine sichere Webpräsenz benötigen. TLS ACMZertifikate werden über Elastic Load Balancing, CloudFront, Amazon, Amazon API Gateway und andere [integrierte AWS Dienstleistungen](#). Die gebräuchlichste Anwendung dieser Art ist eine sichere öffentliche Website mit erheblichen Anforderungen an den Datenverkehr. ACMvereinfacht außerdem das Sicherheitsmanagement, indem die Verlängerung ablaufender Zertifikate automatisiert wird. Sie sind an der richtigen Stelle für diesen Service.
2. **AWS Private CA**—Dieser Service richtet sich an Unternehmenskunden, die eine Public-Key-Infrastruktur (PKI) innerhalb der AWS Cloud und für den privaten Gebrauch innerhalb einer Organisation vorgesehen. Mit AWS Private CA, können Sie Ihre eigene Zertifizierungsstellenhierarchie (CA) erstellen und damit Zertifikate für die Authentifizierung von Benutzern, Computern, Anwendungen, Diensten, Servern und anderen Geräten ausstellen. Zertifikate, die von einer privaten Zertifizierungsstelle ausgestellt wurden, können nicht im Internet verwendet werden. Weitere Informationen finden Sie hier: [AWS Private CA Benutzerleitfaden](#).

AWS Certificate Manager Zertifikate

ACM verwaltet öffentliche, private und importierte Zertifikate. Zertifikate werden verwendet, um eine sichere Kommunikation über das Internet oder innerhalb eines internen Netzwerks herzustellen. Sie können ein öffentlich vertrauenswürdigen Zertifikat direkt von ACM (ein „ACMZertifikat“) anfordern oder ein von einem Drittanbieter ausgestelltes öffentlich vertrauenswürdigen Zertifikat importieren. Selbstsignierte Zertifikate werden ebenfalls unterstützt. Um das interne Zertifikat Ihres Unternehmens bereitzustellen PKI, können Sie ACM Zertifikate ausstellen, die von einer privaten Zertifizierungsstelle (CA) signiert wurden, die von [AWS Private CA](#). Die CA kann sich entweder in Ihrem Konto befinden oder über ein anderes Konto mit Ihnen geteilt werden.

Note

Öffentliche ACM Zertifikate können auf EC2 Amazon-Instances installiert werden, die mit einer [Nitro Enclave](#) verbunden sind, aber nicht mit anderen EC2 Amazon-Instances. Informationen zum Einrichten eines eigenständigen Webservers auf einer EC2 Amazon-Instance, die nicht mit einer Nitro Enclave verbunden ist, finden [Sie unter Tutorial: Einen LAMP Webserver auf Amazon Linux 2 installieren oder Tutorial: Einen LAMP Webserver mit Amazon Linux installieren](#). AMI

Note

Da Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden, standardmäßig nicht vertrauenswürdig sind, müssen Administratoren sie in Clientvertrauensspeichern installieren.

Um mit der Ausstellung von Zertifikaten zu beginnen, melden Sie sich bei AWS Management Console und öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>. Wenn die Einführungsseite angezeigt wird, wählen Sie Get Started. Wählen Sie andernfalls CAs im linken Navigationsbereich Certificate Manager oder Private aus.

Themen

- [Für die Verwendung einrichten AWS Certificate Manager](#)
- [AWS Certificate Manager öffentliche Zertifikate](#)

- [Private Zertifikate in AWS Certificate Manager](#)
- [Importiert Zertifikate in AWS Certificate Manager](#)
- [Listet Zertifikate auf, die verwaltet werden von AWS Certificate Manager](#)
- [Anzeigen AWS Certificate Manager Details zum Zertifikat](#)
- [Löschen Sie Zertifikate, die verwaltet werden von AWS Certificate Manager](#)

Für die Verwendung einrichten AWS Certificate Manager

Mit AWS Certificate Manager (ACM) Sie können SSL/TLS Zertifikate für Ihre bereitstellen und verwalten AWS basierte Websites und Anwendungen. Sie verwenden ACM es, um ein Zertifikat zu erstellen oder zu importieren und anschließend zu verwalten. Sie müssen andere verwenden AWS Dienste zur Bereitstellung des Zertifikats auf Ihrer Website oder Anwendung. Weitere Informationen zu den integrierten Diensten finden Sie unter [In ACM integrierte Services](#). ACM In den folgenden Abschnitten werden die Schritte beschrieben, die Sie vor der Verwendung ausführen müssen ACM.

Themen

- [Melden Sie sich an für eine AWS-Konto](#)
- [Erstellen eines Benutzers mit Administratorzugriff](#)
- [Registrieren Sie einen Domainnamen für ACM](#)
- [\(Optional\) Konfigurieren Sie einen Datensatz CAA](#)

Melden Sie sich an für eine AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/die-Anmeldung>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontos wird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. Als bewährte

Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie sich Ihre Root-Benutzer des AWS-Kontos, aktivieren AWS IAM Identity Center, und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melde dich an bei [AWS Management Console](#) als Kontoinhaber wählen Sie Root-Benutzer und geben Sie Ihren AWS-Konto E-Mail-Adresse. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Als Root-Benutzer anmelden im AWS-Anmeldung Benutzerleitfaden](#).

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren Sie ein virtuelles MFA Gerät für AWS-Konto Root-Benutzer \(Konsole\)](#) im IAMBenutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) in der AWS IAM Identity Center Benutzerleitfaden.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Für ein Tutorial zur Verwendung des IAM-Identity-Center-Verzeichnis als Identitätsquelle finden [Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis](#) in der AWS IAM Identity Center Benutzerleitfaden.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, URL die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie unter [Anmelden bei AWS Zugriffsportal](#) im AWS-Anmeldung Benutzerleitfaden.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie unter [Einen Berechtigungssatz erstellen in](#) der AWS IAM Identity Center Benutzerleitfaden.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Anweisungen finden Sie unter [Gruppen hinzufügen](#) in der AWS IAM Identity Center Benutzerleitfaden.

Registrieren Sie einen Domainnamen für ACM

Ein vollqualifizierter Domainname (FQDN) ist der eindeutige Name einer Organisation oder Einzelperson im Internet, gefolgt von einer Top-Level-Domainendung wie .com oder .org. Wenn Sie noch keinen registrierten Domainnamen haben, können Sie einen über Amazon Route 53 oder Dutzende anderer kommerzieller Registrierstellen registrieren lassen. In der Regel besuchen Sie die Website des Anbieters und fordern einen Domainnamen an. Die Registrierung eines Domainnamens dauert in der Regel für einen bestimmten Zeitraum, z. B. ein oder zwei Jahre, bevor sie erneuert werden muss.

Weitere Informationen über die Registrierung von Domain-Namen mit Amazon Route 53 finden Sie unter [Registrierung von Domain-Namen mit Amazon Route 53](#) im Amazon Route 53 Developer Guide.

(Optional) Konfigurieren Sie einen Datensatz CAA

Ein CAA Datensatz gibt an, welche Zertifizierungsstellen (CAs) Zertifikate für eine Domain oder Subdomain ausstellen dürfen. Durch das Erstellen eines CAA Eintrags zur Verwendung ACM mit können Sie verhindern, dass falsche CAs Benutzer Zertifikate für Ihre Domains ausstellen. Ein CAA Datensatz ist kein Ersatz für die Sicherheitsanforderungen, die von Ihrer Zertifizierungsstelle festgelegt wurden, wie z. B. die Anforderung, zu bestätigen, dass Sie der Eigentümer einer Domain sind.

Nachdem Ihre Domain während der Zertifikatsanforderung ACM validiert wurde, prüft sie, ob ein CAA Datensatz vorhanden ist, um sicherzustellen, dass sie ein Zertifikat für Sie ausstellen kann. Die Konfiguration eines CAA Datensatzes ist optional.

Verwenden Sie die folgenden Werte, wenn Sie Ihren CAA Datensatz konfigurieren:

flags

Gibt an, ob der Wert des Tag-Felds von unterstützt wirdACM. Legen Sie diesen Wert auf 0 fest.

Tag

Das tag-Feld kann einen der folgenden Werte haben. Beachten Sie, dass das iodef-Feld derzeit ignoriert wird.

issue

Zeigt an, dass die ACM Zertifizierungsstelle, die Sie im Wertfeld angeben, berechtigt ist, ein Zertifikat für Ihre Domain oder Subdomain auszustellen.

issuewild

Zeigt an, dass die ACM Zertifizierungsstelle, die Sie im Wertfeld angegeben haben, berechtigt ist, ein Platzhalterzertifikat für Ihre Domain oder Subdomain auszustellen. Ein Platzhalterzertifikat gilt für die Domain oder Unterdomain und alle ihre Unterdomains.

Wert

Der Wert dieses Feldes hängt vom Wert des tag-Feldes ab. Sie müssen diesen Wert mit Anführungszeichen (") umschließen.

Wenn der tag-Wert issue lautet

Das value-Feld enthält den Domainnamen der Zertifizierungsstelle. Dieses Feld kann den Namen einer nicht mit Amazon assoziierten Zertifizierungsstelle enthalten. Wenn Sie jedoch

keinen CAA Datensatz haben, der einen der folgenden vier angibt CAs, ACM kann Amazon kein Zertifikat für Ihre Domain oder Subdomain ausstellen:

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

Das value-Feld kann auch ein Semikolon (;) enthalten, um anzugeben, dass keine Zertifizierungsstelle ein Zertifikat für Ihre Domain oder Unterdomain ausstellen darf. Verwenden Sie dieses Feld, wenn für eine bestimmte Domain keine Zertifikate mehr ausgestellt werden sollen.

Wenn der tag-Wert `issuewild` lautet

Das value-Feld ist mit dem Feld für den tag-Wert `issue` identisch, gilt jedoch für Platzhalterzertifikate.

Wenn ein `CAAIssueWild`-Datensatz vorhanden ist, der keinen ACM CA-Wert enthält, können keine Platzhalter von ausgegeben werden. ACM Wenn kein `IssueWild`-Objekt vorhanden ist, es aber einen `CAA Issue`-Datensatz für gibt ACM, können Platzhalter von ausgegeben werden. ACM

Example CAABeispiele für Datensätze

In den folgenden Beispielen steht Ihr Domainname an erster Stelle, gefolgt vom Datensatztyp (CAA). Das `flags`-Feld ist immer 0. Das `tags`-Feld kann `issue` oder `issuewild` lauten. Wenn das Feld `Problem` lautet und Sie den Domainnamen eines CA-Servers in das Wertfeld eingeben, gibt der CAA Datensatz an, dass der angegebene Server das angeforderte Zertifikat ausstellen darf. Wenn Sie ein Semikolon „;“ in das Wertfeld eingeben, gibt der CAA Datensatz an, dass keine Zertifizierungsstelle berechtigt ist, ein Zertifikat auszustellen. Die Konfiguration der CAA Datensätze variiert je nach Anbieter. DNS

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

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

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

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

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

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

Weitere Informationen zum Hinzufügen oder Ändern von DNS Datensätzen erhalten Sie bei Ihrem DNS Anbieter. Route 53 unterstützt CAA Datensätze. Wenn Route 53 Ihr DNS Anbieter ist, finden Sie unter [CAAFormat](#) weitere Informationen zum Erstellen eines Datensatzes.

AWS Certificate Manager öffentliche Zertifikate

Nachdem Sie ein öffentliches Zertifikat angefordert haben, müssen Sie den Domainbesitz überprüfen, wie unter beschrieben [Bestätigen Sie den Domainbesitz für AWS Certificate Manager öffentliche Zertifikate](#).

Öffentliche ACM Zertifikate entsprechen dem X.509-Standard und unterliegen den folgenden Einschränkungen:

- **Namen:** Sie müssen DNS -konforme Betreffnamen verwenden. Weitere Informationen finden Sie unter [Domainnamen](#).
- **Algorithmus:** Für die Verschlüsselung muss der Algorithmus für den privaten Schlüssel des Zertifikats entweder 2048-BitRSA, ECDSA 256-Bit oder 384-Bit sein. ECDSA
- **Gültigkeitsdauer:** Jedes Zertifikat ist 13 Monate (395 Tage) gültig.
- **Verlängerung:** ACM versucht, ein privates Zertifikat automatisch nach 11 Monaten zu erneuern.

Administratoren können mithilfe von [Richtlinien für ACM bedingte Schlüssel](#) steuern, wie Endbenutzer neue Zertifikate ausstellen. Diese Bedingungsschlüssel ermöglichen es, Einschränkungen für Domains, Validierungsmethoden und andere Attribute im Zusammenhang mit einer Zertifikatsanfrage

festzulegen. Wenn beim Anfordern eines Zertifikats Probleme auftreten, finden Sie weitere Informationen unter [Problembehandlung bei Zertifikatsanfragen](#).

Um ein Zertifikat für eine private PKI Nutzung anzufordern AWS Private CA, finden Sie unter [Fordern Sie ein privates Zertifikat an in AWS Certificate Manager](#).

AWS Certificate Manager Merkmale und Einschränkungen eines öffentlichen Zertifikats

Öffentliche Zertifikate, die von bereitgestellt werden, ACM weisen die Merkmale und Einschränkungen auf, die in diesem Abschnitt beschrieben sind. Diese Merkmale gelten nur für Zertifikate, die von bereitgestellt wurden ACM. Sie gelten möglicherweise nicht für [importierte Zertifikate](#).

Browser- und Anwendungs-Vertrauensstellung

ACMZertifikate werden von allen gängigen Browsern als vertrauenswürdig eingestuft, darunter Google Chrome, Microsoft Internet Explorer und Microsoft Edge, Mozilla Firefox und Apple Safari. Browser, die ACM Zertifikaten vertrauen, zeigen in ihrer Status- oder Adressleiste ein Schlosssymbol an, wenn sie über SSL/mit Websites TLS verbunden sind, die ACM Zertifikate verwenden. ACMZertifikate werden auch von Java als vertrauenswürdig eingestuft.

Zertifizierungsstelle und Hierarchie

Öffentliche Zertifikate, über die Sie anfordern, erhalten ACM Sie von [Amazon Trust Services](#), einer von Amazon verwalteten öffentlichen [Zertifizierungsstelle \(CA\)](#). Amazon Root CAs 1 bis 4 sind von einem älteren Root namens Starfield G2 Root Certificate Authority — G2 quersigniert. Der Starfield-Stamm wird auf Android-Geräten ab späteren Versionen von Gingerbread und von iOS ab Version 4.1 als vertrauenswürdig eingestuft. Amazon-Stämme werden von iOS ab Version 11 als vertrauenswürdig eingestuft. Jeder Browser, jede Anwendung oder jedes Betriebssystem, das Amazon- oder Starfield-Roots enthält, vertraut öffentlichen Zertifikaten, die von ACM bezogen wurden.

Die Leaf - oder ACMEntity-Zertifikate, die an Kunden ausgestellt werden, beziehen ihre Autorität von einer Amazon Trust Services-Stammzertifizierungsstelle über eine von mehreren Zwischeninstanzen. CAs ACMweist anhand des Typs des angeforderten Zertifikats (RSAoderECDSA) nach dem Zufallsprinzip eine Zwischenzertifizierungsstelle zu. Da die Zwischenzertifizierungsstelle nach dem Zufallsprinzip ausgewählt wird, ACM stellt sie keine Informationen zur Zwischenzertifizierungsstelle bereit.

Domaininvalidierung (DV)

ACM-Zertifikate werden von der Domäne validiert. Das heißt, das Betreff-Feld eines ACM Zertifikats identifiziert einen Domainnamen und nichts weiter. Wenn Sie ein ACM Zertifikat anfordern, müssen Sie bestätigen, dass Sie Eigentümer aller Domänen sind oder die Kontrolle über alle Domänen haben, die Sie in Ihrer Anfrage angeben. Sie können die Inhaberschaft per E-Mail oder per E-Mail bestätigen DNS. Weitere Informationen erhalten Sie unter [AWS Certificate Manager E-Mail-Validierung](#) und [AWS Certificate Manager DNSValidierung](#).

Zwischen- und Stamm-CA-Rotation

Um eine robuste und flexible Zertifikatsinfrastruktur aufrechtzuerhalten, kann Amazon jederzeit ohne Vorankündigung eine zwischengeschaltete Zertifizierungsstelle einstellen. Änderungen dieser Art haben keine Auswirkungen auf die Kunden. Weitere Informationen finden Sie im Blog-Beitrag [Amazon introduces dynamic intermediate certificate authorities](#) (Amazon führt dynamische Zwischenzertifizierungsstellen ein).

In dem unwahrscheinlichen Fall, dass Amazon eine Stammzertifizierungsstelle einstellt, erfolgt die Änderung so schnell, wie es die Umstände erfordern. Aufgrund der großen Auswirkungen einer solchen Änderung wird Amazon alle verfügbaren Mechanismen nutzen, um zu benachrichtigen AWS Kunden, einschließlich AWS Health Dashboard, E-Mail an Kontoinhaber und Kontaktaufnahme mit technischen Kundenbetreuern.

Firewall-Zugriff für Widerruf

Wenn ein Endentitätszertifikat nicht mehr vertrauenswürdig ist, wird es gesperrt. OCSP und CRLs sind die Standardmechanismen, mit denen überprüft wird, ob ein Zertifikat gesperrt wurde oder nicht. OCSP und CRLs sind die Standardmechanismen, die zur Veröffentlichung von Sperrinformationen verwendet werden. Einige Kunden-Firewalls benötigen möglicherweise zusätzliche Regeln, damit diese Mechanismen funktionieren können.

Das folgende Beispiel mit URL Platzhaltermustern kann verwendet werden, um den Sperrverkehr zu identifizieren. Ein Sternchen-Platzhalter (*) steht für ein Zeichen oder eine beliebige Kombination von mehreren alphanumerischen Zeichen, ein Fragezeichen (?) steht für ein einzelnes alphanumerisches Zeichen, und ein Rautenzeichen (#) steht für eine Zahl.

- OCSP

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

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

- CRL

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

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

Wichtige Algorithmen

Ein Zertifikat muss einen Algorithmus und eine Schlüsselgröße angeben. Derzeit werden die folgenden Public-Key-Algorithmen RSA und der Elliptic Curve Digital Signature Algorithm (ECDSA) von ACM unterstützt. ACM kann mithilfe von Algorithmen, die mit einem Sternchen (*) gekennzeichnet sind, die Ausstellung neuer Zertifikate beantragen. Die übrigen Algorithmen werden nur für [importierte](#) Zertifikate unterstützt.

Note

Wenn Sie ein privates PKI Zertifikat anfordern, das von einer Zertifizierungsstelle signiert wurde AWS Private CA, muss die angegebene Signaturalgorithmusfamilie (RSA oder ECDSA) mit der Algorithmusfamilie des geheimen Schlüssels der Zertifizierungsstelle übereinstimmen.

- 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-Schlüssel sind kleiner und bieten eine Sicherheit, die mit RSA-Schlüsseln vergleichbar ist, bieten jedoch eine höhere Recheneffizienz. ECDSA wird jedoch nicht von allen Netzwerkclients unterstützt. Die folgende Tabelle, adaptiert von [NIST](#), zeigt die repräsentative Sicherheitsstärke von RSA und ECDSA mit Schlüsseln unterschiedlicher Größe. Alle Werte sind in Bits angegeben.

Vergleich der Sicherheit von Algorithmen und Schlüsseln

Stärke der Sicherheit	RSASchlüsselgröße	ECDSASchlüsselgröße
128	3072	256

Stärke der Sicherheit	RSASchlüsselgröße	ECDSASchlüsselgröße
192	7680	384
256	15360	521

Die Sicherheitsstärke, verstanden als Potenz von 2, bezieht sich auf die Anzahl der Rateversuche, die erforderlich sind, um die Verschlüsselung zu knacken. Beispielsweise können sowohl ein RSA 3072-Bit-Schlüssel als auch ein ECDSA 256-Bit-Schlüssel abgerufen werden, ohne dass mehr als 2¹²⁸ Versuche erforderlich sind.

Informationen, die Ihnen bei der Auswahl eines Algorithmus helfen, finden Sie in der AWS Blogbeitrag [Wie bewertet und verwendet man ECDSA Zertifikate in AWS Certificate Manager](#).

Important

Beachten Sie, dass [integrierte Services](#) nur die von ihnen unterstützten Algorithmen und Schlüsselgrößen für die Zuordnung zu ihren Ressourcen zulassen. Darüber hinaus unterscheidet sich ihre Unterstützung je nachdem, ob das Zertifikat in IAM oder in importiert wird ACM. Weitere Informationen finden Sie in der Dokumentation zu dem jeweiligen Service.

- Informationen zu Elastic Load Balancing finden Sie unter [HTTPSListener für Ihren Application Load Balancer](#).
- Weitere Informationen finden Sie unter [Unterstützte TLS Protokolle SSL und Chiffren](#). CloudFront

Verwaltete Erneuerung und Bereitstellung

ACM verwaltet den Prozess der Erneuerung von ACM Zertifikaten und der Bereitstellung der Zertifikate nach deren Verlängerung. Eine automatische Erneuerung kann Ihnen dabei helfen, Ausfallzeiten aufgrund von falsch konfigurierten, widerrufenen oder abgelaufenen Zertifikaten zu verhindern. Weitere Informationen finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

Mehrere Domainnamen

Jedes ACM Zertifikat muss mindestens einen vollqualifizierten Domainnamen (FQDN) enthalten, und Sie können bei Bedarf weitere Namen hinzufügen. Wenn Sie beispielsweise

ein ACM Zertifikat für erstellen `www.example.com`, können Sie auch den Namen hinzufügen, `www.example.net` falls Kunden Ihre Website über einen der beiden Namen erreichen können. Dies gilt auch für "Bare"-Domains (auch bekannt als "Zone Apex"- oder "Naked"-Domains). Das heißt, Sie können ein ACM Zertifikat für `www.example.com` anfordern und den Namen `example.com` hinzufügen. Weitere Informationen finden Sie unter [AWS Certificate Manager öffentliche Zertifikate](#).

Punycode

Die folgenden [Punycode](#)-Anforderungen in Bezug auf [internationalisierte Domainnamen](#) müssen erfüllt sein:

1. Domainnamen, die mit dem Muster „<character><character>--“ beginnen, müssen mit „xn--“ übereinstimmen.
2. Domainnamen, die mit „xn--“ beginnen, müssen ebenfalls gültige internationalisierte Domainnamen sein.

Beispiele für Punycode

Domainname	Erfüllt #1	Erfüllt #2	Zuläss	Hinweis
<code>example.com</code>	–	–	✓	Beginnt nicht mit „<character><character>--“
<code>a--example.com</code>	–	–	✓	Beginnt nicht mit „<character><character>--“
<code>abc--example.com</code>	–	–	✓	Beginnt nicht mit „<character><character>--“
<code>xn--xyz.com</code>	Ja	Ja	✓	Gültiger internationalisierter Domainname (wird zu 简.com aufgelöst)
<code>xn--example.com</code>	Ja	Nein	✗	Kein gültiger internationalisierter Domainname
<code>ab--example.com</code>	Nein	Nein	✗	Muss mit „xn--“ beginnen

Gültigkeitszeitraum

Die Gültigkeitsdauer für ACM Zertifikate beträgt 13 Monate (395 Tage).

Platzhalternamen

ACM ermöglicht es Ihnen, ein Sternchen (*) im Domainnamen zu verwenden, um ein ACM Zertifikat zu erstellen, das einen Platzhalternamen enthält, der mehrere Websites in derselben Domain schützen kann. Zum Beispiel schützt *.example.com www.example.com und images.example.com.

Note

Wenn Sie ein Platzhalter-Zertifikat anfordern, muss sich das Sternchen (*) ganz links im Domainnamen befinden und es kann nur eine Subdomainn-Ebene geschützt werden. Zum Beispiel kann *.example.com login.example.com und test.example.com schützen, jedoch nicht test.login.example.com. Beachten Sie außerdem, dass *.example.com nur die Subdomains von example.com schützt, jedoch nicht die "Bare-" oder "Apex"-Domain (example.com). Sie können jedoch ein Zertifikat anfordern, das eine "Bare"- oder "Apex"-Domain und deren Subdomains schützt, indem Sie mehrere Domainnamen in Ihrer Anforderung angeben. Beispielsweise können Sie ein Zertifikat anfordern, das example.com und *.example.com schützt.

Einschränkungen

Die folgenden Einschränkungen gelten für öffentliche Zertifikate.

- ACM stellt keine EV-Zertifikate (Extended Validation) oder OV-Zertifikate (Organization Validation) zur Verfügung.
- ACM stellt keine Zertifikate für etwas anderes als die SSL TLS /-Protokolle zur Verfügung.
- Sie können keine ACM Zertifikate für die E-Mail-Verschlüsselung verwenden.
- ACM ermöglicht es Ihnen derzeit nicht, die [verwaltete Zertifikatserneuerung](#) für ACM Zertifikate zu deaktivieren. Außerdem ist die verwaltete Verlängerung für Zertifikate, in die Sie importieren, nicht verfügbar ACM.
- Sie können keine Zertifikate für Amazon-eigene Domainnamen, wie solche, die mit amazonaws.com, cloudfront.net oder elasticbeanstalk.com enden, anfordern.
- Sie können den privaten Schlüssel für ein ACM Zertifikat nicht herunterladen.

- Sie können ACM Zertifikate nicht direkt auf Ihrer Amazon Elastic Compute Cloud (AmazonEC2) -Website oder -Anwendung installieren. Sie können jedoch Ihr Zertifikat mit einem integrierten Service verwenden. Weitere Informationen finden Sie unter [In ACM integrierte Services](#).
- Öffentlich vertrauenswürdige ACM Zertifikate werden automatisch in mindestens zwei Zertifikatstransparenzdatenbanken aufgezeichnet, es sei denn, Sie entscheiden sich dafür, sich abzumelden. Sie können die Konsole derzeit nicht zum Abmelden verwenden. Sie müssen das verwenden AWS CLI oder das ACM API. Weitere Informationen finden Sie unter [Abmelden von der Protokollierung für Zertifikatstransparenz](#). Allgemeine Informationen zu Transparenzprotokollen finden Sie unter [Protokollierung der Zertifikatstransparenz](#).

Fordern Sie ein öffentliches Zertifikat an in AWS Certificate Manager

In den folgenden Abschnitten wird beschrieben, wie Sie die ACM Konsole verwenden oder AWS CLI um ein öffentliches ACM Zertifikat anzufordern.

Themen

- [Anfordern eines öffentlichen Zertifikats mithilfe der Konsole](#)
- [Fordern Sie ein öffentliches Zertifikat an, indem Sie CLI](#)

Anfordern eines öffentlichen Zertifikats mithilfe der Konsole

Um ein ACM öffentliches Zertifikat anzufordern (Konsole)

1. Melden Sie sich an bei AWS Management Console und öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>.

Wählen Sie Request a certificate aus.

2. Geben Sie auf der Seite Domain names (Domainnamen) Ihren Domainnamen ein.

Sie können einen vollqualifizierten Domänennamen (FQDN), z. B. **www.example.com**, oder einen bloßen Domainnamen oder einen Apex-Domänennamen wie **example.com** verwenden. Sie können auch ein Sternchen (*) als Platzhalter in der Position ganz links verwenden, um mehrere Webseitenamen in derselben Domain zu schützen. Zum Beispiel schützt ***.example.com corp.example.com** und **images.example.com**. Der Platzhaltername wird im Feld Betreff und in der Erweiterung „Alternativer Betreffname“ des Zertifikats angezeigt. ACM

Wenn Sie ein Platzhalterzertifikat anfordern, muss sich das Sternchen (*) ganz links im Domainnamen befinden und es kann nur eine Subdomainebene geschützt werden. Zum Beispiel kann ***.example.com** **login.example.com** und **test.example.com** schützen, jedoch nicht **test.login.example.com**. Beachten Sie außerdem, dass ***.example.com** nur die Subdomains von **example.com** schützt, jedoch nicht die "Bare-" oder "Apex"-Domain (**example.com**). Um beide zu schützen, sehen Sie sich den nächsten Schritt an.

 Note

Gemäß [RFC5280](#) darf die Länge des Domainnamens (technisch gesehen der allgemeine Name), den Sie in diesem Schritt eingeben, 64 Byte (Zeichen), einschließlich Punkte, nicht überschreiten. Jeder nachfolgende alternative Betreffname (SAN), den Sie wie im nächsten Schritt angeben, kann bis zu 253 Pfund lang sein.

Um einen anderen Namen hinzuzufügen, wählen Sie Add another name to this certificate (Diesem Zertifikat einen anderen Namen hinzufügen) aus und geben Sie den Namen in das Textfeld ein. Dies ist nützlich für den Schutz einer "Bare"- oder "Apex"-Domain (wie **example.com**) und ihrer Subdomains (wie ***.example.com**).

3. Wählen Sie im Abschnitt Validierungsmethode je nach Ihren Anforderungen entweder DNSValidierung — empfohlen oder E-Mail-Validierung aus.

 Note

Wenn Sie Ihre DNS Konfiguration bearbeiten können, empfehlen wir Ihnen, die DNS Domain-Validierung anstelle der E-Mail-Validierung zu verwenden. DNSDie Validierung hat mehrere Vorteile gegenüber der E-Mail-Validierung. Siehe [AWS Certificate Manager DNSValidierung](#).

Bevor ein ACM Zertifikat ausgestellt wird, wird bestätigt, dass Sie der Eigentümer oder die Kontrolle über die Domainnamen in Ihrer Zertifikatsanfrage haben. Sie können entweder die E-Mail-Validierung oder DNS die Validierung verwenden.

Wenn Sie sich für die E-Mail-Validierung entscheiden, wird eine Bestätigungs-E-Mail an die Domain ACM gesendet, die Sie im Feld Domainname angegeben haben. Wenn Sie eine Validierungsdomäne angeben, wird die E-Mail stattdessen an diese Validierungsdomäne

ACM gesendet. Weitere Informationen zur E-Mail-Validierung finden Sie unter [AWS Certificate Manager E-Mail-Validierung](#).

Wenn Sie die DNS Validierung verwenden, fügen Sie Ihrer DNS Konfiguration einfach einen von bereitgestellten CNAME Datensatz ACM hinzu. Weitere Informationen zur DNS Validierung finden Sie unter [AWS Certificate Manager DNSValidierung](#).

4. Wählen Sie im Abschnitt Schlüsselalgorithmus einen Algorithmus aus.
5. Auf der Seite Tags können Sie Ihr Zertifikat optional mit Tags versehen. Tags sind Schlüssel-Wert-Paare, die als Metadaten zur Identifizierung und Organisation dienen AWS Ressourcen schätzen. Eine Liste der ACM Tag-Parameter und Anweisungen zum Hinzufügen von Tags zu Zertifikaten nach der Erstellung finden Sie unter [Markierung AWS Certificate Manager Ressourcen](#)

Wenn Sie mit dem Hinzufügen von Tags fertig sind, wählen Sie Request (Anfordern) aus.

6. Nach der Bearbeitung der Anforderung kehrt die Konsole zu Ihrer Zertifikatsliste zurück, wo Informationen über das neue Zertifikat angezeigt werden.

Ein Zertifikat gibt den Status Pending validation auf Anfrage aus, es sei denn, es schlägt aus einem der im Thema zur Problembehandlung [Certificate request fails](#) genannten Gründen fehl. ACM unternimmt 72 Stunden lang wiederholte Versuche, ein Zertifikat zu validieren, woraufhin das Zeitlimit überschritten wird. Wenn ein Zertifikat den Status Fehlgeschlagen oder das Timeout bei der Validierung anzeigt, löschen Sie die Anfrage, korrigieren Sie das Problem mit der [DNSValidierung](#) oder [E-Mail-Validierung](#) und versuchen Sie es erneut. Wenn die Validierung erfolgreich ist, gibt das Zertifikat den Status Issued aus.

Note

Je nachdem, wie Sie die Liste geordnet haben, kann es sein, dass ein gesuchtes Zertifikat nicht sofort sichtbar ist. Klicken Sie rechts auf das schwarze Dreieck, um die Reihenfolge zu ändern. Sie können auch mithilfe der Seitenzahlen oben rechts durch mehrere Seiten von Zertifikaten navigieren.

Fordern Sie ein öffentliches Zertifikat an, indem Sie CLI

Verwenden Sie den Befehl [request-certificate](#), um ein neues öffentliches ACM Zertifikat in der Befehlszeile anzufordern. Optionale Werte für die Validierungsmethode sind DNS und EMAIL

Optionale Werte für den Schlüsselalgorithmus sind RSA_2048 (die Standardeinstellung, wenn der Parameter nicht explizit angegeben wird), EC_Prime256V1 und EC_SECP384R1.

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

Dieser Befehl gibt den Amazon-Ressourcennamen (ARN) Ihres neuen öffentlichen Zertifikats aus.

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

Bestätigen Sie den Domainbesitz für AWS Certificate Manager öffentliche Zertifikate

Bevor die Amazon-Zertifizierungsstelle (CA) ein Zertifikat für Ihre Site ausstellen kann, AWS Certificate Manager (ACM) muss nachweisen, dass Sie Eigentümer aller Domainnamen sind oder die Kontrolle über alle Domainnamen haben, die Sie in Ihrer Anfrage angeben. Sie können wählen, ob Sie Ihr Eigentum entweder mit der Validierung des Domain Name Systems (DNS) oder mit einer E-Mail-Bestätigung nachweisen möchten, wenn Sie ein Zertifikat anfordern.

Note

Die Validierung gilt nur für öffentlich vertrauenswürdige Zertifikate, ausgestellt von ACM. ACM validiert nicht den Domainbesitz für [importierte Zertifikate](#) oder für Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden. ACM kann Ressourcen in einer VPC [privaten gehosteten Amazon-Zone](#) oder einer anderen privaten Domain nicht validieren. Weitere Informationen finden Sie unter [Fehlerbehebung bei der Zertifikatsvalidierung](#).

Im Allgemeinen empfehlen wir aus den folgenden Gründen, die Validierung der E-Mail-Validierung vorzuziehen:

- Wenn Sie Amazon Route 53 zur Verwaltung Ihrer öffentlichen DNS Aufzeichnungen verwenden, können Sie Ihre Aufzeichnungen ACM direkt aktualisieren.

- ACM erneuert automatisch DNS validierte Zertifikate, solange ein Zertifikat verwendet wird und der DNS Datensatz vorhanden ist.
- Für die Erneuerung benötigen E-Mail-validierte Zertifikate eine Aktion des Domainbesitzers. ACM beginnt 45 Tage vor Ablauf mit dem Versand von Verlängerungsmitteilungen. Diese Benachrichtigungen gehen an eine oder mehrere der fünf allgemeinen Administratoradressen der Domain. Die Benachrichtigungen enthalten einen Link, auf den der Domaininhaber zur einfachen Erneuerung klicken kann. Sobald alle aufgelisteten Domänen validiert sind ACM, wird ein erneuertes Zertifikat mit demselben ausgestelltARN.

Wenn Sie nicht autorisiert sind, die DNS Datenbank Ihrer Domain zu bearbeiten, müssen Sie stattdessen die [E-Mail-Validierung](#) verwenden.

Note

Nachdem Sie ein Zertifikat mit E-Mail-Validierung erstellt haben, können Sie nicht zur Validierung mit DNS wechseln. Um die DNS Validierung zu verwenden, löschen Sie das Zertifikat und erstellen Sie dann ein neues Zertifikat, das DNS Validierung verwendet.

Themen

- [AWS Certificate Manager DNSValidierung](#)
- [AWS Certificate Manager E-Mail-Validierung](#)

AWS Certificate Manager DNSValidierung

Das Domain Name System (DNS) ist ein Verzeichnisdienst für Ressourcen, die mit einem Netzwerk verbunden sind. Ihr DNS Anbieter unterhält eine Datenbank mit Datensätzen, die Ihre Domain definieren. Wenn Sie sich für die DNS Validierung entscheiden, werden Ihnen ein oder mehrere CNAME Datensätze zur ACM Verfügung gestellt, die zu dieser Datenbank hinzugefügt werden müssen. Diese Datensätze enthalten ein eindeutiges Schlüssel-Wert-Paar, das als Nachweis dient, dass Sie die Domain steuern.

 Note

Nachdem Sie ein Zertifikat mit E-Mail-Validierung erstellt haben, können Sie nicht zur Validierung mit DNS wechseln. Um die DNS Validierung zu verwenden, löschen Sie das Zertifikat und erstellen Sie dann ein neues Zertifikat, das DNS Validierung verwendet.

Wenn Sie beispielsweise ein Zertifikat für die `example.com` Domain mit `www.example.com` einem zusätzlichen Namen anfordern, werden zwei CNAME Datensätze für Sie ACM erstellt. Jeder speziell für Ihre Domain und Ihr Konto erstellte Datensatz enthält einen Namen und einen Wert. Der Wert ist ein Alias, der auf einen verweist AWS Domain, die zur automatischen Verlängerung Ihres Zertifikats ACM verwendet wird. Die CNAME Datensätze dürfen Ihrer DNS Datenbank nur einmal hinzugefügt werden. ACM erneuert Ihr Zertifikat automatisch, solange das Zertifikat verwendet wird und Ihr CNAME Datensatz erhalten bleibt.

 Important

Wenn Sie Amazon Route 53 nicht zur Verwaltung Ihrer öffentlichen DNS Aufzeichnungen verwenden, wenden Sie sich an Ihren DNS Anbieter, um zu erfahren, wie Sie Datensätze hinzufügen können. Wenn Sie nicht befugt sind, die DNS Datenbank Ihrer Domain zu bearbeiten, müssen Sie stattdessen die [E-Mail-Validierung](#) verwenden.

Ohne die Überprüfung wiederholen zu müssen, können Sie zusätzliche ACM Zertifikate für Ihren vollqualifizierten Domainnamen (FQDN) anfordern, solange der CNAME Datensatz gültig ist. Das heißt, Sie können Ersatzzertifikate mit demselben Domainnamen oder Zertifikate erstellen, die verschiedene Subdomains abdecken. Da das CNAME Validierungstoken für alle funktioniert AWS Region: Sie können dasselbe Zertifikat in mehreren Regionen neu erstellen. Sie können auch ein gelöscht Zertifikat ersetzen.

Sie können die automatische Verlängerung entweder beenden, indem Sie das Zertifikat aus dem AWS Dienst, mit dem es verknüpft ist, oder durch Löschen des CNAME Datensatzes. Wenn Route 53 nicht Ihr DNS Anbieter ist, wenden Sie sich an Ihren Anbieter, um zu erfahren, wie Sie einen Datensatz löschen können. Wenn Route 53 Ihr Anbieter ist, finden Sie weitere Informationen unter [Löschen von Ressourcendatensätzen](#) im Route 53 Entwicklerhandbuch aus. Weitere Informationen über die verwaltete Zertifikatverlängerung finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

Note

CNAME Die Auflösung schlägt fehl, wenn in Ihrer DNS Konfiguration mehr als fünf miteinander verkettete CNAMEs sind. Wenn Sie eine längere Verkettung benötigen, empfehlen wir [E-Mail-Validierung](#).

Wie CNAME funktionieren Aufzeichnungen ACM

Note

Dieser Abschnitt richtet sich an Kunden, die Route 53 nicht als DNS Anbieter verwenden.

Wenn Sie Route 53 nicht als Ihren DNS Anbieter verwenden, müssen Sie die von bereitgestellten CNAME Datensätze manuell ACM in die Datenbank Ihres Anbieters eingeben, normalerweise über eine Website. CNAME Datensätze werden für eine Reihe von Zwecken verwendet, unter anderem als Umleitungsmechanismen und als Container für herstellerepezifische Metadaten. Denn ACM diese Aufzeichnungen ermöglichen die anfängliche Überprüfung des Domainbesitzes und die fortlaufende automatische Verlängerung von Zertifikaten.

Die folgende Tabelle zeigt CNAME Beispieldatensätze für sechs Domainnamen. Jeder Datensatzname-Datensatzwert-Paar dient dazu, den Besitz von Domainnamen zu authentifizieren.

Beachten Sie in der Tabelle, dass die ersten beiden Datensatzname-Datensatzwert Paare sind gleich. Dies zeigt, dass für eine Platzhalterdomäne, wie z. B. *.example.com, die von erstellten Zeichenfolgen dieselben ACM sind wie für die Basisdomäne. example.com. Andernfalls wird das gekoppelte Datensatzname und Datensatzwert unterscheiden sich für jeden Domainnamen.

Beispieldatensätze CNAME

Domainname	Datensatzname	Datensatzwert	Kommentar
*.example.com	_ x1 .example.com.	_ x2 .acm-vali dierungen.aws.	Identisch
example.com	_ x1 .example.com.	_ x2 .acm-vali dierungen.aws.	

Domainname	Datensatzname	Datensatzwert	Kommentar
www.example.com	<u>_x3</u> .www.example.com.	<u>_x4</u> .acm-validation.aws.	Unique
host.example.com	<u>_x5</u> .host.example.com.	<u>_x6</u> .acm-validation.aws.	Unique
subdomain.example.com	<u>_x7</u> .subdomain.example.com.	<u>_x8</u> .acm-validation.aws.	Unique
host.subdomain.example.com	<u>_x9</u> .host.subdomain.example.com.	<u>_x10</u> .acm-validation.aws.	Unique

Das Tool *xN* Werte, die auf den Unterstrich () folgen, sind lange Zeichenketten, die von generiert wurden. ACM Zum Beispiel

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

ist repräsentativ für eine resultierende Datensatznameaus. Der zugeordnete Datensatzwert könnte

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

für denselben DNS Datensatz.

Note

Wenn Ihr DNS Anbieter CNAME Werte mit einem führenden Unterstrich nicht unterstützt, finden Sie weitere Informationen unter [Behebung von DNS Validierungsproblemen](#).

Wenn Sie ein Zertifikat anfordern und die DNS Validierung angeben, ACM stellt CNAME Informationen im folgenden Format bereit:

Domainname	Datensatzname	Datensatztyp	Datensatzwert
example.com	_a79865eb4cd1a6ab990a45779b4e0b96.beispiel.com.	CNAME	_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.

Der Domänenname ist dem Zertifikat FQDN zugeordnet. Datensatzname identifiziert den Datensatz eindeutig und dient als Schlüssel des Schlüssel-Wert-Paares. Datensatzwert dient als Wert des Schlüssel-Wert-Paares.

Alle drei Werte (Domainname, Datensatzname und Datensatzwert) müssen in die entsprechenden Felder der Weboberfläche Ihres DNS Anbieters eingegeben werden, um DNS Datensätze hinzuzufügen. Anbieter sind inkonsistent in der Verarbeitung des Datensatznamens (oder nur „Name“) Feld. In einigen Fällen wird erwartet, dass Sie die gesamte Zeichenfolge bereitstellen, wie oben gezeigt. Andere Anbieter hängen den Domainnamen automatisch an die von Ihnen eingegebene Zeichenfolge an. Dies bedeutet (in diesem Beispiel), dass Sie nur

```
_a79865eb4cd1a6ab990a45779b4e0b96
```

in das Namensfeld ein. Wenn Sie dies falsch erraten und einen Datensatznamen eingeben, der einen Domainnamen enthält (z. B. *.example.com*), können Sie Folgendes erhalten:

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

Die Validierung schlägt in diesem Fall fehl. Daher sollten Sie versuchen, im Voraus zu bestimmen, welche Art von Eingabe Ihr Provider erwartet.

Validierung einrichten DNS

In diesem Abschnitt wird beschrieben, wie Sie ein öffentliches Zertifikat für die DNS Validierung konfigurieren.

Um die DNS Validierung in der Konsole einzurichten

Note

Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits mindestens ein Zertifikat erstellt haben und dass Sie im AWS Region, in der Sie es erstellt haben. Wenn Sie

versuchen, die Konsole zu öffnen und stattdessen der Bildschirm „Erste Verwendung“ angezeigt wird, oder wenn Sie die Konsole erfolgreich öffnen und Ihr Zertifikat nicht in der Liste angezeigt wird, vergewissern Sie sich, dass Sie die richtige Region angegeben haben.

1. Öffnen Sie die ACM Konsole unter <https://console.aws.amazon.com/acm/>
2. Wählen Sie in der Liste der Zertifikate die Zertifikat-ID eines Zertifikats mit dem Status Pending validation (Validierung ausstehend) aus, das Sie konfigurieren möchten. Daraufhin wird eine Detailseite für das Zertifikat geöffnet.
3. Führen Sie im Abschnitt Domains eines der beiden folgenden Verfahren durch:
 - a. (Optional) Validieren Sie mit Route 53.

Die aktive Schaltfläche Create record in Route 53 (Einträge in Route 53 erstellen) wird angezeigt, wenn die folgenden Bedingungen zutreffen:

- Sie verwenden Route 53 als Ihren DNS Anbieter.
- Sie haben die Berechtigung, in die von Route 53 gehostete Zone zu schreiben.
- Ihr FQDN wurde noch nicht validiert.

 Note

Wenn die Schaltfläche Datensätze in Route 53 erstellen in Route 53 deaktiviert ist oder fehlt, lesen Sie [ACM in der Konsole wird die Schaltfläche „Datensätze in Route 53 erstellen“ nicht angezeigt](#).

Wählen Sie die Schaltfläche Create records in Route 53 (Einträge in Route 53 erstellen) und dann Create records (Einträge erstellen) aus. Die Seite mit dem Status des Zertifikats sollte mit einem Statusbanner geöffnet werden, in dem die Meldung Erfolgreich erstellte DNS Datensätze angezeigt wird.

Ihr neues Zertifikat kann noch bis zu 30 Minuten lang den Status Pending validation (Validierung ausstehend) anzeigen.

 Tip

Sie können nicht programmgesteuert anfordern, dass Ihr Datensatz in Route 53 ACM automatisch erstellt wird. Sie können jedoch eine erstellen AWS CLI oder API rufen Sie Route 53 auf, um den Datensatz in der Route DNS 53-Datenbank zu erstellen. Weitere Informationen über Route 53-Datensätze finden Sie unter [Arbeiten mit Ressourcendatensätzen](#).

- b. (Optional) Wenn Sie Route 53 nicht als Ihren DNS Anbieter verwenden, müssen Sie die CNAME Informationen abrufen und zu Ihrer DNS Datenbank hinzufügen. Auf der Detailseite für das neue Zertifikat stehen Ihnen zwei Optionen zur Verfügung:
- Kopieren Sie die im Abschnitt Domains angezeigten CNAME Komponenten. Diese Informationen müssen manuell zu Ihrer DNS Datenbank hinzugefügt werden.
 - Wählen Sie alternativ Exportieren nach CSV. Die Informationen in der resultierenden Datei müssen manuell zu Ihrer DNS Datenbank hinzugefügt werden.

 Important

Um Validierungsprobleme zu vermeiden, überprüfen Sie diese, [Wie CNAME funktionieren Aufzeichnungen ACM](#) bevor Sie Informationen zur Datenbank Ihres DNS Anbieters hinzufügen. Bei Problemen finden Sie weitere Informationen unter [Beheben Sie DNS Validierungsprobleme](#).

Wenn ACM der Domainname nicht innerhalb von 72 Stunden nach der Generierung eines CNAME Werts für Sie validiert werden kann, ACM ändern Sie den Zertifikatsstatus in „Timeout bei Validierung“. Der wahrscheinlichste Grund für dieses Ergebnis ist, dass Sie Ihre DNS Konfiguration nicht erfolgreich mit dem ACM generierten Wert aktualisiert haben. Um dieses Problem zu beheben, müssen Sie ein neues Zertifikat anfordern, nachdem Sie die CNAME Anweisungen gelesen haben.

AWS Certificate Manager E-Mail-Validierung

Bevor die Amazon-Zertifizierungsstelle (CA) ein Zertifikat für Ihre Site ausstellen kann, AWS Certificate Manager (ACM) muss verifizieren, dass Sie Eigentümer oder Inhaber aller Domains sind, die Sie in Ihrer Anfrage angegeben haben. Sie können die Überprüfung entweder per E-Mail oder durchführenDNS. In diesem Thema wird die E-Mail-Validierung behandelt.

Wenn Probleme mit der E-Mail-Validierung auftreten, finden Sie weitere Informationen unter [Beheben von E-Mail-Validierungsproblemen](#).

So funktioniert die E-Mail-Validierung

ACM sendet Bestätigungs-E-Mail-Nachrichten an die folgenden fünf gängigen System-E-Mails für jede Domain. Alternativ können Sie eine Superdomain als Validierungsdomäne angeben, wenn Sie diese E-Mails stattdessen unter dieser Domain erhalten möchten. Jede Subdomain bis zur minimalen Website-Adresse ist gültig und wird als Domain für die E-Mail-Adresse als Suffix danach verwendet. @ Sie können beispielsweise eine E-Mail an `admin@example.com` erhalten, wenn Sie `example.com` als Validierungsdomain für `subdomain.example.com` angeben.

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

Um nachzuweisen, dass Sie Eigentümer der Domain sind, müssen Sie den Bestätigungslink auswählen, der in diesen E-Mails enthalten ist. ACM sendet außerdem Bestätigungs-E-Mails an dieselben Adressen, um das Zertifikat zu verlängern, wenn das Zertifikat 45 Tage vor Ablauf abläuft.

Die E-Mail-Validierung für Zertifikatsanfragen mit mehreren Domains mithilfe von ACM API oder CLI führt dazu, dass von jeder angeforderten Domain eine E-Mail-Nachricht gesendet wird, auch wenn die Anfrage Subdomänen anderer Domänen in der Anfrage umfasst. Der Domaininhaber muss eine E-Mail-Nachricht für jede dieser Domains validieren, bevor er das Zertifikat ausstellen ACM kann.

Ausnahme von diesem Prozess

Wenn Sie ein ACM Zertifikat für einen Domainnamen anfordern, der mit `www` oder einem Platzhalter-Sternchen (*) beginnt, wird das führende `www` Sternchen ACM entfernt und eine E-Mail an die Administratoradressen gesendet. Diese Adressen werden gebildet, indem dem verbleibenden Teil des Domainnamens `admin@`, `administrator@`, `hostmaster@`, `postmaster@` und `webmaster@` vorangestellt wird. Wenn Sie beispielsweise ein ACM Zertifikat für `www.example.com` anfordern, wird die E-Mail an `admin@example.com` und nicht an `admin@www.example.com` gesendet. Ebenso wird eine E-Mail an `admin@test.example.com` gesendet, wenn Sie ein ACM Zertifikat für `*.test.example.com` anfordern. Die verbleibenden Verwaltungsadressen werden auf ähnliche Weise gebildet.

Important

Ab Juni 2024 wird die Überprüfung neuer E-Mails über Kontaktadressen nicht ACM mehr unterstützt. WHOIS Bei bestehenden Zertifikaten werden ab Oktober 2024 ACM keine Verlängerungsbenachrichtigungen an die WHOIS Kontaktadressen der Domain gesendet. ACM wird weiterhin Bestätigungs-E-Mails an die fünf gemeinsamen Systemadressen für die angeforderte Domain senden. Weitere Details finden Sie unter [.AWS Certificate Manager wird die WHOIS Suche nach per E-Mail validierten Zertifikaten einstellen](#)

Überlegungen

Beachten Sie die folgenden Überlegungen zur E-Mail-Validierung.

- Sie benötigen eine funktionierende E-Mail-Adresse, die in Ihrer Domain registriert ist, um die E-Mail-Validierung nutzen zu können. Verfahren zum Einrichten einer E-Mail-Adresse werden in dieser Anleitung jedoch nicht behandelt.
- Die Validierung gilt nur für öffentlich vertrauenswürdige Zertifikate, die von ACM ausgestellt wurden. ACM validiert nicht den Domainbesitz für [importierte Zertifikate](#) oder für Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden. ACM kann Ressourcen in einer VPC [privaten gehosteten Amazon-Zone](#) oder einer anderen privaten Domain nicht validieren. Weitere Informationen finden Sie unter [Fehlerbehebung bei der Zertifikatsvalidierung](#).
- Nachdem Sie ein Zertifikat mit E-Mail-Validierung erstellt haben, können Sie nicht zur Validierung mit DNS wechseln. Um die DNS Validierung zu verwenden, löschen Sie das Zertifikat und erstellen Sie dann ein neues Zertifikat, das DNS Validierung verwendet.

Ablaufdatum des Zertifikats und Zertifikaterneuerung

ACMZertifikate sind 13 Monate (395 Tage) gültig. Die Verlängerung eines Zertifikats erfordert Maßnahmen des Domaininhabers. ACM beginnt 45 Tage vor Ablauf mit dem Senden von Verlängerungsmitteln an die mit der Domain verknüpften E-Mail-Adressen. Die Benachrichtigungen enthalten einen Link, auf den der Domaininhaber zur Verlängerung klicken kann. Sobald alle aufgelisteten Domains validiert sind, wird ein erneuertes Zertifikat mit demselben ARN ausgestellt.

(Optional) Bestätigungs-E-Mail erneut senden

Jede Validierungs-E-Mail enthält ein Token, das Sie verwenden können, um eine Zertifikatanforderung zu genehmigen. Da die für den Genehmigungsprozess erforderliche Validierungs-E-Mail jedoch durch Spam-Filter gesperrt oder in der Übertragung verloren gegangen sein kann, läuft das Token nach 72 Stunden automatisch ab. Wenn Sie die Original-E-Mail nicht erhalten oder das Token abgelaufen ist, können Sie verlangen, dass die E-Mail erneut gesendet wird. Informationen zum erneuten Senden einer Bestätigungs-E-Mail finden Sie unter [Erneutes Senden einer Validierungs-E-Mail](#)

Bei weiterhin bestehenden Problemen mit der E-Mail-Validierung finden Sie Informationen im Abschnitt [Beheben von E-Mail-Validierungsproblemen](#) unter [Probleme beheben mit AWS Certificate Manager](#).

Automatisieren AWS Certificate Manager E-Mail-Validierung

E-Mail-validierte ACM Zertifikate erfordern normalerweise manuelle Maßnahmen durch den Domaininhaber. Organizations, die mit einer großen Anzahl von E-Mail-validierten Zertifikaten arbeiten, können es vorziehen, einen Parser zu erstellen, der die erforderlichen Antworten automatisieren kann. Um Kunden bei der E-Mail-Validierung zu unterstützen, werden in den Informationen in diesem Abschnitt die Vorlagen für E-Mail-Nachrichten zur Domaininvalidierung und der Workflow beschrieben, der für den Abschluss des Validierungsprozesses verwendet wird.

Validierungs-E-Mail-Vorlagen

Validierungs-E-Mail-Nachrichten haben eines der beiden folgenden Formate, je nachdem, ob ein neues Zertifikat angefordert oder ein vorhandenes Zertifikat erneuert wird. Der Inhalt der markierten Zeichenfolgen sollte durch Werte ersetzt werden, die spezifisch für die zu validierende Domain sind.

Validieren eines neuen Zertifikats

Text der E-Mail-Vorlage:

```
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

Validieren eines Zertifikats zur Verlängerung

Text der E-Mail-Vorlage:

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.

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>

Sobald Sie eine neue Bestätigungsnachricht erhalten haben von AWS, wir empfehlen, dass Sie sie als aussagekräftigste up-to-date Vorlage für Ihren Parser verwenden. Kunden mit Nachrichtenparsern, die vor November 2020 entworfen wurden, sollten die folgenden Änderungen beachten, die möglicherweise an der Vorlage vorgenommen wurden:

- In der E-Mail-Betreffzeile steht jetzt „Certificate request for *domain name*“ anstelle von „Certificate approval for *domain name*“.
- Die AWS account ID wird jetzt ohne Gedanken- oder Bindestriche dargestellt.
- Der präsentiert Certificate Identifier jetzt das gesamte Zertifikat ARN anstelle einer verkürzten Form, zum Beispiel, *arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369* anstatt. *3b4d78e1-0882-4f51-954a-298ee44ff369*
- Die Zertifikatsgenehmigung enthält URL jetzt *acm-certificates.amazon.com* statt *certificates.amazon.com*.
- Das durch Klicken auf die Zertifikatsgenehmigung geöffnete Genehmigungsformular enthält URL jetzt die Schaltfläche Genehmigung. Der Name des Genehmigungsschaltflächen-div lautet jetzt *approve-button* anstelle von *approval_button*.
- Validierungsnachrichten sowohl für neu angeforderte Zertifikate als auch für erneuerte Zertifikate haben das gleiche E-Mail-Format.

Workflow zur Validierung

Dieser Abschnitt enthält Informationen zum Verlängerungsworkflow für E-Mail-validierte Zertifikate.

- Wenn die ACM Konsole eine Zertifikatsanforderung für mehrere Domänen verarbeitet, sendet sie Bestätigungs-E-Mail-Nachrichten an den Domainnamen oder die Validierungsdomäne, die Sie bei der Anforderung eines öffentlichen Zertifikats angeben. Der Domaininhaber muss eine E-Mail-Nachricht für jede Domain validieren, bevor er das Zertifikat ausstellen ACM kann. Weitere Informationen finden Sie unter [Mit E-Mail den Domainbesitz prüfen](#).
- Die E-Mail-Validierung für Zertifikatsanfragen mit mehreren Domains mithilfe von ACM API oder CLI führt dazu, dass von jeder angeforderten Domain eine E-Mail-Nachricht gesendet wird, auch wenn die Anfrage Subdomänen anderer Domains in der Anfrage umfasst. Der Domaininhaber muss eine E-Mail-Nachricht für jede dieser Domains validieren, bevor er das Zertifikat ausstellen ACM kann.

Wenn Sie E-Mails für ein vorhandenes Zertifikat erneut über die ACM Konsole senden, werden E-Mails an die in der ursprünglichen Zertifikatsanforderung angegebene Validierungsdomäne gesendet, oder an die genaue Domain, falls keine Validierungsdomäne angegeben wurde. Um Bestätigungs-E-Mails auf einer anderen Domain zu erhalten, können Sie ein neues Zertifikat anfordern und dabei die Validierungsdomäne angeben, die Sie für die Validierung verwenden möchten. Alternativ können Sie [ResendValidationEmail](#) mit dem `ValidationDomain` Parameter `APISDK`, oder aufrufen `CLI`. Die in der `ResendValidationEmail` Anfrage angegebene Validierungsdomäne wird jedoch nur für diesen Anruf verwendet und nicht für future Bestätigungs-E-Mails im Zertifikat Amazon Resource Name (ARN) gespeichert. Sie müssen `ResendValidationEmail` jedes Mal aufrufen, wenn Sie eine Bestätigungs-E-Mail für einen Domainnamen erhalten möchten, der in der ursprünglichen Zertifikatsanforderung nicht angegeben wurde.

Note

Vor November 2020 mussten Kunden nur die Apex-Domain validieren und mussten ein Zertifikat ausstellen ACM, das auch alle Subdomänen abdeckte. Kunden mit Nachrichtenparsern, die vor diesem Zeitpunkt entwickelt wurden, sollten die Änderung am E-Mail-Validierungsworkflow notieren.

- Mit dem ACM API oder können Sie erzwingen `CLI`, dass alle Bestätigungs-E-Mail-Nachrichten für eine Zertifikatsanforderung für mehrere Domänen an die Apex-Domain gesendet werden. Verwenden Sie in der den `DomainValidationOptions` Parameter der

[RequestCertificate](#)AktionAPI, um einen Wert für anzugeben `ValidationDomain`, der ein Mitglied des [DomainValidationOption](#) Typs ist. Verwenden Sie in der CLI den `--domain-validation-options` Parameter des Befehls [request-certificate](#), um einen Wert für anzugeben. `ValidationDomain`

Private Zertifikate in AWS Certificate Manager

Wenn Sie Zugriff auf eine bestehende private Zertifizierungsstelle haben, die von erstellt wurde AWS Private CA, AWS Certificate Manager (ACM) kann ein Zertifikat anfordern, das für die Verwendung in Ihrer privaten Schlüsselinfrastruktur (PKI) geeignet ist. Die Zertifizierungsstelle kann sich entweder in Ihrem Konto befinden oder von einem anderen Konto für Sie freigegeben werden. Informationen zum Erstellen einer Private Certificate Authority finden Sie unter [Erstellen einer Private Certificate Authority](#).

Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden, sind standardmäßig ACM nicht vertrauenswürdig und unterstützen keine Form der Validierung für sie. Folglich muss ein Administrator Maßnahmen ergreifen, um sie in den Client Trust Stores Ihres Unternehmens zu installieren.

Private ACM Zertifikate entsprechen dem X.509-Standard und unterliegen den folgenden Einschränkungen:

- **Namen:** Sie müssen DNS -konforme Betreffnamen verwenden. Weitere Informationen finden Sie unter [Domainnamen](#).
- **Algorithmus:** Für die Verschlüsselung muss der Algorithmus für den privaten Schlüssel des Zertifikats entweder 2048-BitRSA, ECDSA 256-Bit oder 384-Bit sein. ECDSA

Note

Die angegebene Signaturalgorithmusfamilie (RSA oder ECDSA) muss mit der Algorithmusfamilie des geheimen Schlüssels der Zertifizierungsstelle übereinstimmen.

- **Gültigkeitsdauer:** Jedes Zertifikat ist 13 Monate (395 Tage) gültig. Das Enddatum des signierenden CA-Zertifikats muss nach dem Enddatum des angeforderten Zertifikats liegen, sonst schlägt die Zertifikatsanforderung fehl.
- **Verlängerung:** ACM versucht, ein privates Zertifikat nach 11 Monaten automatisch zu erneuern.

Die private CA, die zum Signieren der Endentitätszertifikaten verwendet wird, unterliegt ihren eigenen Einschränkungen:

- Der Status der CA muss aktiv sein.
- Der CA-Algorithmus für private Schlüssel muss RSA 2048 oder RSA 4096 lauten.

 Note

Im Gegensatz zu öffentlich vertrauenswürdigen Zertifikaten müssen von einer privaten CA signierte Zertifikate nicht validiert werden.

Bedingungen für die Verwendung AWS Private CA um ACM private Zertifikate zu signieren

Sie können Folgendes verwenden ... AWS Private CA um Ihre ACM Zertifikate in einem von zwei Fällen zu signieren:

- Einzelkonto: Die signierende Zertifizierungsstelle und die AWS Certificate Manager (ACM) Das ausgestellte Zertifikat befindet sich in demselben AWS Konto.

Damit die Ausstellung und Verlängerung von Einzelkonten aktiviert werden kann, ist AWS Private CA Der Administrator muss dem ACM Dienstprinzipal die Erlaubnis erteilen, Zertifikate zu erstellen, abzurufen und aufzulisten. Dies erfolgt mit dem AWS Private CA APIAktion [CreatePermission](#) oder AWS CLI Befehl [create-permission](#). Der Kontoinhaber weist diese Berechtigungen einem IAM Benutzer, einer Gruppe oder einer Rolle zu, die für die Ausstellung von Zertifikaten verantwortlich ist.

- Kontoübergreifend: Die signierende Zertifizierungsstelle und das ausgestellte ACM Zertifikat befinden sich an unterschiedlichen Orten AWS Konten, und der Zugriff auf die Zertifizierungsstelle wurde dem Konto gewährt, auf dem sich das Zertifikat befindet.

Um die kontenübergreifende Ausstellung und Verlängerung zu ermöglichen, AWS Private CA Der Administrator muss der CA eine ressourcenbasierte Richtlinie hinzufügen, indem er den AWS Private CA APIAktion oder [PutPolicy](#) AWS CLI Befehl [put-policy](#). Die Richtlinie gibt Prinzipale in anderen Konten an, denen eingeschränkter Zugriff auf die Zertifizierungsstelle gewährt wird. Weitere Informationen finden Sie unter [Verwenden einer ressourcenbasierten Richtlinie mit einer ACM privaten Zertifizierungsstelle](#).

Das kontenübergreifende Szenario erfordert außerdem ACM die Einrichtung einer dienstbezogenen Rolle (SLR), die als Principal mit der PCA Richtlinie interagiert. ACM erstellt das SLR automatisch bei der Ausstellung des ersten Zertifikats.

ACM weist Sie möglicherweise darauf hin, dass nicht festgestellt werden kann, ob auf Ihrem Konto ein SLR vorhanden ist. Wenn die erforderliche `iam:GetRole` Genehmigung ACM SLR für Ihr Konto bereits erteilt wurde, wird die Warnung nach der Erstellung des Kontos nicht erneut SLR angezeigt. Wenn sie erneut auftritt, müssen Sie oder Ihr Kontoadministrator möglicherweise die `iam:GetRole` Genehmigung für die von Ihnen verwaltete ACM Richtlinie erteilen oder Ihr Konto mit dieser verknüpfen ACM. `AWSCertificateManagerFullAccess`

Weitere Informationen finden Sie unter [Verwenden einer dienstverknüpften Rolle mit ACM](#)

Important

Ihr ACM Zertifikat muss aktiv mit einem unterstützten Zertifikat verknüpft sein AWS Dienst, bevor er automatisch verlängert werden kann. Informationen zu den Ressourcen, die ACM unterstützt werden, finden Sie unter [In ACM integrierte Services](#).

Fordern Sie ein privates Zertifikat an in AWS Certificate Manager

Fordern Sie ein privates Zertifikat an (Konsole)

1. Loggen Sie sich ein in AWS Management Console und öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>.

Wählen Sie Request a certificate aus.

2. Wählen Sie auf der Seite Request certificate (Zertifikat anfordern) die Option Request a private certificate (Privates Zertifikat anfordern) und dann Next (Weiter) aus, um fortzufahren.
3. Klicken Sie im Abschnitt Details zur Zertifizierungsstelle auf das Menü Zertifizierungsstelle und wählen Sie eine der verfügbaren privaten Zertifizierungsstellen aus CAs. Wenn die Zertifizierungsstelle von einem anderen Konto aus gemeinsam genutzt ARN wird, werden ihr Eigentumsinformationen vorangestellt.

Es werden Informationen über die CA angezeigt, damit Sie überprüfen können, ob Sie die richtige ausgewählt haben.

- Eigentümer
 - Typ
 - Allgemeiner Name (CN)
 - Organisation (O)
 - Organisationseinheit (OU)
 - Ländername (C)
 - Bundesstaat oder Provinz
 - Ortsname
4. Geben Sie auf der Seite Domain names (Domainnamen) Ihren Domainnamen ein. Sie können einen vollqualifizierten Domänennamen (FQDN), z. B. **www.example.com**, oder einen bloßen Domainnamen oder einen Apex-Domänennamen wie verwenden. **example.com** Sie können auch ein Sternchen (*) als Platzhalter in der Position ganz links verwenden, um mehrere Websitenamen in derselben Domain zu schützen. Zum Beispiel schützt ***.example.com corp.example.com** und **images.example.com**. Der Platzhaltername wird im Feld **Betreff** und in der Erweiterung „Alternativer Betreffname“ des Zertifikats angezeigt. ACM

 Note

Wenn Sie ein Platzhalterzertifikat anfordern, muss sich das Sternchen (*) ganz links im Domainnamen befinden und es kann nur eine Subdomänebene geschützt werden. Zum Beispiel kann ***.example.com login.example.com** und **test.example.com** schützen, jedoch nicht **test.login.example.com**. Beachten Sie außerdem, dass ***.example.com** nur die Subdomains von **example.com** schützt, jedoch nicht die "Bare-" oder "Apex"-Domain (**example.com**). Um beide zu schützen, sehen Sie sich den nächsten Schritt an.

Optional wählen Sie **Add another name to this certificate** (Diesem Zertifikat einen anderen Namen hinzufügen) aus und geben Sie den Namen in das Textfeld ein. Dies ist nützlich für den Schutz einer "Bare"- oder "Apex"-Domain (wie **example.com**) und ihrer Subdomains (wie ***.example.com**).

5. Wählen Sie im Abschnitt **Schlüsselalgorithmus** einen Algorithmus aus.

Informationen, die Ihnen bei der Auswahl eines Algorithmus helfen, finden Sie unter [Markierung AWS Certificate Manager Ressourcen](#).

6. Im Abschnitt Tags können Sie Ihr Zertifikat optional mit Tags versehen. Tags sind Schlüssel-Wert-Paare, die als Metadaten zur Identifizierung und Organisation dienen AWS Ressourcen schätzen. Eine Liste der ACM Tag-Parameter und Anweisungen zum Hinzufügen von Tags zu Zertifikaten nach der Erstellung finden Sie unter [Markierung AWS Certificate Manager Ressourcen](#)
7. Bestätigen Sie im Abschnitt Certificate renewal permissions (Berechtigungen für die Zertifikaterneuerung) den Hinweis auf die Berechtigungen für die Zertifikaterneuerung. Diese Berechtigungen ermöglichen die automatische Verlängerung von privaten PKI Zertifikaten, die Sie mit der ausgewählten Zertifizierungsstelle signieren. Weitere Informationen finden Sie unter [Verwenden einer dienstverknüpften Rolle mit ACM](#).
8. Nachdem Sie alle erforderlichen Informationen angegeben haben, wählen Sie Request (Anfordern) aus. Die Konsole führt Sie zur Zertifikatliste zurück, in der Sie Ihr neues Zertifikat anzeigen können.

 Note

Je nachdem, wie Sie die Liste geordnet haben, kann es sein, dass ein gesuchtes Zertifikat nicht sofort sichtbar ist. Klicken Sie rechts auf das schwarze Dreieck, um die Reihenfolge zu ändern. Sie können auch mithilfe der Seitenzahlen oben rechts durch mehrere Seiten von Zertifikaten navigieren.

Fordern Sie ein privates Zertifikat an (CLI)

Verwenden Sie den Befehl [request-certificate](#), um ein privates Zertifikat in anzufordern. ACM

 Note

Wenn Sie ein privates PKI Zertifikat anfordern, das von einer Zertifizierungsstelle signiert wurde von AWS Private CA, muss die angegebene Signaturalgorithmusfamilie (RSAoderECDSA) mit der Algorithmusfamilie des geheimen Schlüssels der Zertifizierungsstelle übereinstimmen.

```
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
```

Dieser Befehl gibt den Amazon-Ressourcennamen (ARN) Ihres neuen privaten Zertifikats aus.

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

In den meisten Fällen ACM wird Ihrem Konto automatisch eine serviceverknüpfte Rolle (SLR) zugewiesen, wenn Sie zum ersten Mal eine gemeinsame Zertifizierungsstelle verwenden. Das SLR ermöglicht die automatische Verlängerung der von Ihnen ausgestellten Endzertifikate. Um zu überprüfen, ob das vorhanden SLR ist, können Sie IAM mit dem folgenden Befehl eine Abfrage durchführen:

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

Wenn der vorhanden SLR ist, sollte die Befehlsausgabe wie folgt aussehen:

```
{  
  "Role":{  
    "Path":"/aws-service-role/acm.amazonaws.com/",  
    "RoleName":"AWSServiceRoleForCertificateManager",  
    "RoleId":"AAAAAAA0000000BBBBBBB",  
    "Arn":"arn:aws:iam::{account_no}:role/aws-service-role/acm.amazonaws.com/  
AWSServiceRoleForCertificateManager",  
    "CreateDate":"2020-08-01T23:10:41Z",  
    "AssumeRolePolicyDocument":{  
      "Version":"2012-10-17",  
      "Statement":[  
        {  
          "Effect":"Allow",  
          "Principal":{  
            "Service":"acm.amazonaws.com"  
          },  
          "Action":"sts:AssumeRole"  
        }  
      ]  
    },  
    "Description":"SLR for ACM Service for accessing cross-account Private CA",  
    "MaxSessionDuration":3600,  
  }  
}
```

```
"RoleLastUsed":{
  "LastUsedDate":"2020-08-01T23:11:04Z",
  "Region":"ap-southeast-1"
}
}
```

Falls das SLR fehlt, finden Sie weitere Informationen unter [Verwenden einer dienstverknüpften Rolle mit ACM](#).

Exportieren Sie eine AWS Certificate Manager privates Zertifikat

Sie können ein Zertifikat exportieren, das ausgestellt wurde von AWS Private CA zur Verwendung überall in Ihrer privaten PKI Umgebung. Die exportierte Datei enthält das Zertifikat, die Zertifikatkette und den verschlüsselten privaten Schlüssel. Diese Datei muss sicher gespeichert werden. Weitere Informationen zur AWS Private CA, siehe [AWS Private Certificate Authority Benutzerleitfaden](#).

Note

Sie können ein öffentlich vertrauenswürdiges Zertifikat oder seinen privaten Schlüssel nicht exportieren, unabhängig davon, ob es von ausgestellt ACM oder importiert wurde.

Themen

- [Ein privates Zertifikat exportieren \(Konsole\)](#)
- [Exportieren Sie ein privates Zertifikat \(CLI\)](#)

Ein privates Zertifikat exportieren (Konsole)

1. Melden Sie sich bei AWS Management Console und öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen Sie Certificate Manager
3. Wählen Sie den Link des Zertifikats, das Sie exportieren möchten.
4. Wählen Sie Export aus.
5. Geben Sie eine Passphrase für den privaten Schlüssel ein, und bestätigen Sie diese.

Note

Bei der Erstellung Ihrer Passphrase können Sie jedes ASCII Zeichen außer #, \$ oder % verwenden.

- Wählen Sie „Kodierung generieren“. PEM
- Sie können das Zertifikat, die Zertifikatskette und den verschlüsselten Schlüssel in den Speicher kopieren. Alternativ können Sie diese Komponenten mit Export to a file einzeln als Dateien exportieren.
- Wählen Sie Erledigt aus.

Exportieren Sie ein privates Zertifikat (CLI)

Verwenden Sie den Befehl [export-certificate](#), um ein privates Zertifikat und einen privaten Schlüssel zu exportieren. Sie müssen eine Passphrase zuweisen, wenn Sie den Befehl ausführen. Um die Sicherheit zu erhöhen, speichern Sie Ihre Passphrase in einer Datei und geben Sie die Passphrase durch Angabe der Datei an. Dadurch wird verhindert, dass Ihre Passphrase in der Befehlshistorie gespeichert wird und dass andere die Passphrase während der Eingabe sehen.

Note

Die Datei, die die Passphrase enthält, darf nicht in einem Zeilenabschlusszeichen enden. Sie können Ihre Passwortdatei wie folgt überprüfen:

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

In den folgenden Beispielen wird die Befehlsausgabe an übergeben, jq um die PEM Formatierung anzuwenden.

```
[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)\\"'
```

Dadurch wird ein Base64-codiertes Zertifikat PEM im -Format ausgegeben, das auch die Zertifikatskette und den verschlüsselten privaten Schlüssel enthält, wie im folgenden abgekürzten Beispiel.

```
-----BEGIN CERTIFICATE-----
MIIDTCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQDDAx3d3cuc3B1ZHMuaW8wgwEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwW0dL0kxpwkkKwTcEkQuHE1v5Vn6HpbffFmxkdPEasoDhthH
FFWIf4/+V01bDLgju4HgtmV4IJDtqM9rGOZ42eFYmmc3eQ00GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h71HUmnnS8j6YxmtPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQKDAh0cm9sb2xvbDCCASiWdQYJKoZIhvcNAQEBBQADggEP
...
j2PA0viqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPd1+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZwbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDANBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCAggAMB0GCWCGSAF1AwQBKqQQDViroIHStQgN0jR6nTUUnwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTpskNCdCAHqdh0SqBwt65qUTZe3gBt
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrXuHTWjF1
wEuqyd8X/ApkQsYFX/nhep0EIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxf0C1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs90V/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----
```

Um alles in eine Datei auszugeben, fügen Sie die >-Weiterleitung zum vorherigen Beispiel hinzu. Dies führt zu folgendem Ergebnis.

```
$ 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
```

Importiert Zertifikate in AWS Certificate Manager

Zusätzlich zur Anforderung von SSL/TLS-Zertifikaten, bereitgestellt von AWS Certificate Manager (ACM), Sie können Zertifikate importieren, die Sie außerhalb von erhalten haben AWS. Sie können dies tun, weil Sie bereits über ein Zertifikat von einer Zertifizierungsstelle (CA) eines Drittanbieters verfügen oder weil Sie anwendungsspezifische Anforderungen haben, die von ACM ausgestellten Zertifikaten nicht erfüllt werden.

Sie können ein importiertes Zertifikat mit jedem verwenden [AWS Dienst, der in integriert ist ACM](#). Die Zertifikate, die Sie importieren, funktionieren genauso wie die von bereitgestellten ACM, mit einer wichtigen Ausnahme: bietet ACM keine [verwaltete Verlängerung](#) für importierte Zertifikate.

Um ein importiertes Zertifikat zu verlängern, können Sie ein neues Zertifikat von Ihrem Zertifikatsaussteller anfordern und es dann manuell [erneut importieren](#). ACM Diese Aktion behält die Zuordnung des Zertifikats und seinen Amazon-Ressourcennamen (ARN) bei. Alternativ hierzu können Sie auch ein komplett neues Zertifikat importieren. Es können mehrere Zertifikate mit demselben Domainnamen importiert werden, sie müssen jedoch einzeln importiert werden.

Important

Sie sind verantwortlich für die Überwachung und das Ablaufdatum Ihrer importierten Zertifikate sowie für deren Erneuerung, bevor sie ablaufen. Sie können diese Aufgabe vereinfachen, indem Sie Amazon CloudWatch Events verwenden, um Benachrichtigungen zu versenden, wenn Ihre importierten Zertifikate bald ablaufen. Weitere Informationen finden Sie unter [Amazon verwenden EventBridge](#).

Bei allen Zertifikaten ACM handelt es sich um regionale Ressourcen, einschließlich der Zertifikate, die Sie importieren. Um dasselbe Zertifikat mit Elastic Load Balancing Balancing-Load Balancern in verschiedenen Umgebungen zu verwenden AWS Regionen: Sie müssen das Zertifikat in jede Region importieren, in der Sie es verwenden möchten. Um ein Zertifikat bei Amazon verwenden zu können

CloudFront, müssen Sie es in die Region USA Ost (Nord-Virginia) importieren. Weitere Informationen finden Sie unter [Unterstützte Regionen](#).

Informationen zum Importieren von Zertifikaten in ACM finden Sie in den folgenden Themen. Wenn Sie Probleme beim Importieren eines Zertifikats haben, finden Sie weitere Informationen unter [Zertifikatsimport](#).

Themen

- [Voraussetzungen für den Import von ACM Zertifikaten](#)
- [Zertifikat- und Schlüsselformat für den Import](#)
- [Importiert ein Zertifikat](#)
- [Importieren Sie ein Zertifikat erneut](#)

Voraussetzungen für den Import von ACM Zertifikaten

Um ein selbstsigniertes SSL TLS /-Zertifikat in zu importierenACM, müssen Sie sowohl das Zertifikat als auch seinen privaten Schlüssel angeben. Um ein Zertifikat zu importieren, das nicht signiert wurde AWS Zertifizierungsstelle (CA), Sie müssen auch die privaten und öffentlichen Schlüssel des Zertifikats angeben. Ihr Zertifikat muss alle in diesem Thema beschriebenen Kriterien erfüllen.

Sie müssen für alle Zertifikate einen kryptographischen Algorithmus und eine Schlüsselgröße angeben. ACMunterstützt die folgenden Algorithmen (APIName in Klammern):

- 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

Beachten Sie auch die folgenden zusätzlichen Anforderungen:

- ACMBei [integrierten Diensten](#) können nur die Algorithmen und Schlüsselgrößen, die sie unterstützen, ihren Ressourcen zugeordnet werden. Unterstützt beispielsweise CloudFront nur 256-Bit-, 2048-Bit- RSARSA, 3072-Bit- und Elliptic Prime Curve-256-Bit-SchlüsselRSA, während

Application Load Balancer alle Algorithmen unterstützt, die von verfügbar sind. ACM Weitere Informationen finden Sie in der Dokumentation zum Service, den Sie verwenden.

- Bei einem Zertifikat muss es sich um ein//X.509 Version 3-Zertifikat handeln. SSL TLS Es muss einen öffentlichen Schlüssel, den vollqualifizierten Domainnamen (FQDN) oder die IP-Adresse für Ihre Website sowie Informationen über den Aussteller enthalten.
- Ein Zertifikat kann von Ihrem privaten Schlüssel, der Ihnen gehört, selbstsigniert oder vom privaten Schlüssel einer ausstellenden Zertifizierungsstelle signiert werden. Sie müssen den privaten Schlüssel bereitstellen, der nicht größer als 5 KB (5 120 Bytes) sein darf und unverschlüsselt sein muss.
- Wenn das Zertifikat von einer Zertifizierungsstelle signiert ist und Sie sich dafür entscheiden, die Zertifikatskette bereitzustellen, muss die Kette PEM —codiert sein.
- Ein Zertifikat muss zum Zeitpunkt des Imports gültig sein. Sie können ein Zertifikat nicht importieren, bevor sein Gültigkeitszeitraum beginnt oder nachdem es abgelaufen ist. Das `NotBefore`-Zertifikatsfeld enthält das Startdatum der Gültigkeit und das `NotAfter`-Feld enthält das Enddatum.
- Alle erforderlichen Zertifikatsmaterialien (Zertifikat, privater Schlüssel und Zertifikatskette) müssen —codiert sein PEM. Das Hochladen von DER —codierten Materialien führt zu einem Fehler. Weitere Informationen und Beispiele finden Sie unter [Zertifikat- und Schlüsselformat für den Import](#).
- Wenn Sie ein Zertifikat erneuern (erneut importieren), können Sie keine `KeyUsage`- oder `ExtendedKeyUsage`-Erweiterung hinzufügen, wenn diese im zuvor importierten Zertifikat nicht vorhanden war.
- AWS CloudFormation unterstützt nicht den Import von Zertifikaten in. ACM

Zertifikat- und Schlüsselformat für den Import

ACM erfordert, dass Sie das Zertifikat, die Zertifikatskette und den privaten Schlüssel (falls vorhanden) separat importieren und jede Komponente im PEM Format kodieren. PEM steht für Privacy Enhanced Mail. Das PEM Format wird häufig zur Darstellung von Zertifikaten, Zertifikatsanfragen, Zertifikatsketten und Schlüsseln verwendet. Die typische Erweiterung für eine PEM —formatierte Datei ist `.pem`, muss es aber nicht sein.

Note

AWS bietet keine Hilfsprogramme zum Bearbeiten von PEM Dateien oder anderen Zertifikatsformaten. Die folgenden Beispiele stützen sich auf einen generischen Texteditor

für einfache Operationen. Wenn Sie komplexere Aufgaben ausführen müssen (z. B. das Konvertieren von Dateiformaten oder das Extrahieren von Schlüsseln), SSL stehen kostenlose Open-Source-Tools wie [Open](#) zur Verfügung.

Die folgenden Beispiele veranschaulichen das Format der zu importierenden Dateien. Wenn Sie die Komponenten in einer einzigen Datei erhalten, verwenden Sie einen Texteditor, um sie in drei Dateien (sorgfältig) zu trennen. Beachten Sie, dass das Zertifikat, die Zertifikatskette oder der private Schlüssel ungültig sind, wenn Sie eines der Zeichen in einer PEM Datei falsch bearbeiten oder wenn Sie am Ende einer Zeile ein oder mehrere Leerzeichen hinzufügen.

Example 1. PEM—codiertes Zertifikat

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

Example 2. PEM—verschlüsselte Zertifikatskette

Eine Zertifikatskette enthält ein oder mehrere Zertifikate. Sie können Ihre Zertifikatsdateien mit einem Texteditor dem copy-Befehl in Windows oder dem cat-Befehl in Linux zu einer Kette verknüpfen. Die Zertifikate müssen verkettet werden, damit jedes von ihnen direkt das jeweils vorhergehende zertifiziert. Wenn Sie ein privates Zertifikat importieren, kopieren Sie das Stammzertifikat zuletzt. Das folgende Beispiel enthält drei Zertifikate, Ihre Zertifikatskette enthält möglicherweise jedoch mehr oder weniger.

Important

Kopieren Sie Ihr Zertifikat nicht in die Zertifikatskette.

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

```
-----END CERTIFICATE-----
```

Example 3. PEM—verschlüsselte private Schlüssel

Zertifikate in X.509 Version 3 verwenden Algorithmen mit öffentlichem Schlüssel. Wenn Sie ein X.509-Zertifikat oder Zertifikatanforderung erstellen, geben Sie den Algorithmus und die Größe des Schlüssels in Bit an, die zum Erstellen des privaten/öffentlichen Schlüsselpaars verwendet werden sollen. Der öffentliche Schlüssel wird in das Zertifikat oder die Anforderung aufgenommen. Sie müssen die zugehörigen privaten Schlüssel geheim halten. Geben Sie den privaten Schlüssel an, wenn Sie das Zertifikat importieren. Der Schlüssel muss unverschlüsselt sein. Das folgende Beispiel zeigt einen RSA privaten Schlüssel.

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

Das nächste Beispiel zeigt einen privaten Schlüssel mit elliptischer Kurve, der mit PEM —kodiert ist. Je nachdem, wie Sie den Schlüssel erstellen, sind die Parameterblöcke möglicherweise nicht enthalten. Wenn der Parameterblock enthalten ist, wird er ACM entfernt, bevor der Schlüssel während des Importvorgangs verwendet wird.

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

Importiert ein Zertifikat

Sie können ein extern erworbenes Zertifikat (d. h. ein Zertifikat, das von einem Drittanbieter für Vertrauensdienste bereitgestellt wurde) importieren, ACM indem Sie AWS Management Console, das AWS CLI, oder der ACM API. Die folgenden Themen zeigen Ihnen, wie Sie AWS Management Console und die AWS CLI. Verfahren zur Erlangung eines Zertifikats von einem Nicht-AWS Emittenten fallen nicht in den Geltungsbereich dieses Leitfadens.

⚠ Important

Ihr ausgewählter Signaturalgorithmus muss den [Voraussetzungen für den Import von ACM Zertifikaten](#) aus.

Themen

- [Importieren \(Konsole\)](#)
- [Importieren \(AWS CLI\)](#)

Importieren (Konsole)

Das folgende Beispiel zeigt, wie Sie ein Zertifikat importieren, indem Sie AWS Management Console.

1. Öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>. Wenn Sie es zum ersten Mal verwenden ACM, suchen Sie nach AWS Certificate Manager Überschrift und wählen Sie die Schaltfläche Erste Schritte darunter.
2. Wählen Sie Import a certificate.
3. Gehen Sie wie folgt vor:
 - a. Fügen Sie das zu importierende Zertifikat in das Feld PEM Zertifikatshauptteil ein. Es sollte mit -----BEGIN CERTIFICATE----- beginnen und mit -----END CERTIFICATE----- enden.
 - b. Fügen Sie für den privaten Schlüssel des Zertifikats den PEM -codierten, unverschlüsselten privaten Schlüssel des Zertifikats ein. Es sollte mit -----BEGIN PRIVATE KEY----- beginnen und mit -----END PRIVATE KEY----- enden.
 - c. (Optional) Fügen Sie für die Zertifikatskette die PEM -kodierte Zertifikatskette ein.
4. (Optional) Um Ihrem importierten Zertifikat Tags hinzuzufügen, wählen Sie Tags aus. Ein Tag ist eine Bezeichnung, die Sie einem zuweisen AWS Ressource. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Sie können Tags verwenden, um Ihre Ressourcen zu organisieren oder Ihre AWS Kosten.
5. Wählen Sie Importieren aus.

Importieren (AWS CLI)

Das folgende Beispiel zeigt, wie Sie ein Zertifikat mit dem importieren [AWS Command Line Interface \(AWS CLI\)](#). Das Beispiel geht von folgenden Annahmen aus:

- Das PEM -kodierte Zertifikat wird in einer Datei mit dem Namen gespeichert. `Certificate.pem`
- Die mit PEM -kodierte Zertifikatskette wird in einer Datei mit dem Namen gespeichert. `CertificateChain.pem`
- Der PEM -kodierte, unverschlüsselte private Schlüssel wird in einer Datei mit dem Namen gespeichert. `PrivateKey.pem`

Um das folgende Beispiel zu verwenden, ersetzen Sie den Dateinamen durch Ihren eigenen und geben Sie den Befehl auf einer kontinuierlichen Zeile ein. Das folgende Beispiel enthält Zeilenumbrüche und zusätzliche Leerzeichen, um das Lesen zu vereinfachen.

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

Wenn der `import-certificate` Befehl erfolgreich ist, gibt er den [Amazon-Ressourcennamen \(ARN\)](#) des importierten Zertifikats zurück.

Importieren Sie ein Zertifikat erneut

Wenn Sie ein Zertifikat importiert und es mit anderen verknüpft haben AWS Dienste, Sie können dieses Zertifikat erneut importieren, bevor es abläuft, und dabei Folgendes beibehalten AWS Dienstverknüpfungen des Originalzertifikats. Weitere Informationen zur AWS Dienste, in die integriert ACM sind, siehe [In ACM integrierte Services](#).

Die folgenden Bedingungen gelten, wenn Sie ein Zertifikat erneut importieren:

- Sie können Domainnamen hinzufügen oder entfernen.
- Sie können nicht alle Domainnamen aus einem Zertifikat entfernen.
- Wenn Erweiterungen für die Schlüsselverwendung im ursprünglich importierten Zertifikat vorhanden sind, können Sie neue Erweiterungswerte hinzufügen, vorhandene Werte jedoch nicht entfernen.

- Wenn Erweiterungen für die erweiterte Schlüsselverwendung im ursprünglich importierten Zertifikat vorhanden sind, können Sie neue Erweiterungswerte hinzufügen, vorhandene Werte jedoch nicht entfernen.
- Der Schlüsseltyp und seine Größe können nicht verändert werden.
- Beim erneuten Importieren eines Zertifikats können keine Ressourcen-Tags angewendet werden.

Themen

- [Wiederimportieren \(Konsole\)](#)
- [Erneut importieren \(AWS CLI\)](#)

Wiederimportieren (Konsole)

Das folgende Beispiel zeigt, wie Sie ein Zertifikat erneut importieren, indem Sie AWS Management Console.

1. Öffnen Sie die ACM Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen oder erweitern Sie das Zertifikat, das erneut importiert werden soll.
3. Öffnen Sie den Detailbereich des Zertifikats und klicken Sie auf die Schaltfläche Reimport certificate. Wenn Sie das Zertifikat durch Aktivierung des Kontrollkästchens neben dem Namen ausgewählt haben, klicken Sie auf Reimport certificate im Menü Actions.
4. Fügen Sie in das Feld Certificate body das PEM -kodierte Endentitätszertifikat ein.
5. Fügen Sie für den privaten Schlüssel des Zertifikats den unverschlüsselten, PEM -codierten privaten Schlüssel ein, der dem öffentlichen Schlüssel des Zertifikats zugeordnet ist.
6. (Optional) Fügen Sie für die Zertifikatskette die PEM -kodierte Zertifikatskette ein. Die Zertifikatskette enthält ein oder mehrere Zertifikate für alle ausstellenden Stellen für Zwischenzertifikate und das Stammzertifikat. Wenn das zu importierende Zertifikat selbst zugewiesen ist, ist keine Zertifikatskette erforderlich.
7. Überprüfen Sie die Informationen zu Ihrem Zertifikat. Wenn keine Fehler vorhanden sind, wählen Sie Reimport.

Erneut importieren (AWS CLI)

Das folgende Beispiel zeigt, wie Sie ein Zertifikat erneut importieren, indem Sie [AWS Command Line Interface \(AWS CLI\)](#). Das Beispiel geht von folgenden Annahmen aus:

- Das PEM -kodierte Zertifikat wird in einer Datei mit dem Namen gespeichert. `Certificate.pem`
- Die mit PEM -kodierte Zertifikatskette wird in einer Datei mit dem Namen gespeichert. `CertificateChain.pem`
- (Nur private Zertifikate) Der PEM -kodierte, unverschlüsselte private Schlüssel wird in einer Datei mit dem Namen gespeichert. `PrivateKey.pem`
- Sie haben das ARN Zertifikat, das Sie erneut importieren möchten.

Um das folgende Beispiel zu verwenden, ersetzen Sie die Dateinamen und die ARN durch Ihre eigenen und geben Sie den Befehl in einer durchgehenden Zeile ein. Das folgende Beispiel enthält Zeilenumbrüche und zusätzliche Leerzeichen, um das Lesen zu vereinfachen.

Note

Um ein Zertifikat erneut zu importieren, müssen Sie das Zertifikat ARN angeben.

```
$ 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
```

Wenn der `import-certificate` Befehl erfolgreich ist, gibt er den [Amazon-Ressourcennamen \(ARN\)](#) des Zertifikats zurück.

Listet Zertifikate auf, die verwaltet werden von AWS Certificate Manager

Sie können die ACM Konsole verwenden oder AWS CLI um die Zertifikate aufzulisten, die von verwaltet werden ACM. Die Konsole kann bis zu 500 Zertifikate auf einer Seite auflisten und CLI bis zu 1000.

So führen Sie Ihre Zertifikate mit der Konsole auf

1. Öffnen Sie die ACM Konsole unter <https://console.aws.amazon.com/acm/>.

2. Überprüfen Sie die Informationen in der Zertifikatliste. Sie können mithilfe der Seitenzahlen oben rechts durch mehrere Seiten von Zertifikaten navigieren. Jedes Zertifikat belegt eine Zeile mit den folgenden Spalten, die standardmäßig für jedes Zertifikat angezeigt werden:
- Domainname — Der vollqualifizierte Domainname (FQDN) für das Zertifikat.
 - Typ: Der Typ des Zertifikats. Die möglichen Werte sind: Von Amazon ausgestellt | Privat | Importiert.
 - Status: Zertifikatsstatus. Die möglichen Werte sind: Validierung ausstehend | Ausgestellt | Inaktiv | Abgelaufen | Widerrufen | Fehlgeschlagen | Zeitüberschreitung der Validierung
 - In Verwendung? — Ob das ACM Zertifikat aktiv mit einem verknüpft ist AWS Dienst wie Elastic Load Balancing oder CloudFront. Der Wert kann No oder Yes lauten.
 - Verlängerungsberechtigung — Gibt an, ob das Zertifikat automatisch verlängert werden kann, bis ACM es fast abläuft. Mögliche Werte sind: Eligible (Berechtigt) | Ineligible (Nicht berechtigt). Die Berechtigungsregeln finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

Durch Auswahl des Einstellungssymbols in der oberen rechten Ecke der Konsole können Sie die Anzahl der auf einer Seite angezeigten Zertifikate anpassen, das Zeilenumbruchverhalten von Zellen festlegen und zusätzliche Informationsfelder anzeigen. Die folgenden optionalen Felder sind verfügbar:

- Additional domain names (Zusätzliche Domainnamen) – Ein oder mehrere Domainnamen (alternative Betreffnamen), die im Zertifikat enthalten sind.
- Angefordert am — Der Zeitpunkt, zu dem das Zertifikat ACM angefordert wurde.
- Issued at (Ausgestellt um) – Die Uhrzeit, zu der das Zertifikat ausgestellt wurde. Diese Informationen sind nur für von Amazon ausgestellte Zertifikate verfügbar, nicht für Importe.
- Not before (Nicht vor) – Die Zeit, vor der das Zertifikat nicht gültig ist.
- Not after (Nicht nach) – Der Zeitpunkt, nach dem das Zertifikat nicht gültig ist.
- Revoked at (Widerrufen um) – Bei widerrufenen Zertifikaten der Zeitpunkt des Widerrufs.
- Name tag (Namensschild) – Der Wert eines Tags auf diesem Zertifikat namens Name, falls ein solches Tag vorhanden ist.
- Verlängerungsstatus – Status der angeforderten Verlängerung eines Zertifikats. Dieses Feld wird nur dann angezeigt und hat nur dann einen Wert, wenn eine Verlängerung angefordert wurde. Mögliche Werte sind: Pending automatic renewal (Automatische Verlängerung steht aus) | Pending validation (Validierung steht aus) | Success (Erfolg) | Failure (Fehler).

Note

Es kann mehrere Stunden dauern, bis Änderungen am Zertifikatsstatus in der Konsole zur Verfügung stehen. Wenn ein Problem auftritt, läuft eine Zertifikatsanforderung nach 72 Stunden ab, und der Ausstellungs- oder Verlängerungsprozess muss von Anfang an wiederholt werden.

Die Einstellung Page size (Seitengröße) gibt die Anzahl der Zertifikate an, die auf jeder Konsolenseite zurückgegeben werden.

Weitere Informationen zu den verfügbaren Zertifikatdetails finden Sie unter [Anzeigen AWS Certificate Manager Details zum Zertifikat](#).

Um Ihre Zertifikate aufzulisten, verwenden Sie den AWS CLI

Verwenden Sie den Befehl [list-certificates](#), um Ihre ACM -verwalteten Zertifikate aufzulisten, wie im folgenden Beispiel gezeigt:

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

Die vom System zurückgegebenen Informationen ähneln den Folgenden:

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

Standardmäßig werden nur Zertifikate mit `keyTypesRSA_1024` oder `RSA_2048` und mit mindestens einer angegebenen Domain zurückgegeben. Wenn Sie andere Zertifikate anzeigen möchten, die Sie steuern, z. B. domainlose Zertifikate oder Zertifikate mit einem anderen Algorithmus oder einer anderen Bitgröße, geben Sie den `--includes`-Parameter an, wie im folgenden Beispiel gezeigt. Mit dem Parameter können ein Element der [Filters](#)-Struktur angeben.

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

Anzeigen AWS Certificate Manager Details zum Zertifikat

Sie können die ACM Konsole verwenden oder AWS CLI um detaillierte Metadaten zu Ihren Zertifikaten aufzulisten.

So lassen Sie sich Zertifikatdetails in der Konsole anzeigen

1. Öffnen Sie die ACM Konsole unter <https://console.aws.amazon.com/acm/>, um Ihre Zertifikate anzuzeigen. Sie können mithilfe der Seitenzahlen oben rechts durch mehrere Seiten von Zertifikaten navigieren.
2. Zum Anzeigen von detaillierten Metadaten für ein aufgelistetes Zertifikat wählen Sie die Zertifikat-ID aus. Eine Seite mit den folgenden Informationen wird geöffnet:

- Zertifikatstatus
 - ID: Hexadezimale eindeutige 32-Byte-Kennung des Zertifikats
 - ARN— Ein Amazon-Ressourcenname (ARN) in der Form
`arn:aws:acm:Region:444455556666:certificate/certificate_ID`

- **Typ** — Identifiziert die Verwaltungskategorie eines ACM Zertifikats. Die möglichen Werte sind: Amazon ausgestellt|Privat|Importiertaus. Weitere Informationen finden Sie unter [AWS Certificate Manager öffentliche Zertifikate](#), [Fordern Sie ein privates Zertifikat an in AWS Certificate Manager](#) oder [Importiert Zertifikate in AWS Certificate Manager](#).
- **Status**: Der Zertifikatstatus. Die möglichen Werte sind: Validierung ausstehend | Ausgestellt | Inaktiv | Abgelaufen | Widerrufen | Fehlgeschlagen | Zeitüberschreitung der Validierung
- **Detaillierter Status**: Datum und Uhrzeit der Ausstellung bzw. des Imports des Zertifikats.
- **Domains**
 - **Domain** — Der vollqualifizierte Domainname (FQDN) für das Zertifikat.
 - **Status**: Der Validierungsstatus der Domain. Die möglichen Werte sind: Validierung ausstehend | Widerrufen | Fehlgeschlagen | Zeitüberschreitung der Validierung | Erfolg
- **Details**
 - **In Verwendung?** — Ob das Zertifikat mit einem verknüpft ist [AWS integrierter Dienst](#)
Mögliche Werte sind: Ja | Nein
 - **Domainname** — Der erste vollqualifizierte Domainname (FQDN) für das Zertifikat.
 - **Anzahl zusätzlicher Namen**: Anzahl der Domainnamen, für die das Zertifikat gültig ist
 - **Seriennummer**: Hexadezimale 16-Byte-Seriennummer des Zertifikats.
 - **Informationen zum öffentlichen Schlüssel**: Der kryptografische Algorithmus, der das Schlüsselpaar generiert hat.
 - **Signatur-Algorithmus**— Der zum Signieren des Zertifikats verwendete kryptografische Algorithmus
 - **Kann verwendet werden mit** — Eine Liste ACM [integrierter Dienste](#), die ein Zertifikat mit diesen Parametern unterstützen
 - **Angefordert um**: Das Datum und die Uhrzeit der Ausstellungsanforderung.
 - **Ausgestellt um**: Gegebenenfalls Datum und Uhrzeit der Ausstellung.
 - **Importiert um**: Gegebenenfalls Datum und Uhrzeit des Imports.
 - **Nicht vor**: Der Beginn der Gültigkeitsdauer des Zertifikats.
 - **Nicht nach**: Ablaufdatum und -uhrzeit des Zertifikats.
 - **Erneuerungsberechtigung**: Die möglichen Werte sind: Berechtig | Nicht berechtigt. Die Berechtigungsregeln finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

- Verlängerungsstatus – Status der angeforderten Verlängerung eines Zertifikats. Dieses Feld wird nur dann angezeigt und hat nur dann einen Wert, wenn eine Verlängerung angefordert wurde. Mögliche Werte sind: Pending automatic renewal (Automatische Verlängerung steht aus) | Pending validation (Validierung steht aus) | Success (Erfolg) | Failure (Fehler).

 Note

Es kann mehrere Stunden dauern, bis Änderungen am Zertifikatsstatus in der Konsole zur Verfügung stehen. Wenn ein Problem auftritt, läuft eine Zertifikatsanforderung nach 72 Stunden ab, und der Ausstellungs- oder Verlängerungsprozess muss von Anfang an wiederholt werden.

- CA — Die ARN der signierenden CA
- Tags
 - Key (Schlüssel)
 - Value (Wert)
- Validierungsstatus — Falls zutreffend, sind die möglichen Werte:
 - Ausstehend — Die Validierung wurde angefordert und wurde nicht abgeschlossen.
 - Zeitüberschreitung für die Validierung— Ein Zeitlimit für die angeforderte Validierung ist abgelaufen, Sie können die Anforderung jedoch wiederholen.
 - Keine — Das Zertifikat ist privat PKI oder selbstsigniert und muss nicht validiert werden.

Um die Zertifikatsdetails anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie das [Describe-Zertifikat](#) in der AWS CLI um Zertifikatsdetails anzuzeigen, wie im folgenden Befehl gezeigt:

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

Die vom System zurückgegebenen Informationen ähneln den Folgenden:

```
{
  "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"
}
```

Löschen Sie Zertifikate, die verwaltet werden von AWS Certificate Manager

Sie können die ACM Konsole verwenden oder AWS CLI um ein Zertifikat zu löschen.

Important

- Sie können kein ACM Zertifikat löschen, das von einem anderen verwendet wird AWS Dienst. Zum Löschen eines Zertifikats, das verwendet wird, müssen Sie zuerst die Zertifikatszuordnung entfernen. Dies erfolgt über die Konsole oder CLI für den zugehörigen Dienst.
- Das Löschen eines Zertifikats, das von einer Private Certificate Authority (CA) ausgestellt wurde, hat keine Auswirkungen auf die CA. Sie werden weiterhin für die Zertifizierungsstelle belastet, bis sie gelöscht wird. Weitere Informationen finden Sie unter [Löschen Ihrer privaten CA](#) im AWS Private Certificate Authority Benutzerleitfaden.

So deaktivieren Sie ein Zertifikat mithilfe der Konsole

1. Öffnen Sie die ACM Konsole unter <https://console.aws.amazon.com/acm/>.
2. Aktivieren Sie in der Liste der Zertifikate das Kontrollkästchen für ein ACM Zertifikat und wählen Sie dann Löschen aus.

Note

Je nachdem, wie Sie die Liste geordnet haben, kann es sein, dass ein gesuchtes Zertifikat nicht sofort sichtbar ist. Klicken Sie rechts auf das schwarze Dreieck, um die Reihenfolge zu ändern. Sie können auch mithilfe der Seitenzahlen oben rechts durch mehrere Seiten von Zertifikaten navigieren.

Um ein Zertifikat zu löschen, verwenden Sie AWS CLI

Verwenden der [Löschen-Zertifikat](#) So löschen Sie ein -Zertifikat, wie im folgenden Befehl gezeigt:

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

Verwaltete Zertifikatserneuerung in AWS Certificate Manager

ACM bietet eine verwaltete Verlängerung für Ihre von Amazon ausgestellten SSL/TLS-Zertifikate. Das bedeutet, dass Ihre Zertifikate entweder automatisch erneuert werden (wenn Sie die DNS-Validierung verwenden) oder dass Ihnen E-Mail-Benachrichtigungen gesendet werden, wenn der Ablauf näher rückt. Diese Dienste werden sowohl für öffentliche als auch für private ACM-Zertifikate bereitgestellt.

Ein Zertifikat kann unter folgenden Gesichtspunkten automatisch verlängert werden:

- **ELIGIBLE** wenn sie mit einem anderen verknüpft sind AWS-Dienst, wie Elastic Load Balancing oder CloudFront.
- **ELIGIBLE** wenn der Export seit der Ausgabe oder der letzten Verlängerung erfolgt.
- **ELIGIBLE** wenn es sich um ein privates Zertifikat handelt, das durch Aufrufen von [ausgestelltes ACM RequestCertificateAPI](#) und dann exportiert oder einem anderen Zertifikat zugeordnet wurde AWS-Dienst.
- **ELIGIBLE** wenn es sich um ein privates Zertifikat handelt, das über die [Managementkonsole](#) ausgestellt und dann exportiert oder einem anderen Zertifikat zugeordnet wurde AWS-Dienst.
- **NOT ELIGIBLE** wenn es sich um ein privates Zertifikat handelt, das durch Aufrufen des [ausgestelltes AWS Private CA IssueCertificate API](#) wurde.
- **NOT ELIGIBLE** wenn [importiert](#).
- **NOT ELIGIBLE** wenn es bereits abgelaufen ist.

Darüber hinaus müssen die folgenden [Punycode](#)-Anforderungen in Bezug auf [internationalisierte Domainnamen](#) erfüllt sein:

1. Domainnamen, die mit dem Muster „<character><character>--“ beginnen, müssen mit „xn--“ übereinstimmen.
2. Domainnamen, die mit „xn--“ beginnen, müssen ebenfalls gültige internationalisierte Domainnamen sein.

Beispiele für Punycode

Domainname	Erfüllt #1	Erfüllt #2	Zulässig	Hinweis
example.com	–	–	✓	Beginnt nicht mit „<character><character>--“
a--example.com	–	–	✓	Beginnt nicht mit „<character><character>--“
abc--example.com	–	–	✓	Beginnt nicht mit „<character><character>--“
xn--xyz.com	Ja	Ja	✓	Gültiger internationalisierter Domainname (wird zu 簡.com aufgelöst)
xn--example.com	Ja	Nein	✗	Kein gültiger internationalisierter Domainname
ab--example.com	Nein	Nein	✗	Muss mit „xn--“ beginnen

Wenn ein Zertifikat ACM erneuert wird, bleibt der Amazon-Ressourcenname (ARN) des Zertifikats derselbe. Außerdem sind ACM-Zertifikate [regionale Ressourcen](#). Wenn Sie mehrere Zertifikate für denselben Domainnamen haben AWS Regionen, jedes dieser Zertifikate muss unabhängig erneuert werden.

Themen

- [Erneuern Sie ACM öffentliche Zertifikate](#)
- [Erneuerung des privaten Zertifikats in AWS Certificate Manager](#)
- [Überprüfen des Erneuerungsstatus eines Zertifikats](#)

Erneuern Sie ACM öffentliche Zertifikate

Bei der Ausstellung eines verwalteten, öffentlich vertrauenswürdigen Zertifikats AWS Certificate Manager verlangt von Ihnen den Nachweis, dass Sie der Domaininhaber sind. Dies geschieht entweder durch [DNSValidierung](#) oder [E-Mail-Validierung](#). Wenn ein Zertifikat verlängert werden muss, ACM verwendet es dieselbe Methode, die Sie zuvor gewählt haben, um Ihr Eigentum erneut zu bestätigen. In den folgenden Themen wird beschrieben, wie der Erneuerungsprozess jeweils funktioniert.

Themen

- [Verlängerung für Domains, die validiert wurden von DNS](#)
- [Verlängerung für Domains, die per E-Mail validiert wurden](#)

Verlängerung für Domains, die validiert wurden von DNS

[Die verwaltete Verlängerung von ACM Zertifikaten, die ursprünglich mithilfe einer Validierung ausgestellt wurden, ist vollständig automatisiert. DNS](#)

ACM prüft 60 Tage vor Ablauf, ob die folgenden Verlängerungskriterien erfüllt sind:

- Das Zertifikat wird derzeit von einem verwendeten AWS Dienst.
- Alle erforderlichen ACM, bereitgestellten DNS CNAME Datensätze (einer für jeden eindeutigen alternativen Betreffnamen) sind vorhanden und öffentlich DNS zugänglich.

Wenn diese Kriterien erfüllt sind, ACM betrachtet die Domainnamen als validiert und erneuert das Zertifikat.

ACM sendet AWS Health Ereignisse und EventBridge Amazon-Ereignisse, wenn eine Domain während der Verlängerung nicht automatisch validiert werden kann (z. B. aufgrund des Vorhandenseins eines CAA Datensatzes). Diese Ereignisse werden 45 Tage, 30 Tage, 15 Tage, sieben Tage, drei Tage und einen Tag vor Ablauf gesendet. Weitere Informationen finden Sie unter [EventBridge Amazon-Unterstützung für ACM](#).

Verlängerung für Domains, die per E-Mail validiert wurden

ACM Zertifikate sind 13 Monate (395 Tage) gültig. Die Verlängerung eines Zertifikats erfordert Maßnahmen des Domaininhabers. ACM beginnt 45 Tage vor Ablauf mit dem Senden

von Verlängerungsmitteilungen an die mit der Domain verknüpften E-Mail-Adressen. Die Benachrichtigungen enthalten einen Link, auf den der Domaininhaber zur Verlängerung klicken kann. Sobald alle aufgelisteten Domains validiert sind ACM, wird ein erneuertes Zertifikat mit demselben ausgestellt ARN.

Weitere Informationen zu E-Mails zu Validierungszwecken finden Sie unter [AWS Certificate Manager E-Mail-Validierung](#)

Informationen dazu, wie Sie programmgesteuert auf E-Mails zu Validierungszwecken reagieren können, finden Sie unter [Automatisieren AWS Certificate Manager E-Mail-Validierung](#).

Erneutes Senden einer Validierungs-E-Mail

Nachdem Sie die E-Mail-Validierung für Ihre Domain konfiguriert haben, wenn Sie ein Zertifikat anfordern (siehe [AWS Certificate Manager E-Mail-Validierung](#)), können Sie die AWS Certificate Manager API um zu verlangen, dass ACM wir Ihnen eine E-Mail mit der Domaininvalidierung für die Verlängerung Ihres Zertifikats zusenden. Sie sollten dies in folgenden Fällen tun:

- Sie haben bei der ursprünglichen Anforderung Ihres ACM Zertifikats die E-Mail-Validierung verwendet.
- Der Erneuerungsstatus Ihres Zertifikats lautet pending validation. Weitere Informationen zum Ermitteln des Erneuerungsstatus eines Zertifikats finden Sie unter [Überprüfen des Erneuerungsstatus eines Zertifikats](#).
- Sie haben die ursprüngliche E-Mail-Nachricht zur Domaininvalidierung, die zur Verlängerung des Zertifikats ACM gesendet wurde, nicht erhalten oder können sie nicht finden.

Um Bestätigungs-E-Mails an eine andere Domain zu senden als die, die Sie ursprünglich in Ihrer Zertifikatsanforderung konfiguriert haben, können Sie den [ResendValidationEmail](#) Vorgang in der ACM API AWS CLI, oder AWS SDKs. ACM sendet E-Mails an die angegebene Validierungsdomäne. Sie können auf die zugreifen AWS CLI im Browser mit AWS CloudShell in unterstützten Regionen.

Um dies zu beantragen, ACM senden Sie die E-Mail-Nachricht zur Domaininvalidierung erneut (Konsole)

1. Öffnen Sie AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen Sie die Zertifikat-ID des Zertifikats aus, das eine Validierung erfordert.
3. Wählen Sie Resend validation email (Validierungs-E-Mail erneut senden) aus.

Um dies zu beantragen, ACM senden Sie die E-Mail zur Domainvalidierung erneut () ACM API

Verwenden Sie den [ResendValidationEmail](#)Vorgang in der ACM API. Übergeben Sie dabei das Zertifikat, die ARN Domain, für die eine manuelle Validierung erforderlich ist, und die Domain, für die Sie die E-Mails zur Domainvalidierung erhalten möchten. Das folgende Beispiel zeigt, wie das geht mit dem AWS CLI. Dieses Beispiel enthält Zeilenumbrüche, um das Lesen zu erleichtern.

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

Erneuerung des privaten Zertifikats in AWS Certificate Manager

ACMZertifikate, die von einer privaten Zertifizierungsstelle von signiert wurden AWS Private CA kommen für eine verwaltete Verlängerung in Frage. Im Gegensatz zu öffentlich vertrauenswürdigen ACM Zertifikaten PKI erfordert ein Zertifikat für ein privates Zertifikat keine Validierung. Vertrauenswürdigkeit wird hergestellt, wenn ein Administrator das entsprechende Stammzertifizierungsstellenzertifikat in Clientvertrauensspeichern installiert.

Note

Nur Zertifikate, die über die ACM Konsole oder über die [RequestCertificate](#)Konsole erworben wurden, ACM API kommen für eine verwaltete Verlängerung in Frage. Zertifikate, die direkt ausgestellt wurden von AWS Private CA unter Verwendung der [IssueCertificate](#)Aktion des AWS Private CA API werden nicht verwaltet von ACM.

Wenn ein verwaltetes Zertifikat in 60 Tagen abläuft, ACM wird automatisch versucht, es zu verlängern. Dazu gehören Zertifikate, die manuell exportiert und installiert wurden (z. B. in einem On-Premises-Rechenzentrum). Kunden können die Verlängerung auch jederzeit erzwingen, indem sie die [RenewCertificate](#)Aktion von verwenden ACM API. Eine Beispiel-Java-Implementierung der erzwungenen Erneuerung finden Sie unter [Erneuern eines Zertifikats](#) aus.

Nach der Erneuerung erfolgt die Bereitstellung eines -Zertifikats auf eine der folgenden Arten:

- Wenn das Zertifikat mit einem ACM [integrierten Dienst](#) verknüpft ist, ersetzt das neue Zertifikat das alte, ohne dass der Kunde zusätzliche Maßnahmen ergreifen muss.

- Wenn das Zertifikat keinem ACM [integrierten Dienst](#) zugeordnet ist, muss der Kunde aktiv werden, um das erneuerte Zertifikat zu exportieren und zu installieren. Sie können diese Aktionen manuell oder mit Unterstützung von durchführen [AWS Health](#) EventBridge, [Amazon](#) und [AWS Lambda](#) wie folgt. Weitere Informationen finden Sie unter [Automatisieren Sie den Export erneuerter Zertifikate](#)

Automatisieren Sie den Export erneuerter Zertifikate

Das folgende Verfahren bietet eine Beispiellösung für die Automatisierung des Exports Ihrer privaten PKI Zertifikate bei deren ACM Verlängerung. In diesem Beispiel werden nur ein Zertifikat und sein privater Schlüssel aus exportiert. ACM Nach dem Export muss das Zertifikat weiterhin auf dem Zielgerät installiert sein.

Automatisieren des Zertifikatexports mithilfe der Konsole

1. Folgende Verfahren finden Sie in AWS Lambda Developer Guide, erstellen und konfigurieren Sie eine Lambda-Funktion, die Export aufruft ACM. API
 - a. [Erstellen Sie eine Lambda-Funktion.](#)
 - b. [Erstellen einer Lambda-Ausführungsrolle](#) für Ihre Funktion und fügen Sie ihr die folgende Vertrauensrichtlinie hinzu. Die Richtlinie erteilt dem Code in Ihrer Funktion die Erlaubnis, das erneuerte Zertifikat und den privaten Schlüssel abzurufen, indem die [ExportCertificate](#) Aktion von aufgerufen wird. ACM API

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

2. [Erstellen Sie in Amazon eine Regel EventBridge](#), um auf ACM Gesundheitsereignisse zu warten, und rufen Sie Ihre Lambda-Funktion auf, wenn sie eines erkennt. ACM schreibt an eine AWS Health Ereignis bei jedem Versuch, ein Zertifikat zu erneuern. Weitere Informationen zu diesen Werten finden Sie unter [Überprüfen Sie den Status mit dem Personal Health Dashboard \(PHD\)](#).

Konfigurieren Sie die Regel, indem Sie das folgende Ereignismuster hinzufügen.

```
{
  "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. Schließen Sie den Erneuerungsprozess ab, indem Sie das Zertifikat manuell auf dem Zielsystem installieren.

Testen Sie die verwaltete Verlängerung von privaten PKI Zertifikaten

Sie können das oder verwenden ACM API AWS CLI um die Konfiguration Ihres ACM verwalteten Verlängerungsworkflows manuell zu testen. Auf diese Weise können Sie sicherstellen, dass Ihre Zertifikate ACM vor Ablauf automatisch verlängert werden.

Note

Sie können nur die Verlängerung von Zertifikaten testen, die ausgestellt und exportiert wurden von AWS Private CA.

Wenn Sie die unten beschriebenen API Aktionen oder CLI Befehle verwenden, wird ACM versucht, das Zertifikat zu erneuern. Wenn die Verlängerung erfolgreich ist, werden die Metadaten des Zertifikats ACM aktualisiert, die in der Managementkonsole oder in der API Ausgabe angezeigt werden. Wenn das Zertifikat mit einem ACM [integrierten Service](#) verknüpft ist, wird das neue Zertifikat bereitgestellt und ein Verlängerungsereignis wird in Amazon CloudWatch Events generiert. Schlägt die Verlängerung fehl, wird ein Fehler ACM zurückgegeben und es werden Abhilfemaßnahmen vorgeschlagen. (Sie können diese Informationen mit der [describe-certificate](#)-Befehl.) Wenn das Zertifikat nicht über einen integrierten Dienst bereitgestellt wird, müssen Sie es trotzdem exportieren und manuell auf Ihrer Ressource installieren.

Important

Um Ihre zu verlängern AWS Private CA Zertifikate mit ACM, Sie müssen dem ACM Dienstprinzipal zunächst die entsprechenden Berechtigungen erteilen. Weitere Informationen finden Sie unter [Zuweisen von Berechtigungen zur Zertifikatserneuerung an ACM](#).

Um die Zertifikatserneuerung manuell zu testen (AWS CLI)

1. Verwenden Sie den Befehl [renew-certificate](#), um ein privates exportiertes Zertifikat zu erneuern.

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

2. Verwenden Sie dann den Befehl [describe-certificate](#), um zu prüfen, ob die Details der Zertifikatserneuerung aktualisiert wurden.

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

Um die Zertifikatsverlängerung manuell zu testen (ACMAPI)

- Senden Sie eine [RenewCertificate](#) Anfrage, in ARN der Sie angeben, welches private Zertifikat erneuert werden soll. Verwenden Sie dann den [DescribeCertificate](#) Vorgang, um zu überprüfen, ob die Verlängerungsdetails des Zertifikats aktualisiert wurden.

Überprüfen des Erneuerungsstatus eines Zertifikats

Wenn Sie versucht haben, ein Zertifikat zu verlängern, wird in ACM den Zertifikatsdetails ein Feld mit Informationen zum Verlängerungsstatus angezeigt. Sie können das AWS Certificate Manager Konsole, die ACM API, die AWS CLI, oder das AWS Health Dashboard um den Verlängerungsstatus eines ACM Zertifikats zu überprüfen. Wenn Sie die Konsole verwenden, AWS CLI ACM API, oder der Verlängerungsstatus kann einen der vier unten aufgeführten möglichen Statuswerte haben. Ähnliche Werte werden angezeigt, wenn Sie AWS Health Dashboard.

Pending automatic renewal

ACM versucht, die Domainnamen im Zertifikat automatisch zu validieren. Weitere Informationen finden Sie unter [Verlängerung für Domains, die validiert wurden von DNS](#). Es sind keine weiteren Maßnahmen erforderlich.

Pending validation

ACM konnte einen oder mehrere Domainnamen im Zertifikat nicht automatisch validieren. Sie müssen Maßnahmen ergreifen, um diese Domainnamen zu validieren, oder das Zertifikat wird nicht erneuert. Wenn Sie ursprünglich die E-Mail-Validierung für das Zertifikat verwendet haben, suchen Sie nach einer E-Mail von ACM und folgen Sie dann dem Link in dieser E-Mail, um die Validierung durchzuführen. Wenn Sie die DNS Validierung verwendet haben, stellen Sie sicher, dass Ihr DNS Datensatz existiert und dass Ihr Zertifikat weiterhin verwendet wird.

Herzlichen Glückwunsch

Alle Domainnamen im Zertifikat wurden validiert und das Zertifikat ACM wurde erneuert. Es sind keine weiteren Maßnahmen erforderlich.

Fehlgeschlagen

Ein oder mehrere Domainnamen wurden vor Ablauf des Zertifikats nicht validiert und das Zertifikat ACM wurde nicht erneuert. Sie können [ein neues Zertifikat anfordern](#).

Ein Zertifikat kann verlängert werden, wenn es mit einem anderen verknüpft ist AWS Dienst, wie Elastic Load Balancing oder CloudFront, oder wenn er seit seiner Ausgabe oder letzten Verlängerung exportiert wurde.

Note

Es kann mehrere Stunden dauern, bis Änderungen am Verlängerungsstatus in der Konsole zur Verfügung stehen. Wenn ein Problem auftritt, läuft eine Verlängerungsanforderung nach 72 Stunden ab, und der Verlängerungsprozess muss von Anfang an wiederholt werden. Hilfe zur Problembhebung finden Sie unter [Problembehandlung bei Zertifikatsanfragen](#).

Themen

- [Überprüfen des Status \(Konsole\)](#)
- [Überprüfen Sie den Status \(API\)](#)
- [Überprüfen Sie den Status \(CLI\)](#)
- [Überprüfen Sie den Status mit dem Personal Health Dashboard \(PHD\)](#)

Überprüfen des Status (Konsole)

Im folgenden Verfahren wird beschrieben, wie Sie die ACM Konsole verwenden, um den Verlängerungsstatus eines ACM Zertifikats zu überprüfen.

1. Öffnen Sie AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Erweitern eines Zertifikats, um seine Details anzuzeigen.
3. Suchen Sie den Renewal Status (Verlängerungsstatus) im Abschnitt Details. Wenn Sie den Status nicht sehen, wurde der verwaltete Verlängerungsprozess für dieses Zertifikat ACM noch nicht gestartet.

Überprüfen Sie den Status (API)

Ein Java-Beispiel, das zeigt, wie die [DescribeCertificate](#)Aktion zur Überprüfung des Status verwendet wird, finden Sie unter [Beschreiben eines Zertifikats](#).

Überprüfen Sie den Status (CLI)

Das folgende Beispiel zeigt, wie Sie den Status Ihrer ACM Zertifikatserneuerung mit dem überprüfen können [AWS Command Line Interface \(AWS CLI\)](#).

```
$ aws acm describe-certificate \
```

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

Achten Sie in der Antwort auf den Wert im `RenewalStatus`-Feld. Wenn Sie das `RenewalStatus` Feld nicht sehen, wurde der verwaltete Verlängerungsprozess für Ihr Zertifikat ACM noch nicht gestartet.

Überprüfen Sie den Status mit dem Personal Health Dashboard (PHD)

ACM versucht, Ihr ACM Zertifikat 60 Tage vor Ablauf automatisch zu verlängern. Wenn Ihr Zertifikat ACM nicht automatisch verlängert werden kann, sendet es Benachrichtigungen über Ereignisse zur Verlängerung des Zertifikats an Ihre AWS Health Dashboard in Intervallen von 45 Tagen, 30 Tagen, 15 Tagen, 7 Tagen, 3 Tagen und 1 Tag vor Ablauf, um Sie darüber zu informieren, dass Sie Maßnahmen ergreifen müssen. Das Tool AWS Health Dashboard ist Teil der AWS Health Dienst. Sie benötigt keine Einrichtung und kann von jedem Benutzer angezeigt werden, der in Ihrem Konto authentifiziert ist. Weitere Informationen finden Sie unter [AWS Health Benutzerleitfaden](#).

Note

ACM schreibt aufeinanderfolgende Benachrichtigungen zu Verlängerungseignissen zu einem einzelnen Ereignis in Ihrer PHD Zeitleiste. Jede Benachrichtigung überschreibt die vorherige, bis die Erneuerung erfolgreich ist.

Um das AWS Health Dashboard:

1. Loggen Sie sich ein in den AWS Health Dashboard zu https://phd.aws.amazon.com/phd/Hause#.
2. Wählen Sie Event log.
3. Wählen Sie für Filter by tags or attributes die Option Service.
4. Wählen Sie Certificate Manager.
5. Wählen Sie Apply (Anwenden) aus.
6. Wählen Sie für Event category die Option Scheduled Change.
7. Wählen Sie Apply (Anwenden) aus.

Markierung AWS Certificate Manager Ressourcen

Ein Tag ist eine Bezeichnung, die Sie einem ACM Zertifikat zuweisen können. Jedes Tag besteht aus einem Schlüssel und einem Wert. Sie können das AWS Certificate Manager Konsole, AWS Command Line Interface (AWS CLI), oder ACM API um Tags für ACM Zertifikate hinzuzufügen, anzuzeigen oder zu entfernen. Sie können wählen, welche Tags in der ACM Konsole angezeigt werden sollen.

Sie können benutzerdefinierte Tags erstellen, die Ihren Anforderungen entsprechen. Sie könnten beispielsweise mehrere ACM Zertifikate mit einem `Environment = Prod Environment = Beta` Oder-Tag kennzeichnen, um zu identifizieren, für welche Umgebung jedes ACM Zertifikat bestimmt ist. In der folgende Liste sind einige weitere Beispiele für andere benutzerdefinierte Tags enthalten:

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

Sonstige AWS Ressourcen unterstützen auch Tagging. Sie können deshalb denselben Tag für verschiedene Ressourcen zuweisen, um anzugeben, ob diese Ressourcen verknüpft sind. Sie können beispielsweise dem ACM Zertifikat, dem Load Balancer und anderen Ressourcen, die für Ihre Website `example.com` verwendet werden, ein Tag zuweisen. `Website = example.com`

Themen

- [Tag-Einschränkungen](#)
- [Verwalten von Tags](#)

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für ACM Zertifikat-Tags:

- Die maximale Anzahl von Tags pro ACM Zertifikat beträgt 50.
- Die maximale Länge eines Tag-Schlüssels beträgt 127 Zeichen.
- Die maximale Länge eines Tag-Werts beträgt 255 Zeichen.

- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Das `aws :` Präfix ist reserviert für AWS verwenden; Sie können keine Tags hinzufügen, bearbeiten oder löschen, deren Schlüssel mit `beginntaws :` Tags, die mit `beginnen`, werden `aws :` nicht auf Ihr `tags-per-resource` Kontingent angerechnet.
- Wenn Sie das Tagging-Schema für mehrere Services und Ressourcen verwenden möchten, denken Sie daran, dass andere Services möglicherweise andere Einschränkungen für zulässige Zeichen haben. Weitere Informationen finden Sie in der Dokumentation des jeweiligen Services.
- ACMZertifikat-Tags sind nicht für die Verwendung in der verfügbar AWS Management Console Die [Resource Groups und der Tag-Editor](#).

Für allgemeine Informationen über AWS Tag-Konventionen finden Sie unter [Tagging AWS Ressourcen](#).

Verwalten von Tags

Sie können Tags hinzufügen, bearbeiten und löschen, indem Sie AWS Management Console, die AWS Command Line Interface, oder der AWS Certificate Manager API.

Verwalten von Tags (Konsole)

Sie können das AWS Management Console um Tags hinzuzufügen, zu löschen oder zu bearbeiten. Sie können Tags auch in Spalten anzeigen.

Hinzufügen von Tags

Gehen Sie wie folgt vor, um Tags mithilfe der ACM Konsole hinzuzufügen.

So fügen Sie ein Tag zu einem Zertifikat hinzu (Konsole)

1. Melden Sie sich bei AWS Management Console und öffne das AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen Sie den Pfeil neben dem Zertifikat aus, die Sie taggen möchten.
3. Scrollen Sie im Detailbereich nach unten zu Tags.
4. Wählen Sie Edit und Add Tag.
5. Geben Sie einen Schlüssel und einen Wert für das Tag ein.
6. Wählen Sie Save (Speichern) aus.

Löschen von Markierungen

Gehen Sie wie folgt vor, um Tags mithilfe der ACM Konsole zu löschen.

So löschen Sie einen Tag (Konsole)

1. Melden Sie sich bei AWS Management Console und öffne das AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen Sie den Pfeil neben dem Zertifikat mit einem Tag, das Sie löschen möchten.
3. Scrollen Sie im Detailbereich nach unten zu Tags.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Wählen Sie X neben dem Tag, das Sie löschen möchten.
6. Wählen Sie Save (Speichern) aus.

Bearbeiten eines Tags

Gehen Sie wie folgt vor, um Tags mithilfe der ACM Konsole zu bearbeiten.

So bearbeiten Sie ein Tag (Konsole)

1. Melden Sie sich bei AWS Management Console und öffne das AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.
2. Wählen Sie den Pfeil neben dem Zertifikat aus, das Sie bearbeiten möchten.
3. Scrollen Sie im Detailbereich nach unten zu Tags.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Ändern Sie den Schlüssel oder Wert des Tags, das Sie ändern möchten.
6. Wählen Sie Save (Speichern) aus.

Anzeigen von Tags in Spalten

Gehen Sie wie folgt vor, um Tags in Spalten in der ACM Konsole anzuzeigen.

So zeigen Sie Tags in Spalten an (Konsole)

1. Melden Sie sich bei AWS Management Console und öffne das AWS Certificate Manager Konsole zu <https://console.aws.amazon.com/acm/Hause>.

2. Wählen Sie die Tags aus, die Sie als Spalten anzeigen möchten, indem Sie auf das Tool-Symbol



rechts oben in der Konsole klicken.

3. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie in einer Spalte anzeigen möchten.

Tags verwalten (CLI)

In den folgenden Themen erfahren Sie, wie Sie mithilfe von Tags hinzufügen, auflisten und löschen AWS CLI.

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

Tags verwalten (ACMAPI)

In den folgenden Themen erfahren Sie, wie Sie mithilfe von Tags hinzufügen, auflisten und löschen könnenAPI.

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

In ACM integrierte Services

AWS Certificate Manager unterstützt eine wachsende Anzahl von AWS Dienstleistungen. Sie können Ihr ACM Zertifikat oder Ihr privates nicht installieren AWS Private CA Zertifikat direkt auf Ihrem AWS basierte Website oder Anwendung.

Note

Öffentliche ACM Zertifikate können auf EC2 Amazon-Instances installiert werden, die mit einer [Nitro Enclave](#) verbunden sind, aber nicht mit anderen EC2 Amazon-Instances. Informationen zum Einrichten eines eigenständigen Webservers auf einer EC2 Amazon-Instance, die nicht mit einer Nitro Enclave verbunden ist, finden [Sie unter Tutorial: Einen LAMP Webserver auf Amazon Linux 2 installieren oder Tutorial: Einen LAMP Webserver mit Amazon Linux installieren. AMI](#)

ACMZertifikate werden von den folgenden Diensten unterstützt:

Elastic Load Balancing

Elastic Load Balancing verteilt Ihren eingehenden Anwendungsdatenverkehr automatisch auf mehrere EC2 Amazon-Instances. Es erkennt fehlerhafte Instances und leitet den Datenverkehr zu den funktionsfähigen Instances um, bis die fehlerhaften Instances wiederhergestellt sind. Elastic Load Balancing skaliert seine Kapazität zur Bearbeitung von Anfragen automatisch in Abhängigkeit vom eingehenden Datenverkehr. Weitere Informationen zu Elastic Load Balancing finden Sie im [Elastic Load Balancing-Entwicklerhandbuch](#).

Um sichere Inhalte überSSL/bereitzustellen, erfordern Load Balancer im AllgemeinenTLS, dass SSL TLS /-Zertifikate entweder auf dem Load Balancer oder der Back-End-Amazon-Instance installiert sind. EC2 ACMist in Elastic Load Balancing integriert, um ACM Zertifikate auf dem Load Balancer bereitzustellen. Weitere Informationen finden Sie unter [Create an Application Load Balancer](#).

Amazon CloudFront

Amazon CloudFront ist ein Webservice, der die Verteilung Ihrer dynamischen und statischen Webinhalte an Endnutzer beschleunigt, indem er Ihre Inhalte über ein weltweites Netzwerk von Edge-Standorten bereitstellt. Wenn ein Endbenutzer Inhalte anfordert, über die Sie bereitstellen CloudFront, wird der Benutzer an den Edge-Standort weitergeleitet, der die niedrigste Latenz

bietet. Auf diese Weise wird sichergestellt, dass die Inhalte mit der bestmöglichen Leistung bereitgestellt werden. Wenn sich der Inhalt derzeit an diesem Edge-Standort befindet, wird er CloudFront sofort zugestellt. Wenn sich der Inhalt derzeit nicht an diesem Edge-Standort befindet, CloudFront ruft er ihn vom Amazon S3 S3-Bucket oder Webserver ab, den Sie als endgültige Inhaltsquelle identifiziert haben. Weitere Informationen zu CloudFront finden Sie im [Amazon CloudFront Developer Guide](#).

Um sichere Inhalte überSSL/bereitzustellenTLS, CloudFront müssen SSL TLS /-Zertifikate entweder auf der CloudFront Distribution oder auf der gesicherten Inhaltsquelle installiert sein. ACM integriert CloudFront , um ACM Zertifikate auf der CloudFront Distribution bereitzustellen. Weitere Informationen finden Sie unter [Abrufen eines SSL TLS /-Zertifikats](#).

 Note

Um ein ACM Zertifikat mit verwenden zu können CloudFront, müssen Sie das Zertifikat in der Region USA Ost (Nord-Virginia) anfordern oder importieren.

Amazon Cognito

Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und Mobilanwendungen. Benutzer können sich direkt mit Ihrem anmelden AWS-Konto Anmeldeinformationen oder über Dritte wie Facebook, Amazon, Google oder Apple. Weitere Informationen zu Amazon Cognito erhalten Sie im [Entwicklerhandbuch von Amazon Cognito](#).

Wenn Sie einen Cognito-Benutzerpool für die Verwendung eines CloudFront Amazon-Proxys konfigurieren, CloudFront können Sie ein ACM Zertifikat einrichten, um die benutzerdefinierte Domain zu sichern. Beachten Sie in diesem Fall, dass Sie die Zuordnung zum Zertifikat entfernen müssen, CloudFront bevor Sie es löschen können.

AWS Elastic Beanstalk

Elastic Beanstalk unterstützt Sie bei der Bereitstellung und Verwaltung von Anwendungen in AWS Cloud, ohne sich Gedanken über die Infrastruktur machen zu müssen, auf der diese Anwendungen ausgeführt werden. AWS Elastic Beanstalk reduziert die Komplexität der Verwaltung. Sie laden Ihre Anwendung einfach hoch, und Elastic Beanstalk übernimmt automatisch Kapazitätsbereitstellung, Lastverteilung, Skalierung und Überwachung des Anwendungsstatus. Elastic Beanstalk verwendet den Elastic Load Balancing Dienst, um einen Load Balancer zu erstellen. Weitere Informationen zu Elastic Beanstalk finden Sie im [AWS Elastic Beanstalk Leitfaden für Entwickler](#).

Um ein Zertifikat auszuwählen, müssen Sie den Load Balancer für Ihre Anwendung in der Elastic Beanstalk-Konsole konfigurieren. Weitere Informationen finden Sie unter [Den Load Balancer Ihrer Elastic Beanstalk Beanstalk-Umgebung so konfigurieren](#), dass er beendet wird. HTTPS

AWS App Runner

App Runner ist ein AWS Service, der eine schnelle, einfache und kostengünstige Möglichkeit bietet, Quellcode oder ein Container-Image direkt in eine skalierbare und sichere Webanwendung in der AWS Wolke. Sie müssen sich nicht mit neuen Technologien auskennen, entscheiden, welchen Rechen dienst Sie verwenden möchten, oder wissen, wie Sie diese bereitstellen und konfigurieren AWS Ressourcen schätzen. Weitere Informationen zu App Runner finden Sie im [AWS App Runner Leitfaden für Entwickler](#).

Wenn Sie Ihrem App Runner-Dienst benutzerdefinierte Domainnamen zuordnen, erstellt App Runner intern Zertifikate, die die Domaingültigkeit verfolgen. Sie sind gespeichert in ACM. App Runner löscht diese Zertifikate sieben Tage lang nicht, nachdem eine Domain von Ihrem Dienst getrennt wurde oder nachdem der Dienst gelöscht wurde. Dieser gesamte Prozess ist automatisiert und Sie müssen keine Zertifikate selbst hinzufügen oder verwalten. Weitere Informationen finden Sie unter [Verwaltung benutzerdefinierter Domainnamen für einen App Runner-Dienst](#) im AWS App Runner Leitfaden für Entwickler.

API Amazon-Gateway

Mit der Verbreitung mobiler Geräte und dem Wachstum des Internet der Dinge (IoT) ist es immer üblicher geworden, Geräte zu entwickeln, APIs die für den Zugriff auf Daten und die Interaktion mit Backend-Systemen verwendet werden können AWS. Sie können API Gateway verwenden, um Ihre zu veröffentlichen, zu verwalten, zu überwachen und zu sichern APIs. Nachdem Sie Ihr API auf API Gateway bereitgestellt haben, können Sie [einen benutzerdefinierten Domainnamen einrichten](#), um den Zugriff darauf zu vereinfachen. Um einen benutzerdefinierten Domainnamen einzurichten, müssen Sie ein SSL TLS /-Zertifikat bereitstellen. Sie können ACM es verwenden, um das Zertifikat zu generieren oder zu importieren. Weitere Informationen zu Amazon API Gateway finden Sie im [Amazon API Gateway Developer Guide](#).

AWS Nitro-Enklaven

AWS Nitro Enclaves ist eine EC2 Amazon-Funktion, mit der Sie isolierte Ausführungsumgebungen, sogenannte Enklaven, aus Amazon-Instances erstellen können. EC2 Enklaven sind separate, gehärtete und stark eingeschränkte virtuelle Maschinen. Sie bieten nur sichere lokale Socket-Konnektivität mit ihrer übergeordneten Instance. Sie verfügen über keinen persistenten Speicher, keinen interaktiven Zugriff oder kein externes Netzwerk. Benutzer können

nicht auf eine Enklave zugreifen, und auf die Daten und Anwendungen SSH in der Enklave können die Prozesse, Anwendungen oder Benutzer der übergeordneten Instance nicht zugreifen (einschließlich Root oder Admin).

EC2Instanzen, die mit Nitro Enclaves verbunden sind, unterstützen Zertifikate. ACM Weitere Informationen finden Sie unter [AWS Certificate Manager für Nitro Enclaves](#).

 Note

Sie können ACM Zertifikate keiner EC2 Instanz zuordnen, die nicht mit einer Nitro Enclave verbunden ist.

AWS CloudFormation

AWS CloudFormation hilft Ihnen bei der Modellierung und Einrichtung Ihrer Amazon Web Services Services-Ressourcen. Sie erstellen eine Vorlage, die beschreibt AWS Ressourcen, die Sie verwenden möchten, wie Elastic Load Balancing oder API Gateway. Dann AWS CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie. Sie müssen sie nicht einzeln erstellen und konfigurieren AWS Ressourcen und finde heraus, was wovon abhängt; AWS CloudFormation kümmert sich um all das. ACMZertifikate sind als Vorlagenressource enthalten, was bedeutet, dass AWS CloudFormation kann ACM Zertifikate anfordern, die Sie mit verwenden können AWS Dienste, um sichere Verbindungen zu ermöglichen. Darüber hinaus sind ACM Zertifikate in vielen der AWS Ressourcen, mit denen Sie einrichten können AWS CloudFormation.

Allgemeine Informationen zu CloudFormation finden Sie im [AWS CloudFormation Benutzerleitfaden](#). Informationen zu ACM Ressourcen, die von unterstützt werden CloudFormation, finden Sie unter [AWS::CertificateManager: :Certificate](#).

Mit der leistungsstarken Automatisierung von AWS CloudFormation, es ist leicht, Ihr [Zertifikatskontingent](#) zu überschreiten, insbesondere bei neuen AWS Konten. Wir empfehlen Ihnen, die ACM [bewährten Methoden](#) zu befolgen für AWS CloudFormation.

 Note

Wenn Sie ein ACM Zertifikat erstellen mit AWS CloudFormation, der AWS CloudFormation Der Stapel verbleibt im Zustand CREATE_IN_PROGRESS. Alle weiteren Stack-Vorgänge werden verzögert, bis Sie auf die Anweisungen in der E-Mail für die

Zertifikatsvalidierung reagieren. Weitere Informationen finden Sie unter [Resource Failed to Stabilize During a Create, Update, or Delete Stack Operation](#).

AWS Amplify

Amplify ist eine Reihe von speziell entwickelten Tools und Funktionen, mit denen Frontend-Web- und Mobilentwickler schnell und einfach Full-Stack-Anwendungen erstellen können AWS. Amplify bietet zwei Dienste an: Amplify Hosting und Amplify Studio. Amplify Hosting bietet einen Git-basierten Workflow zum Hosten serverless Web-Apps mit kontinuierlicher Bereitstellung. Amplify Studio ist eine visuelle Entwicklungsumgebung, die die Erstellung skalierbarer Full-Stack-Web- und mobiler Apps vereinfacht. Verwenden Sie Studio, um Ihre Front-End-Benutzeroberfläche mit einer Reihe von ready-to-use UI-Komponenten zu erstellen, ein App-Backend zu erstellen und die beiden dann miteinander zu verbinden. Weitere Informationen zu Amplify finden Sie in der [AWS Amplify](#)-Benutzerhandbuch.

Wenn Sie eine benutzerdefinierte Domain mit Ihrer Anwendung verbinden, stellt die Amplify-Konsole ein ACM Zertifikat aus, um sie zu sichern.

OpenSearch Amazon-Dienst

Amazon OpenSearch Service ist eine Such- und Analyse-Engine für Anwendungsfälle wie Protokollanalysen, Anwendungsüberwachung in Echtzeit und Click-Stream-Analyse. Weitere Informationen finden Sie im [Amazon OpenSearch Service Developer Guide](#).

Wenn Sie einen OpenSearch Service-Cluster erstellen, der eine [benutzerdefinierte Domäne und einen Endpunkt](#) enthält, können ACM Sie damit dem zugehörigen Application Load Balancer ein Zertifikat bereitstellen.

AWS Network Firewall

AWS Network Firewall ist ein verwalteter Service, der es einfach macht, wichtige Netzwerkschutzmaßnahmen für all Ihre Amazon Virtual Private Clouds (VPCs) bereitzustellen. Weitere Informationen zur Network Firewall finden Sie in der [AWS Network Firewall Entwicklerhandbuch](#).

Die Netzwerk-Firewall-Firewall lässt sich ACM zur TLS Inspektion in sie integrieren. Wenn Sie die TLS Inspektion in der Network Firewall verwenden, müssen Sie ein ACM Zertifikat für die Entschlüsselung und erneute Verschlüsselung des SSL TLS /-Datenverkehrs konfigurieren, der Ihre Firewall durchläuft. Informationen darüber, wie die Network Firewall ACM zur TLS Inspektion

verwendet, finden Sie unter [Anforderungen für die Verwendung von SSL TLS /-Zertifikaten mit TLS Inspektionskonfigurationen](#) in der AWS Network Firewall Leitfaden für Entwickler.

Sicherheit bei AWS Certificate Manager

Cloud-Sicherheit bei AWS hat höchste Priorität. Als AWS Als Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung zwischen AWS und du. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die läuft AWS Dienstleistungen in der AWS Wolke. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheit im Rahmen der [AWS Compliance-Programme](#) . Um mehr über die Compliance-Programme zu erfahren, die gelten für AWS Certificate Manager, siehe [AWS Im Leistungsumfang aufgeschlüsselte Dienstleistungen nach Compliance-Programmen](#) .
- Sicherheit in der Cloud — Ihre Verantwortung wird bestimmt durch AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung anwenden können, wenn Sie AWS Certificate Manager (ACM). In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen ACM, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere verwenden AWS Dienste, die Ihnen helfen, Ihre ACM Ressourcen zu überwachen und zu sichern.

Themen

- [Datenschutz in AWS Certificate Manager](#)
- [Identity and Access Management für AWS Certificate Manager](#)
- [Resilienz in AWS Certificate Manager](#)
- [Sicherheit der Infrastruktur in AWS Certificate Manager](#)
- [Bewährte Methoden](#)

Datenschutz in AWS Certificate Manager

Das Tool AWS [Modell](#) der der gilt für den Datenschutz in AWS Certificate Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Sie sind auch verantwortlich für die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie in der [Datenschutzerklärung FAQ](#). Informationen zum Datenschutz in Europa finden Sie auf der [AWS Modell der geteilten Verantwortung und GDPR](#) Blogbeitrag auf der AWS Blog zum Thema Sicherheit.

Aus Datenschutzgründen empfehlen wir Ihnen, AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center or AWS Identity and Access Management (IAM). So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit zu kommunizieren AWS Ressourcen schützen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Für Informationen zur Verwendung von CloudTrail Pfaden zum Erfassen AWS Aktivitäten finden Sie unter [Arbeiten mit CloudTrail Pfaden](#) in der AWS CloudTrail Benutzerleitfaden.
- Verwenden Sie AWS Verschlüsselungslösungen, zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff FIPS 140-3 validierte kryptografische Module benötigen AWS über eine Befehlszeilenschnittstelle oder einen API, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dazu gehört auch, wenn Sie mit oder anderen arbeiten ACM AWS-Services mit der Konsole API, AWS CLI, oder AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine

URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Sicherheit für private Zertifikatsschlüssel

Wenn Sie [ein öffentliches Zertifikat anfordern](#), AWS Certificate Manager (ACM) generiert ein öffentliches/privates key pair. Für [importierte Zertifikate](#) generieren Sie das Schlüsselpaar. Der öffentliche Schlüssel wird Teil des Zertifikats. ACM speichert das Zertifikat und den entsprechenden privaten Schlüssel und verwendet AWS Key Management Service (AWS KMS), um den privaten Schlüssel zu schützen. Der Prozess funktioniert wie folgt:

1. Wenn Sie zum ersten Mal ein Zertifikat anfordern oder importieren AWS Region, ACM erstellt eine verwaltete AWS KMS key mit dem Alias `aws/acm`. Dieser KMS Schlüssel ist in jedem Fall einzigartig AWS Konto und jeder AWS Region.
2. ACM verwendet diesen KMS Schlüssel, um den privaten Schlüssel des Zertifikats zu verschlüsseln. ACM speichert nur eine verschlüsselte Version des privaten Schlüssels; ACM speichert den privaten Schlüssel nicht in Klartextform. ACM verwendet denselben KMS Schlüssel, um die privaten Schlüssel für alle Zertifikate in einem bestimmten AWS Konto und ein bestimmtes AWS Region.
3. Wenn Sie das Zertifikat einem Dienst zuordnen, der integriert ist AWS Certificate Manager, ACM sendet das Zertifikat und den verschlüsselten privaten Schlüssel an den Dienst. Ein Zuschuss wird auch in erstellt AWS KMS Dadurch kann der Dienst den Schlüssel verwenden, um den privaten KMS Schlüssel des Zertifikats zu entschlüsseln. Weitere Informationen zu Zuschüssen finden Sie unter [Verwendung von Zuschüssen](#) in der AWS Key Management Service Leitfaden für Entwickler. Weitere Informationen zu Diensten, die von unterstützt werden ACM, finden Sie unter [In ACM integrierte Services](#).

Note

Sie haben die Kontrolle über die automatisch erstellten AWS KMS gewähren. Wenn Sie diesen Zuschuss aus irgendeinem Grund löschen, verlieren Sie die ACM Funktionalität des integrierten Dienstes.

4. Integrierte Dienste verwenden den KMS Schlüssel, um den privaten Schlüssel zu entschlüsseln. Dann verwendet der Dienst das Zertifikat und den entschlüsselten privaten Schlüssel (Klartext), um sichere Kommunikationskanäle (SSL/TLS Sessions) mit seinen Clients einzurichten.

5. Wenn die Zuordnung eines Zertifikat von einem integrierten Service getrennt wird, wird die in Schritt 3 erstellte Berechtigung zurückgezogen. Das bedeutet, dass der Dienst den Schlüssel nicht mehr verwenden kann, um den privaten KMS Schlüssel des Zertifikats zu entschlüsseln.

Identity and Access Management für AWS Certificate Manager

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um ACM Ressourcen zu verwenden. IAM ist eine AWS-Service, die Sie ohne zusätzliche Kosten verwenden können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Certificate Manager funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#)
- [ACM-API-Berechtigungen: Referenztabelle für Aktionen und Ressourcen](#)
- [AWS Von verwaltete Richtlinien für AWS Certificate Manager](#)
- [Verwenden Sie Bedingungsstasten mit ACM](#)
- [Verwenden Sie eine dienstverknüpfte Rolle \(SLR\) mit ACM](#)
- [Fehlerbehebung bei AWS Certificate Manager Identität und Zugriff](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten ACM.

Service-Benutzer: Wenn Sie den ACM-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere ACM-Features ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter [Fehlerbehebung bei AWS Certificate Manager Identität und Zugriff](#) finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in ACM haben.

Service-Administrator: Wenn Sie in Ihrem Unternehmen für ACM-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf ACM. Es ist Ihre Aufgabe, zu bestimmen, auf welche ACM-Features und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen anschließend bei Ihrem IAM-Administrator entsprechende Änderungen für die Berechtigungen Ihrer Service-Benutzer anfordern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM zu verstehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit ACM verwenden kann, finden Sie unter [Wie AWS Certificate Manager funktioniert mit IAM](#).

IAM Administrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten ACM. Beispiele für identitätsbasierte ACM-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM Benutzerhandbuch unter [AWS Signature Version 4 für API Anfragen](#).

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise, die Multi-

Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center Benutzerhandbuch und [AWS Multi-Faktor-Authentifizierung IAM im IAM Benutzerhandbuch](#).

AWS-Konto Root-Benutzer

Wenn Sie ein neues AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAMBenutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen

Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich](#) sind.

Ein [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe einen Namen geben IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie im Benutzerhandbuch unter [Anwendungsfälle für IAM IAM Benutzer](#).

IAM-Rollen

Eine [IAMRolle](#) ist eine Identität innerhalb von Ihrem AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM Rolle in der zu übernehmen AWS Management Console, können Sie [von einem Benutzer zu einer IAM Rolle \(Konsole\) wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwenden URL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter [Methoden zur Übernahme einer Rolle](#) im IAM Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden [Sie im IAM Benutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter \(Federation\)](#). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff: Sie können eine IAM-Rolle verwenden, um jemandem (einem vertrauenswürdigen Prinzipal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAM Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Wenn Sie einige Dienste verwenden, führen Sie möglicherweise eine Aktion aus, die dann eine weitere Aktion in einem anderen Dienst auslöst. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgeschaltete Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle — Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).
- Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Das ist empfehlenswerter, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2 Instance eine AWS Rolle zuzuweisen und sie all ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Verwenden einer IAM Rolle, um Berechtigungen für Anwendungen zu erteilen, die auf EC2 Amazon-Instances ausgeführt werden](#).

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter [Überblick über JSON Richtlinien](#).

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie im Benutzerhandbuch unter [Definieren benutzerdefinierter IAM Berechtigungen mit vom Kunden verwalteten Richtlinien](#). IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie [wählen können, finden Sie im IAMBenutzerhandbuch unter Wählen Sie zwischen verwalteten Richtlinien und Inline-Richtlinien](#).

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten ACLs. Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAM Benutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAM Benutzerhandbuch unter [Berechtigungsgrenzen für IAM Entitäten](#).
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.
- **Richtlinien zur Ressourcenkontrolle (RCPs)** — RCPs sind JSON Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Sie RCP schränken die Berechtigungen für Ressourcen in Mitgliedskonten ein und können sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu OrganizationsRCPs, einschließlich einer Liste AWS-Services dieser Support-LeistungenRCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) im AWS Organizations Benutzerhandbuch.

- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im Benutzerhandbuch zu IAM.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie AWS Certificate Manager funktioniert mit IAM

Informieren Sie sich vor der Verwendung IAM zur Verwaltung des Zugriffs auf ACM, welche IAM Funktionen zur Verwendung verfügbar sind ACM.

IAM Funktionen, die Sie zusammen verwenden können AWS Certificate Manager

IAM-Feature	ACM-Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Teilweise

IAM-Feature	ACM-Support
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie ACM und wie andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter [AWS Dienste, die mit funktionieren](#).

Identitätsbasierte Richtlinien für ACM

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie im Benutzerhandbuch unter [Definieren benutzerdefinierter IAM Berechtigungen mit vom Kunden verwalteten Richtlinien](#). IAM

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der [Referenz zu IAM JSON Richtlinienelementen](#) im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für ACM

Beispiele für identitätsbasierte ACM-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#).

Ressourcenbasierte Richtlinien in ACM

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalidentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie [IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff](#).

Richtlinienaktionen für ACM

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Action Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der ACM-Aktionen finden Sie unter [Von AWS Certificate Manager definierte Aktionen](#) in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in ACM verwenden das folgende Präfix vor der Aktion:

```
acm
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte ACM-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#).

Richtlinienressourcen für ACM

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem [Amazon-Ressourcennamen \(ARN\)](#) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der ACM Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter [Ressourcen definiert von AWS Certificate Manager](#) in der Service Authorization Reference. Informationen

darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter [Aktionen definiert von AWS Certificate Manager](#).

Beispiele für identitätsbasierte ACM-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#).

Richtlinien-Bedingungsschlüssel für ACM

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMRichtlinienelemente: Variablen und Tags](#).

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontext-Schlüssel für AWS globale Bedingungen](#) im IAMBenutzerhandbuch.

Eine Liste von ACM-Bedingungsschlüsseln finden Sie unter [Bedingungsschlüssel für AWS Certificate Manager](#) in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Aktionen definiert von AWS Certificate Manager](#).

Beispiele für identitätsbasierte ACM-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager](#).

ACLs in ACM

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABAC mit ACM

Unterstützungen ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABAC ist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen dazu finden Sie ABAC unter [Definieren von Berechtigungen mit ABAC Autorisierung](#) im IAM Benutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter [Verwenden der attributbasierten Zugriffskontrolle \(ABAC\)](#). IAM

Verwenden temporärer Anmeldeinformationen mit ACM

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen [arbeiten können AWS-Services](#) , finden Sie [IAM im IAMBenutzerhandbuch unter Informationen zum Arbeiten mit](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum [Rollenwechsel finden Sie im Benutzerhandbuch unter Von einem Benutzer zu einer IAM Rolle \(Konsole\)](#) wechseln. IAM

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen unter IAM](#).

Serviceübergreifende Prinzipal-Berechtigungen für ACM

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Wenn Sie einige Dienste verwenden, führen Sie möglicherweise eine Aktion aus, die dann eine weitere Aktion in einem anderen Dienst auslöst. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgeschaltete Dienste zu stellen. FASANfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für ACM

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und

löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).

Warning

Die Änderung der Berechtigungen für eine Servicerolle kann die Funktionalität von ACM beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn ACM eine Anleitung dazu gibt.

Serviceverknüpfte Rollen für ACM

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter [AWS Dienste, die mit funktionieren](#). IAM Suchen Sie in der Tabelle nach einem Service mit einem Yes in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Certificate Manager

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, ACM-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. AWS API Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie mithilfe dieser Beispieldokumente zu JSON Richtlinien finden [Sie im IAMBenutzerhandbuch unter IAM Richtlinien erstellen \(Konsole\)](#).

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden ACM, einschließlich des Formats von ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Certificate Manager](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der ACM-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Auflisten von Zertifikaten](#)
- [Abrufen eines Zertifikats](#)
- [Importieren eines Zertifikats](#)
- [Löschen eines Zertifikats](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand ACM-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen](#).
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie [IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen](#). IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten

Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMJSONRichtlinienelemente: Bedingung](#).

- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtlinien Sprache (JSON) und den IAM bewährten Methoden entsprechen. IAM Access Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Überprüfen von Richtlinien mit IAM Access Analyzer](#).
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter [Sicherer API Zugriff mit MFA](#) im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter [Bewährte Sicherheitsmethoden IAM im IAM](#) Benutzerhandbuch. IAM

Verwenden der ACM-Konsole

Um auf die AWS Certificate Manager Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den ACM Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die ACM Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die ACM *AWSCertificateManagerReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie im [Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM](#) Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der Inline-Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. 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": "*"
    }
  ]
}
```

Auflisten von Zertifikaten

Mit der folgenden Richtlinie können Benutzer alle ACM-Zertifikate im Benutzerkonto auflisten.

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

Note

Diese Berechtigung ist erforderlich, damit ACM Zertifikate im Elastic Load Balancing und in den CloudFront Konsolen angezeigt werden.

Abrufen eines Zertifikats

Mit der folgenden Richtlinie können Benutzer ein bestimmtes ACM-Zertifikat abrufen.

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

Importieren eines Zertifikats

Mit der folgenden Richtlinie kann ein Benutzer ein Zertifikat importieren.

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

```
}  
}
```

Löschen eines Zertifikats

Mit der folgenden Richtlinie können Benutzer ein bestimmtes ACM-Zertifikat löschen.

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

ACM-API-Berechtigungen: Referenztabelle für Aktionen und Ressourcen

Wenn Sie die Zugriffskontrolle einrichten und Berechtigungsrichtlinien erstellen, die Sie einem IAM-Benutzer oder einer -Rolle anfügen können, verwenden Sie die folgende Tabelle als Referenz. Die erste Spalte in der Tabelle enthält jede AWS Certificate Manager-API-Operation. Sie geben Aktionen in einem Action-Element der Richtlinie an. Die restlichen Spalten enthalten die zusätzlichen Informationen:

Sie können die &IAM;-Richtlinienelemente in Ihren ACM-Richtlinien verwenden, um Bedingungen auszudrücken. Eine vollständige Liste finden Sie im Abschnitt [Available Keys](#) im IAM-Benutzerhandbuch.

Note

Um eine Aktion anzugeben, verwenden Sie das Präfix `acm:` gefolgt vom Namen der API-Operation (z. B. `acm:RequestCertificate`).

ACM-API-Operationen und -Berechtigungen

ACM-API-Operationen	Erforderliche Berechtigungen (API-Operationen)	Ressourcen
AddTagsToCertificate	acm:AddTagsToCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
DeleteCertificate	acm:DeleteCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
DescribeCertificate	acm:DescribeCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
ExportCertificate	acm:ExportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
GetAccountConfiguration	acm:GetAccountConfiguration	*
GetCertificate	acm:GetCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
ImportCertificate	acm:ImportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/* oder *
ListCertificates	acm:ListCertificates	*

ACM-API-Operationen	Erforderliche Berechtigungen (API-Operationen)	Ressourcen
ListTagsForCertificate	acm:ListTagsForCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
PutAccountConfiguration	acm:PutAccountConfiguration	*
RemoveTagsFromCertificate	acm:RemoveTagsFromCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
RequestCertificate	acm:RequestCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/* oder *
ResendValidationEmail	acm:ResendValidationEmail	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
UpdateCertificateOptions	acm:UpdateCertificateOptions	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>

AWS Von verwaltete Richtlinien für AWS Certificate Manager

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWSCertificateManagerReadOnly

Diese Richtlinie bietet schreibgeschützten Zugriff auf ACM-Zertifikate. Sie ermöglicht Benutzern, ACM-Zertifikate zu beschreiben, aufzulisten und abzurufen.

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

Zum Anzeigen dieser von AWS verwalteten Richtlinie in der Konsole gehen Sie zu <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly>.

AWSCertificateManagerFullAccess

Diese Richtlinie bietet vollständigen Zugriff auf alle ACM-Aktionen und -Ressourcen.

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

Zum Anzeigen dieser von AWS verwalteten Richtlinie in der Konsole gehen Sie zu <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess>.

ACM-Updates für AWS-verwaltete Richtlinien

Zeigen Sie Details zu den Aktualisierungen von AWS verwalteten Richtlinien für ACM an, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed auf der ACM [Dokumentverlauf](#)-Seite.

Änderung	Beschreibung	Datum
hinzugefügtGetAccountConfiguration - Unterstützung für AWSCertificateManagerReadOnly -Politik.	Die <code>AWSCertificateManagerReadOnly</code> -Richtlinie enthält jetzt die Berechtigung zum Aufrufen des <code>GetAccountConfiguration</code> API-Aktion	3. März 2021
ACM beginnt mit der Verfolgung von Änderungen	ACM beginnt mit der Verfolgung von Änderungen für AWS verwaltete Richtlinien.	3. März 2021

Verwenden Sie Bedingungstasten mit ACM

AWS Certificate Manager Verwendungszwecke AWS Identity and Access Management (IAM) [Bedingungsschlüssel](#), um den Zugriff auf Zertifikatsanfragen einzuschränken. Mit Bedingungsschlüsseln aus IAM Richtlinien oder Service Control-Richtlinien (SCP) können Sie Zertifikatsanforderungen erstellen, die den Richtlinien Ihrer Organisation entsprechen.

Note

Kombinieren Sie ACM Bedingungsschlüssel mit AWS [globale Bedingungsschlüssel](#) `aws:PrincipalArn`, um beispielsweise Aktionen weiter auf bestimmte Benutzer oder Rollen zu beschränken.

Unterstützte Bedingungen für ACM

ACMAPI Operationen und unterstützte Bedingungen

Bedingungsschlüssel	Unterstützte ACM API Operationen	Typ	Beschreibung
acm:ValidationMethod	RequestCertificate	Zeichenfolge (EMAIL, DNS)	Filtern Sie Anfragen auf der Grundlage der ACM Validierungsmethode
acm:DomainNames	RequestCertificate	ArrayOfString	Filtern Sie basierend auf den Domainnamen in der ACM Anfrage
acm:KeyAlgorithm	RequestCertificate	String	Filtern Sie Anfragen anhand des ACM Schlüsselalgorithmus und der Größe
acm:CertificateTransparencyLogging	RequestCertificate	Zeichenfolge (ENABLED, DISABLED)	Filtern Sie Anfragen anhand der Präferenz für die Protokollierung der ACM Zertifikatstransparenz
acm:CertificateAuthority	RequestCertificate	ARN	Filtern Sie Anfragen auf der Grundlage der in der ACM Anfrage enthaltenen Zertifizierungsstellen

Beispiel 1: Validierungsmethode einschränken

Die folgende Richtlinie verweigert neue Zertifikatsanträge, die die [E-Mail-Validierungsmethode](#) verwenden, mit Ausnahme von Anträgen, die über die `arn:aws:iam::123456789012:role/AllowedEmailValidation`-Rolle gestellt werden.

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

Beispiel 2: Platzhalter-Domains verhindern

Die folgende Richtlinie lehnt jede neue ACM Zertifikatsanforderung ab, die Platzhalterdomänen verwendet.

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

```

    ]
  }
}

```

Beispiel 3: Zertifikatsdomains einschränken

Die folgende Richtlinie lehnt jede neue ACM Zertifikatsanforderung für Domänen ab, die nicht mit enden `*.amazonaws.com`

```

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

```

Die Richtlinie kann weiter auf bestimmte Subdomains beschränkt werden. Diese Richtlinie würde nur Anfragen zulassen, bei denen jede Domain mit mindestens einem der bedingten Domainnamen übereinstimmt.

```

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

```

```

    }
  }
}

```

Beispiel 4: Schlüsselalgorithmus einschränken

Die folgende Richtlinie verwendet den Bedingungsschlüssel `StringNotLike`, um nur Zertifikate zuzulassen, die mit dem ECDSA 384-Bit-Schlüsselalgorithmus (`EC_secp384r1`) angefordert wurden.

```

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

```

Die folgende Richtlinie verwendet den Bedingungsschlüssel `StringLike` und den `*` Platzhalterabgleich, um zu verhindern, dass Anfragen nach neuen Zertifikaten ACM mit einem beliebigen RSA Schlüsselalgorithmus angefordert werden.

```

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

```

```

    }
  }
}

```

Beispiel 5: Zertifizierungsstelle einschränken

Die folgende Richtlinie würde nur Anfragen nach privaten Zertifikaten über die bereitgestellte private Zertifizierungsstelle (PCA) ARN zulassen.

```

{
  "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"
      }
    }
  }
}

```

Diese Richtlinie verwendet die Bedingung `acm:CertificateAuthority`, um nur Anfragen für öffentlich vertrauenswürdige Zertifikate zuzulassen, die von Amazon Trust Services ausgestellt wurden. Wenn Sie die Zertifizierungsstelle ARN auf einstellen, `false` wird verhindert, dass Anfragen nach privaten Zertifikaten von PCA.

```

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

```

```
    "acm:CertificateAuthority": "false"
  }
}
}
```

Verwenden Sie eine dienstverknüpfte Rolle (SLR) mit ACM

AWS Certificate Manager verwendet ein AWS Identity and Access Management (IAM) Eine [dienstbezogene Rolle](#), um die automatische Verlängerung von privaten Zertifikaten zu ermöglichen, die von einer privaten Zertifizierungsstelle ausgestellt wurden, für ein anderes Konto, das gemeinsam genutzt wird von AWS Resource Access Manager. Eine dienstbezogene Rolle (SLR) ist eine IAM Rolle, die direkt mit dem ACM Dienst verknüpft ist. SLRs sind von vordefiniert ACM und enthalten alle Berechtigungen, die der Dienst benötigt, um andere aufzurufen AWS Dienste in Ihrem Namen.

Das SLR ACM erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen für das unbeaufsichtigte Signieren von Zertifikaten nicht manuell hinzufügen müssen. ACM definiert die Berechtigungen von Its und ACM kann SLR, sofern nicht anders definiert, nur die Rolle übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

Informationen zu anderen Diensten, die dies unterstützen SLRs, finden Sie unter [AWS Dienste, die mit Diensten arbeiten, IAM](#) und suchen nach den Diensten, für die in der Spalte Serviceverknüpfte Rolle der Wert Ja steht. Wählen Sie Ja mit einem Link, um die SLR Dokumentation für diesen Dienst aufzurufen.

SLR Berechtigungen für ACM

ACM verwendet eine SLR benannte Amazon Certificate Manager Service Role Policy.

The AWS Service Role For Certificate Manager SLR vertraut darauf, dass die folgenden Dienste diese Rolle übernehmen:

- `acm.amazonaws.com`

Die Richtlinie für Rollenberechtigungen ACM ermöglicht es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktionen: `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` auf `"*"`

Sie müssen Berechtigungen konfigurieren, damit eine IAM Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine erstellen, bearbeiten oder löschen kann SLR. Weitere Informationen finden Sie unter [Berechtigungen für serviceverknüpfte Rollen](#) im IAM Benutzerhandbuch.

Important

ACM weist Sie möglicherweise darauf hin, dass nicht festgestellt werden kann, ob in Ihrem Konto eine SLR vorhanden ist. Wenn die erforderliche `iam:GetRole` Genehmigung ACM SLR für Ihr Konto bereits erteilt wurde, wird die Warnung nach der Erstellung des Kontos nicht erneut SLR angezeigt. Wenn sie erneut auftritt, müssen Sie oder Ihr Kontoadministrator möglicherweise die `iam:GetRole` Genehmigung für die von Ihnen verwaltete ACM Richtlinie erteilen oder Ihr Konto mit dieser verknüpfen ACM. `AWSCertificateManagerFullAccess`

Erstellen des für SLR ACM

Sie müssen das, das ACM verwendet SLR, nicht manuell erstellen. Wenn Sie ein ACM Zertifikat mit dem ausstellen AWS Management Console, der AWS CLI, oder der AWS API, ACM erstellt SLR für Sie beim ersten Mal eine private CA für ein anderes Konto, das gemeinsam genutzt wird von AWS RAM um Ihr Zertifikat zu signieren.

Wenn Sie auf Nachrichten stoßen, die besagen, dass ACM nicht festgestellt werden kann, ob ein auf Ihrem Konto SLR vorhanden ist, kann dies bedeuten, dass Ihr Konto keine Leseberechtigung erteilt hat AWS Private CA benötigt. Dadurch wird die SLR Installation nicht verhindert, und Sie können weiterhin Zertifikate ausstellen, aber ACM Sie können die Zertifikate nicht automatisch erneuern, bis Sie das Problem behoben haben. Weitere Informationen finden Sie unter [Probleme mit der ACM serviceverknüpften Rolle \(\) SLR](#).

Important

Dies SLR kann in Ihrem Konto angezeigt werden, wenn Sie eine Aktion in einem anderen Dienst abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet. Außerdem, wenn Sie den ACM Dienst vor dem 1. Januar 2017 genutzt haben, als er mit der Unterstützung begann SLRs, und dann die `AWSServiceRoleForCertificateManager` Rolle in Ihrem Konto ACM erstellt haben. Weitere Informationen finden Sie unter [Eine neue Rolle wurde in „Mein IAM Konto“](#) angezeigt.

Wenn Sie dies SLR löschen und es dann erneut erstellen müssen, können Sie eine der folgenden Methoden verwenden:

- Wählen Sie in der IAM Konsole Rolle, Rolle erstellen, Certificate Manager aus, um eine neue Rolle mit dem CertificateManagerServiceRolePolicyAnwendungsfall zu erstellen.
- Verwenden Sie den IAM API [CreateServiceLinkedRole](#) oder den entsprechenden AWS CLI Befehl [create-service-linked-role](#), erstellen Sie eine SLR mit dem `acm.amazonaws.com` Dienstnamen.

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer dienstbezogenen Rolle](#).

Bearbeiten des für SLR ACM

ACMerlaubt es Ihnen nicht, die mit dem AWSServiceRoleForCertificateManager Dienst verknüpfte Rolle zu bearbeiten. Nachdem Sie eine erstellt habenSLR, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können die Beschreibung der Rolle jedoch mithilfe von bearbeitenIAM. Weitere Informationen finden Sie unter [Bearbeiten einer dienstbezogenen Rolle](#) im IAMBenutzerhandbuch.

Löschen des für SLR ACM

Normalerweise müssen Sie das nicht löschen AWSServiceRoleForCertificateManager SLR. Sie können die Rolle jedoch manuell über die IAM Konsole löschen, AWS CLI oder das AWS API. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Löschen einer serviceverknüpften Rolle](#).

Unterstützte Regionen für ACM SLRs

ACMunterstützt die Verwendung SLRs in allen Regionen, in denen ACM sowohl als auch AWS Private CA sind verfügbar. Weitere Informationen finden Sie unter [AWS Regionen und Endpunkte](#).

Name der Region	Regions-ID	Support in ACM
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja

Name der Region	Regions-ID	Support in ACM
USA West (Oregon)	us-west-2	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Zürich)	eu-central-2	Ja
Europa (Irland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Paris)	eu-west-3	Ja
Südamerika (São Paulo)	sa-east-1	Ja
AWS GovCloud (US-West)	us-gov-west-1	Ja
AWS GovCloud (US-Ost) Ost	us-gov-east-1	Ja

Fehlerbehebung bei AWS Certificate Manager Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit ACM und IAM auftreten könnten.

Themen

- [Ich bin nicht autorisiert, eine Aktion in ACM auszuführen.](#)

- [Ich bin nicht berechtigt, ein Zertifikat in anfordern ACM](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine ACM Ressourcen ermöglichen](#)

Ich bin nicht autorisiert, eine Aktion in ACM auszuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der mateojackson IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *my-example-widget* Ressource anzuzeigen, aber nicht über die fiktiven *acm:GetWidget* Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer mateojackson aktualisiert werden, damit er mit der *acm:GetWidget*-Aktion auf die *my-example-widget*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, ein Zertifikat in anfordern ACM

Wenn Sie diesen Fehler erhalten, hat Ihr PKI Administrator ACM oder Ihr Administrator Regeln festgelegt, die Sie daran hindern, das Zertifikat in seinem aktuellen Status anzuordern.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer versucht, mithilfe der Konsole ein Zertifikat mithilfe von Optionen anzuordern, die DENY vom Organisationsadministrator mit a konfiguriert wurden.

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

In diesem Fall sollten Sie die Anfrage erneut stellen, und zwar so, dass sie den Richtlinien entspricht, die Ihr Administrator festgelegt hat. Oder die Richtlinie muss aktualisiert werden, damit das Zertifikat angefordert werden kann.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an ACM übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in ACM auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine ACM Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob ACM diese Features unterstützt, finden Sie unter [Wie AWS Certificate Manager funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im Benutzerhandbuch unter [Gewähren des Zugriffs IAM für einen Benutzer in einem anderen AWS-Konto, dem IAM Sie gehören](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund [gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

Resilienz in AWS Certificate Manager

Das Tool AWS Die globale Infrastruktur basiert auf AWS Regionen und Verfügbarkeitszonen. AWS -Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zur AWS Regionen und Verfügbarkeitszonen, siehe [AWS Globale Infrastruktur](#).

Sicherheit der Infrastruktur in AWS Certificate Manager

Als verwalteter Dienst AWS Certificate Manager ist geschützt durch AWS globale Netzwerksicherheit. Für Informationen über AWS Sicherheitsdienste und wie AWS schützt die Infrastruktur, siehe [AWS Cloud-Sicherheit](#). Um Ihre zu entwerfen AWS Umgebung, in der die besten Methoden für die Infrastruktursicherheit verwendet werden, finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Gut durchdachtes Framework.

Du verwendest AWS veröffentlichte API Aufrufe für den Zugriff ACM über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Oder Sie können das verwenden [AWS Security Token Service](#) (AWS STS), um temporäre Sicherheitsanmeldedaten zum Signieren von Anfragen zu generieren.

Gewährung des programmatischen Zugriffs auf ACM

Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb der AWS Management Console. Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt von der Art des Benutzers ab, der zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (In IAM Identity Center verwaltete Benutzer)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das zu signieren AWS CLI, AWS SDKs, oder AWS APIs.	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> Für den AWS CLI, siehe Konfiguration der AWS CLI zu verwenden AWS IAM Identity Center in der AWS Command Line Interface Benutzerleitfaden. Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. AWS SDKs, Tools und AWS APIs, siehe IAM Identity Center-Authentifizierung im AWS SDKsund Referenzhandbuch für Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen	Folgen Sie den Anweisungen unter Temporäre Anmeldeinformationen verwenden

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	an das zu signieren AWS CLI, AWS SDKs, oder AWS APIs.	mit AWS Ressourcen im IAMBenutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das zu signieren AWS CLI, AWS SDKs, oder AWS APIs.	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> • Für den AWS CLI, siehe Authentifizierung mit IAM Benutzeranmeldedaten in der AWS Command Line Interface Benutzerleitfaden. • Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. AWS SDKsund Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen in der AWS SDKsund Referenzhandbuch für Tools. • Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. AWS APIs, siehe Verwaltung von Zugriffsschlüsseln für IAM IAM Benutzer im Benutzerhandbuch.

Bewährte Methoden

Bewährte Verfahren sind Empfehlungen, die Ihnen bei der Verwendung helfen können AWS Certificate Manager (AWS Certificate Manager) effektiver. Die folgenden bewährten Methoden basieren auf realen Erfahrungen aktueller ACM Kunden.

Themen

- [Trennung auf Kontoebene](#)
- [AWS CloudFormation](#)
- [Zertifikat-Pinning](#)
- [Domaininvalidierung](#)
- [Hinzufügen oder Löschen von Domainnamen](#)
- [Abmelden von der Protokollierung für Zertifikatstransparenz](#)
- [Einschalten AWS CloudTrail](#)

Trennung auf Kontoebene

Verwenden Sie die Trennung auf Kontoebene in Ihren Richtlinien, um zu kontrollieren, wer auf Kontoebene auf Zertifikate zugreifen kann. Bewahren Sie Ihre Produktionszertifikate in separaten Konten auf als Ihre Test- und Entwicklungszertifikate. Wenn Sie die Trennung auf Kontoebene nicht verwenden können, können Sie den Zugriff auf bestimmte Rollen einschränken, indem Sie in Ihren Richtlinien `kms:CreateGrant` Aktionen verweigern. Dadurch wird eingeschränkt, welche Rollen in einem Konto Zertifikate auf hoher Ebene signieren können. Informationen zu Zuschüssen, einschließlich der Terminologie der Zuschüsse, finden Sie unter [Zuschüsse in AWS KMS](#) in der AWS Key Management Service Leitfaden für Entwickler.

Wenn Sie eine detailliertere Kontrolle wünschen, als die Verwendung von `kms:CreateGrant` nach Konto zu beschränken, können Sie die Verwendung von [kms: EncryptionContext](#) Condition Keys `kms:CreateGrant` auf bestimmte Zertifikate beschränken. Geben Sie `arn:aws:acm` als Schlüssel und den Wert von `an`, der eingeschränkt werden ARN soll. Die folgende Beispielrichtlinie verhindert die Verwendung eines bestimmten Zertifikats, erlaubt aber andere.

```
{
  "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

Mit AWS CloudFormation Sie können eine Vorlage erstellen, die beschreibt AWS Ressourcen, die Sie verwenden möchten. AWS CloudFormation stellt diese Ressourcen dann für Sie bereit und konfiguriert sie. AWS CloudFormation kann Ressourcen bereitstellen, die von ACM Elastic Load Balancing CloudFront, Amazon und Amazon API Gateway unterstützt werden. Weitere Informationen finden Sie unter [In ACM integrierte Services](#).

Wenn Sie verwenden AWS CloudFormation Um schnell mehrere Testumgebungen zu erstellen und zu löschen, empfehlen wir, nicht für jede Umgebung ein eigenes ACM Zertifikat zu erstellen. Dadurch wird Ihr Zertifikatkontingent schnell ausgeschöpft. Weitere Informationen finden Sie unter [Kontingente](#). Erstellen Sie stattdessen ein Platzhalter-Zertifikat für alle Domainnamen, die Sie für das Testen verwenden. Wenn Sie beispielsweise wiederholt ACM Zertifikate für Domainnamen erstellen, die sich nur durch eine Versionsnummer unterscheiden, wie `<version>.service.example.com`, erstellen Sie stattdessen ein einzelnes Platzhalterzertifikat für `<*>.service.example.com`. Fügen Sie das Platzhalterzertifikat in die Vorlage ein AWS CloudFormation verwendet, um Ihre Testumgebung zu erstellen.

Zertifikat-Pinning

Certificate Pinning, manchmal auch als SSL Pinning bezeichnet, ist ein Prozess, den Sie in Ihrer Anwendung verwenden können, um einen Remote-Host zu validieren, indem Sie diesen Host direkt seinem X.509-Zertifikat oder öffentlichen Schlüssel zuordnen und nicht einer Zertifikatshierarchie. Die Anwendung verwendet daher Pinning, um die Validierung der Zertifikatskette zu umgehenSSL. TLS Der typische SSL Validierungsprozess überprüft Signaturen in der gesamten Zertifikatskette, vom Stammzertifikat der Zertifizierungsstelle (CA) bis hin zu den untergeordneten CA-Zertifikaten, falls vorhanden. Außerdem überprüft er das Zertifikat für den Remote-Host unten in der Hierarchie. Ihre

Anwendung kann stattdessen an das Zertifikat für den Remote-Host pinnen, um zu vermitteln, dass nur das Zertifikat und nicht das Stammzertifikat oder ein anderes in der Kette vertrauenswürdig ist. Sie können Ihrer Anwendung während der Entwicklung das Zertifikat oder den öffentlichen Schlüssel des Remote-Hosts hinzufügen. Alternativ kann die Anwendung das Zertifikat oder den Schlüssel hinzufügen, wenn sie zum ersten Mal eine Verbindung mit dem Host einrichtet.

Warning

Wir empfehlen, dass Ihre Anwendung kein ACM Zertifikat anheftet. ACM führt [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#) dazu, dass Ihre von Amazon ausgestellten SSL TLS /-Zertifikate automatisch erneuert werden, bevor sie ablaufen. ACM generiert ein neues öffentlich-privates key pair, um ein Zertifikat zu erneuern. Wenn Ihre Anwendung das ACM Zertifikat als Pin festlegt und das Zertifikat erfolgreich mit einem neuen öffentlichen Schlüssel erneuert wurde, kann die Anwendung möglicherweise keine Verbindung zu Ihrer Domain herstellen.

Wenn Sie sich entscheiden, ein Zertifikat zu pinnen, hindern die folgenden Optionen Ihre Anwendung nicht daran, eine Verbindung zu Ihrer Domain herzustellen:

- [Importieren Sie Ihr eigenes Zertifikat](#) in ACM und heften Sie dann Ihre Anwendung an das importierte Zertifikat. ACM versucht nicht, importierte Zertifikate automatisch zu erneuern.
- Wenn Sie ein öffentliches Zertifikat verwenden, heften Sie Ihre Anwendung an alle verfügbaren [Amazon-Stammzertifikate](#) an. Wenn Sie ein privates Zertifikat verwenden, heften Sie Ihre Anwendung an das Stammzertifikat der Zertifizierungsstelle an.

Domaininvalidierung

Bevor die Amazon-Zertifizierungsstelle (CA) ein Zertifikat für Ihre Site ausstellen kann, AWS Certificate Manager (ACM) muss verifizieren, dass Sie Eigentümer oder Inhaber aller Domains sind, die Sie in Ihrer Anfrage angegeben haben. Sie können die Überprüfung entweder per E-Mail oder durchführen DNS. Weitere Informationen erhalten Sie unter [AWS Certificate Manager DNSValidierung](#) und [AWS Certificate Manager E-Mail-Validierung](#).

Hinzufügen oder Löschen von Domainnamen

Sie können einem vorhandenen ACM Zertifikat keine Domainnamen hinzufügen oder daraus entfernen. Stattdessen müssen Sie ein neues Zertifikat mit der überarbeiteten Liste der

Domainnamen anfordern. Beispiel: Wenn Ihr Zertifikat fünf Domainnamen hat und Sie vier weitere hinzufügen möchten, müssen Sie ein neues Zertifikat mit allen neun Domainnamen anfordern. Wie bei jedem neuen Zertifikat müssen Sie den Besitz aller Domainnamen in der Anforderung validieren, einschließlich der Namen, die Sie zuvor für das ursprüngliche Zertifikat validiert haben.

Wenn Sie eine E-Mail-Validierung verwenden, erhalten Sie für jede Domain bis zu 8 Validierungs-E-Mails, wobei mindestens eine innerhalb von 72 Stunden bearbeitet werden muss. Wenn Sie beispielsweise ein Zertifikat mit fünf Domainnamen anfordern, erhalten Sie bis zu 40 Validierungsnachrichten, wobei mindestens fünf innerhalb von 72 Stunden bearbeitet werden müssen. Da die Anzahl der Domainnamen in der Zertifikatsanforderung steigt, steigt auch der Arbeitsaufwand für die Validierung des Besitzes der Domain per E-Mail.

Wenn Sie stattdessen die DNS Validierung verwenden, müssen Sie für den DNS Datensatz, den FQDN Sie validieren möchten, einen neuen Datensatz in die Datenbank schreiben. ACMsendet Ihnen den zu erstellenden Datensatz und fragt später die Datenbank ab, um festzustellen, ob der Datensatz hinzugefügt wurde. Das Hinzufügen des Datensatzes garantiert, dass Sie die Domain besitzen oder kontrollieren. Wenn Sie im vorherigen Beispiel ein Zertifikat mit fünf Domainnamen anfordern, müssen Sie fünf DNS Datensätze erstellen. Wir empfehlen, wenn möglich die DNS Validierung zu verwenden.

Abmelden von der Protokollierung für Zertifikatstransparenz

Important

Unabhängig davon, welche Maßnahmen Sie ergreifen, um die Protokollierung der Zertifikatstransparenz zu deaktivieren, kann Ihr Zertifikat weiterhin von jedem Client oder jeder Person protokolliert werden, die Zugriff auf den öffentlichen oder privaten Endpunkt haben, an den Sie das Zertifikat binden. Das Zertifikat wird jedoch keinen signierten Zertifikatszeitstempel (SCT) enthalten. Nur die ausstellende Zertifizierungsstelle kann einen SCT in ein Zertifikat einbetten.

Seit dem 30. April 2018 vertraut Google Chrome öffentlichen SSL Zertifikaten bzw. Zertifikaten, die nicht in einem TLS Zertifikatstransparenzprotokoll aufgezeichnet sind, nicht mehr. Daher begann die Amazon CA ab dem 24. April 2018 mit der Veröffentlichung aller neuen Zertifikate und Verlängerungen in mindestens zwei öffentlichen Protokollen. Ein einmal protokolliertes Zertifikat kann nicht mehr entfernt werden. Weitere Informationen finden Sie unter [Protokollierung der Zertifikatstransparenz](#).

Die Protokollierung wird automatisch durchgeführt, wenn Sie ein Zertifikat anfordern oder wenn ein Zertifikat erneuert wird, aber Sie können sich dafür entscheiden, sie zu deaktivieren. Häufige Gründe dafür sind die Sorge um die Sicherheit und der Schutz der Privatsphäre. Beispielsweise gibt die Protokollierung interner Host-Domainnamen potenziellen Angreifern Informationen über interne Netzwerke, die ansonsten nicht öffentlich wären. Darüber hinaus könnte die Protokollierung die Namen neuer oder unveröffentlichter Produkte und Websites durchsickern lassen.

[Um die Transparenzprotokollierung zu deaktivieren, wenn Sie ein Zertifikat anfordern, verwenden Sie den `options` Parameter des `Request-Zertifikats` AWS CLI Befehl oder die `RequestCertificate` API-Operation.](#) Wenn Ihr Zertifikat vor dem 24. April 2018 ausgestellt wurde und Sie sicherstellen möchten, dass es bei der Verlängerung nicht protokolliert wird, können Sie den [`update-certificate-options`](#) Befehl oder den [`UpdateCertificateOptions`](#) API-Vorgang verwenden, um sich abzumelden.

Einschränkungen

- Sie können die -Protokollierung nicht aktivieren oder deaktivieren.
- Sie können den Protokollierungsstatus nicht ändern, nachdem ein Zertifikat seinen Verlängerungszeitraum eingegeben hat, normalerweise 60 Tage vor Ablauf des Zertifikats. Wenn eine Statusänderung fehlschlägt, wird keine Fehlermeldung generiert.

Ein einmal protokolliertes Zertifikat kann nicht mehr aus dem Protokoll entfernt werden. Ein Abmelden in diesem Zustand hat keine Wirkung. Wenn Sie sich bei der Anforderung eines Zertifikats von der Protokollierung abmelden und dann später wieder anmelden, wird Ihr Zertifikat erst dann protokolliert, wenn es erneuert wird. Wenn Sie möchten, dass das Zertifikat sofort protokolliert wird, empfehlen wir Ihnen, ein neues auszustellen.

Das folgende Beispiel zeigt Ihnen, wie Sie die Zertifikatstransparenz mit dem Befehl [`request-certificate`](#) deaktivieren, wenn Sie ein neues Zertifikat anfordern.

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

```

Der vorherige Befehl gibt das ARN Ihres neuen Zertifikats aus.

```
{
```

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

Wenn Sie bereits über ein Zertifikat verfügen und nicht möchten, dass es bei der Verlängerung protokolliert wird, verwenden Sie den [update-certificate-options](#) Befehl. Dieser Befehl gibt keinen Wert zurück.

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

Einschalten AWS CloudTrail

Schalten Sie die CloudTrail Protokollierung ein, bevor Sie mit der Verwendung beginnen ACM. CloudTrail ermöglicht es Ihnen, Ihre zu überwachen AWS Bereitstellungen durch Abrufen eines Verlaufs von AWS API Anrufe für Ihr Konto, einschließlich API Anrufe über AWS Management-Konsole, die AWS SDKs, das AWS Command Line Interface und Amazon Web Services auf höherer Ebene. Sie können auch feststellen, welche Benutzer und Konten angerufen haben ACM APIs, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. Sie können sie mithilfe von CloudTrail in Anwendungen integrieren API, die Erstellung von Trails für Ihr Unternehmen automatisieren, den Status Ihrer Trails überprüfen und kontrollieren, wie Administratoren die CloudTrail Anmeldung ein- und ausschalten. Weitere Informationen finden Sie unter [Erstellen eines Trails](#). Gehen Sie zu [Verwenden CloudTrail mit AWS Certificate Manager](#), um sich Beispielpfade für ACM Aktionen anzusehen.

Überwachen und protokollieren AWS Certificate Manager

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS Certificate Manager und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können.

In den folgenden Themen werden Tools zur AWS Cloud-Überwachung beschrieben, die zur Verwendung mit verfügbar sind. ACM

Themen

- [Amazon verwenden EventBridge](#)
- [Verwenden CloudTrail mit AWS Certificate Manager](#)
- [Unterstützte Metriken CloudWatch](#)

Amazon verwenden EventBridge

Sie können [Amazon EventBridge](#) (ehemals CloudWatch Events) verwenden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse von AWS Diensten, einschließlich ACM, werden nahezu EventBridge in Echtzeit an Amazon übermittelt. Sie können Ereignisse verwenden, um Ziele wie AWS Lambda Funktionen, AWS Batch Jobs, SNS Amazon-Themen und viele andere auszulösen. Weitere Informationen finden Sie unter [Was ist Amazon EventBridge?](#)

Themen

- [EventBridge Amazon-Unterstützung für ACM](#)
- [Auslösen von Aktionen mit Amazon EventBridge in ACM](#)

EventBridge Amazon-Unterstützung für ACM

In diesem Thema werden die ACM verwandten Veranstaltungen aufgeführt und beschrieben, die von Amazon unterstützt werden EventBridge.

ACMEreignis, bei dem das Zertifikat bald abläuft

ACM sendet ab 45 Tagen vor Ablauf tägliche Ablaufereignisse für alle aktiven Zertifikate (öffentlich, privat und importiert). Dieses Timing kann mit der [PutAccountConfiguration](#)-Aktion von geändert werden ACM API.

ACM leitet automatisch die Verlängerung berechtigter Zertifikate ein, die von ihr ausgestellt wurden. Importierte Zertifikate müssen jedoch vor Ablauf erneut ausgestellt und erneut importiert werden, um Ausfälle zu vermeiden. Weitere Informationen finden Sie unter [Erneuter Import eines öffentlichen Zertifikats](#). Sie können Ablaufereignisse verwenden, um die Automatisierung für den erneuten Import von Zertifikaten einzurichten. ACM Ein Beispiel für die Verwendung von Automatisierung finden Sie AWS Lambda unter [Auslösen von Aktionen mit Amazon EventBridge in ACM](#).

ACMEreignisse, die sich dem Ablauf eines Zertifikats nähern, haben die folgende Struktur.

```
{
  "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"
  }
}
```

ACMEreignis „Zertifikat abgelaufen“

Kunden können sich dieses Ereignis anhören, um sie zu benachrichtigen, wenn ein ACM ausgestellt öffentliches oder privates Zertifikat in ihrem Konto abläuft. Ereignisse „Zertifikat abgelaufen“ sind nicht für [importierte Zertifikate](#) oder für verwaltete Zertifikate verfügbar, die [nicht verlängert](#) werden können.

ACMEreignisse mit abgelaufenem Zertifikat haben die folgende Struktur.

```
{
```

```

"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
}
}

```

ACMEreignis „Zertifikat verfügbar“

Kunden können per Listener auf dieses Ereignis achten, um benachrichtigt zu werden, wenn ein verwaltetes öffentliches oder privates Zertifikat einsatzbereit ist. Das Ereignis wird bei Ausgabe, Verlängerung und Import veröffentlicht. Bei einem privaten Zertifikat muss der Kunde, sobald es verfügbar ist, immer noch Maßnahmen ergreifen, um es für Hosts bereitzustellen.

ACMDie Ereignisse „Zertifikat verfügbar“ haben die folgende Struktur.

```

{
  "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
  }
}

```

ACMAktion zur Zertifikatserneuerung (Ereignis erforderlich)

Note

Ereignisse „Aktion zur Zertifikatserneuerung erforderlich“ sind für [importierte Zertifikate](#) nicht verfügbar.

Kunden können per Listener auf dieses Ereignis achten, um benachrichtigt zu werden, wenn eine Kundenaktion erforderlich ist, bevor ein Zertifikat erneuert werden kann. Wenn ein Kunde beispielsweise CAA Datensätze hinzufügt, die die Verlängerung eines Zertifikats ACM verhindern, wird dieses Ereignis ACM veröffentlicht, wenn die automatische Verlängerung 45 Tage vor Ablauf fehlschlägt. Wenn der Kunde nichts ACM unternimmt, versucht er innerhalb von 30 Tagen, 15 Tagen, 3 Tagen und 1 Tag erneut zu verlängern, oder bis der Kunde Maßnahmen ergreift, läuft das Zertifikat ab oder das Zertifikat ist nicht mehr verlängerbar. Für jeden dieser Verlängerungsversuche wird ein Ereignis veröffentlicht.

ACMAktion zur Zertifikatserneuerung Erforderliche Ereignisse haben die folgende Struktur.

```

{
  "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 Gesundheitsereignisse

AWS Gesundheitsereignisse werden für ACM Zertifikate generiert, die verlängert werden können. Weitere Informationen zur Erneuerungsberechtigung finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

Zustandsereignisse werden in zwei Szenarien generiert:

- Bei erfolgreicher Erneuerung eines öffentlichen oder privaten Zertifikats.
- Wenn ein Kunde Maßnahmen ergreifen muss, damit eine Erneuerung stattfindet. Dies kann bedeuten, auf einen Link in einer E-Mail-Nachricht zu klicken (für per E-Mail validierte Zertifikate) oder einen Fehler zu beheben. Einer der folgenden Ereigniscodes ist in jedem Ereignis enthalten. Die Codes werden als Variablen angezeigt, die Sie zum Filtern verwenden können.
 - AWS_ACM_RENEWAL_STATE_CHANGE(das Zertifikat wurde erneuert, ist abgelaufen oder läuft ab)
 - CAA_CHECK_FAILURE(CAAPrüfung fehlgeschlagen)
 - AWS_ACM_RENEWAL_FAILURE(für von einer privaten Zertifizierungsstelle signierte externe Zertifikate)

Health Ereignisse haben die folgende Struktur. In diesem Beispiel wird für eine AWS_ACM_RENEWAL_STATE_CHANGE-Ereignis generiert wurde.

```
{
```

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

Auslösen von Aktionen mit Amazon EventBridge in ACM

Sie können EventBridge Amazon-Regeln auf der Grundlage dieser Ereignisse erstellen und die EventBridge Amazon-Konsole verwenden, um Aktionen zu konfigurieren, die ausgeführt werden, wenn die Ereignisse erkannt werden. Dieser Abschnitt enthält Beispielfahrer für die Konfiguration von EventBridge Amazon-Regeln und die daraus resultierenden Aktionen.

Themen

- [Mit Amazon auf ein Ereignis antworten SNS](#)
- [Reagieren auf ein Ereignis mit einer Lambda Funktion](#)

Mit Amazon auf ein Ereignis antworten SNS

In diesem Abschnitt wird gezeigt, wie Amazon so konfiguriert wird SNS, dass bei jedem Auftreten eines Gesundheitsereignisses ACM eine Textbenachrichtigung gesendet wird.

Führen Sie das folgende Verfahren durch, um eine Antwort zu konfigurieren.

Um eine EventBridge Amazon-Regel zu erstellen und eine Aktion auszulösen

1. Erstellen Sie eine EventBridge Amazon-Regel. Weitere Informationen finden Sie unter [EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren](#).

- a. Navigieren Sie in der EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/> zur Seite Ereignisse > Regeln und wählen Sie Regel erstellen aus.
- b. Klicken Sie auf der Regel erstellen Wählen Sie Ereignismusteraus.
- c. Für Service-Name, wählen Sie Integrität aus dem Menü.
- d. Für Ereignistyp, wählen Sie Spezifische Health Ereignisse aus.
- e. Wählen Sie Bestimmte (s) Service (s) aus und wählen Sie ACM aus dem Menü.
- f. Wählen Sie die Kategorie (n) für bestimmte Ereignistypen aus und wählen Sie accountNotification.
- g. Klicken Sie auf Jeder Ereignistypcode aus.
- h. Wählen Sie Irgendeine Ressource.
- i. Fügen Sie im Vorschau-Editor für JSON Ereignismuster das vom Ereignis ausgegebene Muster ein. In diesem Beispiel wird das Muster aus der [AWS Gesundheitsereignisse](#) Abschnitts erstellt.

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

2. Konfigurieren Sie eine Aktion.

Im Bereich Ziele können Sie aus vielen Diensten wählen, die Ihr Ereignis sofort verarbeiten können, z. B. Amazon Simple Notification Service (SNS), oder Sie können die Lambda-Funktion wählen, um das Ereignis an benutzerdefinierten ausführbaren Code weiterzuleiten. Für ein Beispiel eines AWS Lambda -Implementierung finden Sie unter [Reagieren auf ein Ereignis mit einer Lambda Funktion](#) aus.

Reagieren auf ein Ereignis mit einer Lambda Funktion

Dieses Verfahren zeigt, wie Sie AWS Lambda Amazon anhören EventBridge, Benachrichtigungen mit Amazon Simple Notification Service (SNS) erstellen und Ergebnisse veröffentlichen können AWS Security Hub, um Administratoren und Sicherheitsteams einen Überblick zu verschaffen.

So richten Sie eine Lambda-Funktion und IAM -Rolle ein

1. Konfigurieren Sie zunächst eine AWS Identity and Access Management (IAM) -Rolle und definieren Sie die Berechtigungen, die für die Lambda-Funktion benötigt werden. Diese bewährte Sicherheitspraxis bietet Ihnen Flexibilität bei der Festlegung, wer die Berechtigung zum Aufrufen der Funktion hat, und beim Beschränken der Berechtigungen, die dieser Person gewährt werden. Es wird nicht empfohlen, die meisten AWS Operationen direkt unter einem Benutzerkonto und insbesondere nicht unter einem Administratorkonto auszuführen.

Öffnen Sie die IAM Konsole unter <https://console.aws.amazon.com/iam/>.

2. Verwenden Sie den JSON Richtlinien-Editor, um die in der folgenden Vorlage definierte Richtlinie zu erstellen. Geben Sie Ihre eigene Region und Ihre AWS Kontodaten an. Weitere Informationen finden Sie [auf der JSON Registerkarte unter Richtlinien erstellen](#).

```
{
  "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. Erstellen Sie eine IAM Rolle und fügen Sie ihr die neue Richtlinie hinzu. Informationen zum Erstellen einer IAM Rolle und zum Anhängen einer Richtlinie finden Sie unter [Rolle für einen AWS Dienst erstellen \(Konsole\)](#).
4. Öffnen Sie die AWS Lambda Konsole unter <https://console.aws.amazon.com/lambda/>
5. So erstellen Sie die Lambda-Funktion: Weitere Informationen zur Verwendung von Lambda finden Sie unter [Erstellen einer Lambda-Funktion mit der Konsole](#). Führen Sie folgende Schritte aus:
 - a. Wählen Sie auf der Seite Create function die Option Author from scratch.
 - b. Geben Sie im Feld Funktionsname einen Namen wie handle-expiring-certificates "" ein.
 - c. Wählen Sie in der Liste Laufzeit „Python 3.8“.
 - d. Erweitern/Ändern der standardmäßigen Ausführungsrolle und wählen Sie Verwenden einer vorhandenen Rolle aus.
 - e. Wählen Sie in der Liste Existing role (Vorhandene Rolle) die oben erstellte Rolle aus.
 - f. Wählen Sie Funktion erstellen aus.
 - g. Fügen Sie unter Function code (Funktionscode) den folgenden Code ein.

```
# 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. **UNDERUMGEBUNGSVARIABLEN**, wählen Sie **Bearbeiten** und fügen Sie optional die folgenden Variablen hinzu.
 - (Optional) **EXPIRY _ DAYS**
 Gibt an, wie viel Vorlaufzeit in Tagen vor dem Versenden der Zertifikatablaufbenachrichtigung gesendet wird. Die Funktion ist standardmäßig 45 Tage, Sie können jedoch benutzerdefinierte Werte angeben.
 - (Fakultativ) **SNS _ TOPIC _ ARN**
 Gibt an ARN für einen Amazon SNS. Geben Sie die vollständige Datei ARN im Format `arn:aws:sns:an:<region>:<account-number>:<topic-name>`.
 - (Fakultativ) **_ _ SECURITY HUB REGION**
 Gibt eine AWS Security Hub in einer anderen Region an. Wenn dies nicht angegeben ist, wird die Region der laufenden Lambda Funktion verwendet. Wenn die Funktion in mehreren Regionen ausgeführt wird, ist es möglicherweise wünschenswert, dass alle Zertifikatnachrichten an den Security Hub in einer einzigen Region gesendet werden.
- i. Legen Sie unter **Basic settings** (Grundlegende Einstellungen) die Zeitüberschreitung unter **Timeout** auf 30 Sekunden fest.
- j. Wählen Sie oben auf der Seite **Deploy**.

Führen Sie die Aufgaben im folgenden Verfahren aus, um mit der Verwendung dieser Lösung zu beginnen.

So automatisieren Sie eine E-Mail-Benachrichtigung über das Ablaufdatum

In diesem Beispiel stellen wir für jedes abgelaufene Zertifikat eine einzige E-Mail bereit, sobald das Ereignis über Amazon EventBridge ausgelöst wird. Standardmäßig wird für ACM ein Zertifikat, das 45 Tage oder weniger vor Ablauf liegt, jeden Tag ein Ereignis ausgelöst. (Dieser Zeitraum kann mithilfe von [PutAccountConfiguration](#) angepasst werden ACM API.) Jedes dieser Ereignisse löst die folgende Kaskade automatisierter Aktionen aus:

```
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. Erstellen Sie die Lambda -Funktion und konfigurieren Sie Berechtigungen. (Bereits abgeschlossen — siehe [So richten Sie eine Lambda-Funktion und IAM -Rolle ein](#)) enthalten.
2. Erstellen Sie ein SNSStandardthema für die Lambda-Funktion, das zum Versenden von Benachrichtigungen verwendet werden soll. Weitere Informationen finden Sie unter [Ein SNS Amazon-Thema erstellen](#).
3. Abonnieren Sie das neue SNS Thema für alle Interessierten. Weitere Informationen finden Sie unter [Ein SNS Amazon-Thema abonnieren](#).
4. Erstellen Sie eine EventBridge Amazon-Regel, um die Lambda-Funktion auszulösen. Weitere Informationen finden Sie unter [EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren](#).

Navigieren Sie in der EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/> zur Seite Ereignisse > Regeln und wählen Sie Regel erstellen aus. Geben Sie Service-Name, Ereignistyp, und Lambda-Funktion an. In der Vorschau auf Ereignismuster Fügen Sie in folgenden Code ein:

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

Ein Ereignis wie Lambda empfängt, wird unter Beispielergebnis anzeigen:

```
{
  "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"
}
}
```

So bereinigen Sie

Wenn Sie die Beispielkonfiguration oder eine Konfiguration nicht mehr benötigen, empfiehlt es sich, alle Spuren davon zu entfernen, um Sicherheitsprobleme und unerwartete zukünftige Gebühren zu vermeiden:

- IAMRichtlinie und Rolle
- Lambda-Funktion
- CloudWatch Ereignisse herrschen
- CloudWatch Logs im Zusammenhang mit Lambda
- SNSThema

Verwenden CloudTrail mit AWS Certificate Manager

AWS Certificate Manager ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden ACM. CloudTrail ist in Ihrem AWS Konto standardmäßig aktiviert. CloudTrail erfasst API Aufrufe ACM als Ereignisse, einschließlich Aufrufe von der ACM Konsole und Codeaufrufen für die ACM API Operationen. Wenn Sie einen Trail konfigurieren, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für ACM. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen.

Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde ACM, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Informationen. Weitere Informationen finden Sie

unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#). Wenn unterstützte Ereignisaktivitäten in auftretenACM, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS - Konto herunterladen und dort suchen und anzeigen.

Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren.

Weitere Informationen CloudTrail dazu finden Sie in der folgenden Dokumentation:

- [AWS CloudTrail Benutzerleitfaden](#).
- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von SNS Amazon-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Themen

- [ACMAPIAktionen, die bei der CloudTrail Protokollierung unterstützt werden](#)
- [Protokollierung von API Aufrufen für integrierte Dienste](#)

ACMAPIAktionen, die bei der CloudTrail Protokollierung unterstützt werden

ACMunterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root-Benutzer des AWS-Kontos oder AWS Identity and Access Management (IAM) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie im [CloudTrail userIdentity Element](#).

Die folgenden Abschnitte enthalten Beispielprotokolle für die unterstützten API Operationen.

- [Hinzufügen von Tags zu einem ZertifikatAddTagsToCertificate](#)
- [Löschen eines ZertifikatsDeleteCertificate](#)
- [Beschreiben eines ZertifikatsDescribeCertificate](#)
- [Exportieren eines ZertifikatsExportCertificate](#)
- [Importieren eines Zertifikats \(ImportCertificate\)](#)
- [Auflisten von ACM-Zertifikaten](#)
- [Auflisten von Tags für ein ZertifikatListTagsForCertificate](#)
- [Entfernen von Tags aus einem ZertifikatRemoveTagsFromCertificate](#)
- [Anfordern eines ZertifikatsRequestCertificate](#)
- [Erneutes Senden einer Validierungs-E-MailResendValidationEmail](#)
- [Abrufen eines ZertifikatsGetCertificate](#)

Hinzufügen von Tags zu einem Zertifikat[AddTagsToCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an [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"
  }
]
}

```

Löschen eines Zertifikats [DeleteCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an die [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"
}
]
}

```

Beschreiben eines Zertifikats [DescribeCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an die [DescribeCertificate](#) API.

Note

Das CloudTrail Protokoll für den DescribeCertificate Vorgang enthält keine Informationen zu dem von Ihnen angegebenen ACM Zertifikat. Sie können Informationen über das Zertifikat in der Konsole AWS Command Line Interface, dem oder dem anzeigen [DescribeCertificate](#) API.

```

{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-03-18T00:00:42Z",
      "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"
  }
]
}

```

Exportieren eines Zertifikats [ExportCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs von [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
    ],
    "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"
    }
}
]
```

Importieren eines Zertifikats ([ImportCertificate](#))

Das folgende Beispiel zeigt den CloudTrail Protokolleintrag, der einen Aufruf des ACM [ImportCertificate](#) API Vorgangs aufzeichnet.

```
{
  "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"
}
```

Auflisten von ACM-Zertifikaten

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs von [ListCertificatesAPI](#).

Note

Das CloudTrail Protokoll für den ListCertificates Vorgang zeigt Ihre ACM Zertifikate nicht an. Sie können die Zertifikatsliste mit der Konsole AWS Command Line Interface, dem oder dem anzeigen [ListCertificatesAPI](#).

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

```

    "eventID": "cdfe1051-88aa-4aa3-8c33-a325270bff21",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }
]
}

```

Auflisten von Tags für ein Zertifikat [ListTagsForCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs von [ListTagsForCertificate](#) API.

Note

Das CloudTrail Protokoll für den `ListTagsForCertificate` Vorgang zeigt Ihre Tags nicht an. Sie können die Tagliste mit der Konsole AWS Command Line Interface, dem oder dem anzeigen [ListTagsForCertificate](#) API.

```

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

```

```
    "eventID": "32181be6-a4a0-48d3-8014-c0d972b5163b",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }
]
```

Entfernen von Tags aus einem Zertifikat [RemoveTagsFromCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs von [RemoveTagsFromCertificate](#) API.

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
      },
      "eventTime": "2016-04-06T14:10:01Z",
      "eventSource": "acm.amazonaws.com",
      "eventName": "RemoveTagsFromCertificate",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.10.16",
      "requestParameters": {
        "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012",
        "tags": [
          {
            "value": "Bob",
            "key": "Admin"
          }
        ]
      },
      "responseElements": null,
      "requestID": "40ded461-fc01-11e5-a747-85804766d6c9",
      "eventID": "0cfa142e-ef74-4b21-9515-47197780c424",
    }
  ]
}
```

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

Anfordern eines Zertifikats [RequestCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an die [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"
    }
]
}

```

Erneutes Senden einer Validierungs-E-Mail [ResendValidationEmail](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an die [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"
  }
]
}

```

Abrufen eines Zertifikats [GetCertificate](#)

Das folgende CloudTrail Beispiel zeigt die Ergebnisse eines Aufrufs an die [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"  
}  
]  
}
```

Protokollierung von API Aufrufen für integrierte Dienste

Sie können CloudTrail es verwenden, um API Aufrufe zu überprüfen, die von Diensten getätigt wurden, die in integriert sind ACM. Weitere Informationen zur Verwendung CloudTrail finden Sie im [AWS CloudTrail Benutzerhandbuch](#). Die folgenden Beispiele zeigen, welche Protokolltypen je nach den AWS Ressourcen, auf denen Sie das ACM Zertifikat bereitstellen, generiert werden können.

Themen

- [Erstellen eines Load Balancers](#)

Erstellen eines Load Balancers

Sie können CloudTrail es verwenden, um API Aufrufe zu prüfen, die von Diensten getätigt wurden, die in integriert sind ACM. Weitere Informationen zur Verwendung CloudTrail finden Sie im [AWS CloudTrail Benutzerhandbuch](#). Die folgenden Beispiele zeigen, welche Protokolltypen je nach den AWS Ressourcen, auf denen Sie das ACM Zertifikat bereitstellen, generiert werden können.

Themen

- [Erstellen eines Load Balancers](#)
- [Registrierung einer EC2 Amazon-Instance bei einem Load Balancer](#)
- [Verschlüsseln eines privaten Schlüssels](#)
- [Entschlüsseln eines privaten Schlüssels](#)

Erstellen eines Load Balancers

Das folgende Beispiel zeigt einen Aufruf der `CreateLoadBalancer` Funktion durch einen IAM Benutzer namens Alice. Der Name des Load Balancers lautet `TestLinuxDefault`, und der Listener wird mithilfe eines ACM Zertifikats erstellt.

```
{
  "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"
}
```

Registrierung einer EC2 Amazon-Instance bei einem Load Balancer

Wenn Sie Ihre Website oder Anwendung auf einer Amazon Elastic Compute Cloud (AmazonEC2)-Instance bereitstellen, muss der Load Balancer über diese Instance informiert werden. Dies kann über die Elastic Load Balancing-Konsole oder die AWS Command Line Interface erreicht werden. Das folgende Beispiel zeigt einen Aufruf `RegisterInstancesWithLoadBalancer` für einen Load Balancer mit dem Namen `LinuxTest 123456789012 AWS`.

```
{
  "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"
}

```

Verschlüsseln eines privaten Schlüssels

Das folgende Beispiel zeigt einen Encrypt Aufruf, der den privaten Schlüssel verschlüsselt, der einem Zertifikat zugeordnet ist. ACM Die Verschlüsselung erfolgt innerhalb von 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"
  }
]
}

```

Entschlüsseln eines privaten Schlüssels

Das folgende Beispiel zeigt einen Decrypt Aufruf, der den mit einem Zertifikat verknüpften privaten Schlüssel entschlüsselt. ACM Die Entschlüsselung erfolgt innerhalb des Geräts AWS, und der entschlüsselte Schlüssel wird nicht gelöscht. 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"
  }
}
```

Unterstützte Metriken CloudWatch

Amazon CloudWatch ist ein Überwachungsdienst für AWS Ressourcen. Sie können CloudWatch damit Kennzahlen sammeln und verfolgen, Alarme einrichten und automatisch auf Änderungen Ihrer AWS Ressourcen reagieren. ACM veröffentlicht bis zum Ablauf einmal täglich Metriken für jedes Zertifikat in einem Konto.

Der `AWS/CertificateManager`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung	Einheit	Dimensionen
DaysToExpiry	Anzahl der Tage, bis ein Zertifikat abläuft. ACM beendet die Veröffentlichung dieser Metrik, nachdem ein Zertifikat abgelaufen ist.	Ganzzahl	CertificateArn <ul style="list-style-type: none">Wert: ARN des Zertifikats

Weitere Informationen zu CloudWatch Metriken finden Sie in den folgenden Themen:

- [Amazon CloudWatch Metrics verwenden](#)
- [CloudWatchAmazon-Alarme erstellen](#)

Verwenden Sie AWS Certificate Manager mit dem SDK für Java

Sie können das AWS Certificate Manager API programmgesteuert mit dem Dienst zu interagieren, indem Anfragen gesendet HTTP werden. Weitere Informationen finden Sie hier: [AWS Certificate Manager API Referenz](#).

Zusätzlich zum Web API (oder HTTPAPI) können Sie die AWS SDKs und Befehlszeilentools zur Interaktion mit ACM und anderen Diensten. Weitere Informationen finden Sie unter [Tools für Amazon Web Services](#).

In den folgenden Themen erfahren Sie, wie Sie einen der folgenden verwenden AWS SDKs, der [AWS SDK for Java](#), um einige der verfügbaren Operationen in der AWS Certificate Manager API.

Themen

- [Hinzufügen von Tags zu einem Zertifikat](#)
- [Löschen eines Zertifikats](#)
- [Beschreiben eines Zertifikats](#)
- [Exportieren eines Zertifikats](#)
- [Ein Zertifikat und eine Zertifikatkette abrufen](#)
- [Importieren eines Zertifikats](#)
- [Auflisten von Zertifikaten](#)
- [Erneuern eines Zertifikats](#)
- [Auflisten von Zertifikat-Tags](#)
- [Entfernen von Tags aus einem Zertifikat](#)
- [Anfordern eines Zertifikats](#)
- [Erneutes Senden einer Validierungs-E-Mail](#)

Hinzufügen von Tags zu einem Zertifikat

Das folgende Beispiel zeigt, wie die [AddTagsToCertificate](#) Funktion verwendet wird.

```
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);
}
}

```

Löschen eines Zertifikats

Das folgende Beispiel zeigt, wie die [DeleteCertificate](#) Funktion verwendet wird. Im Erfolgsfall gibt die Funktion einen leeren Satz {} zurück.

```

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);

}
}
```

Beschreiben eines Zertifikats

Das folgende Beispiel zeigt, wie die [DescribeCertificate](#) Funktion verwendet wird.

```
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);

}
}
```

Im Erfolgsfall werden für das vorherige Beispiel Informationen der folgenden Art angezeigt.

```
{
  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,  
  }  
}
```

Exportieren eines Zertifikats

Das folgende Beispiel zeigt, wie die [ExportCertificate](#)-Funktion verwendet wird. Die Funktion exportiert ein privates Zertifikat, das von einer privaten Zertifizierungsstelle (CA) ausgestellt wurde, im Format PKCS #8. (Es ist nicht möglich, öffentliche Zertifikate zu exportieren, unabhängig davon, ob sie ACM ausgestellt oder importiert wurden.) Darüber hinaus exportiert sie die Zertifikatskette und den privaten Schlüssel. In diesem Beispiel wird die Passphrase für den Schlüssel in einer lokalen Datei gespeichert.

```
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();
}
}
```

Ein Zertifikat und eine Zertifikatkette abrufen

Das folgende Beispiel zeigt, wie die [GetCertificate](#) Funktion verwendet wird.

```
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);
}
}
```

Das vorherige Beispiel erstellt eine Ausgabe der folgenden Art.

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

Importieren eines Zertifikats

Das folgende Beispiel zeigt, wie die [ImportCertificate](#) Funktion verwendet wird.

```
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);
}
}
```

Auflisten von Zertifikaten

Das folgende Beispiel zeigt, wie die [ListCertificates](#) Funktion verwendet wird.

```
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);
  }
}
```

Das vorherige Beispiel erstellt eine Ausgabe der folgenden Art.

```
{
  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
  }
}]
}
```

Erneuern eines Zertifikats

Das folgende Beispiel zeigt, wie die [RenewCertificate](#) Funktion verwendet wird. Die Funktion erneuert ein privates Zertifikat, das von einer privaten Zertifizierungsstelle (CA) ausgestellt und mit der [ExportCertificate](#) Funktion exportiert wurde. Derzeit können nur exportierte private Zertifikate mit dieser Funktion erneuert werden. Um Ihr zu erneuern AWS Private CA Zertifikate mit ACM, Sie müssen dem ACM Dienstprinzipal zunächst die entsprechenden Berechtigungen erteilen. Weitere Informationen finden Sie unter [Zuweisen von Berechtigungen zur Zertifikatserneuerung an 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);
}
}
```

Auflisten von Zertifikat-Tags

Das folgende Beispiel zeigt, wie die [ListTagsForCertificate](#) Funktion verwendet wird.

```
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);
}
}
```

Das vorherige Beispiel erstellt eine Ausgabe der folgenden Art.

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

Entfernen von Tags aus einem Zertifikat

Das folgende Beispiel zeigt, wie die [RemoveTagsFromCertificate](#) Funktion verwendet wird.

```
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);
}
}
```

Anfordern eines Zertifikats

Das folgende Beispiel zeigt, wie die [RequestCertificate](#) Funktion verwendet wird.

```
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);

}
}
```

Das vorherige Beispiel erstellt eine Ausgabe der folgenden Art.

```
{CertificateArn:  
  arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

Erneutes Senden einer Validierungs-E-Mail

Das folgende Beispiel zeigt Ihnen, wie Sie die [ResendValidationEmail](#) Funktion verwenden.

```
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());  
  
    }  
}
```

Beim vorherigen Beispiel wird Ihre Validierungs-E-Mail erneut gesendet und eine leere Gruppe angezeigt.

Probleme beheben mit AWS Certificate Manager

Lesen Sie die folgenden Themen, falls Sie Probleme mit der folgenden Anwendung haben AWS Certificate Manager.

Note

Wenn Ihr Problem in diesem Abschnitt nicht behoben wird, empfehlen wir Ihnen, die [AWS Wissenszentrum](#).

Themen

- [Problembehandlung bei Zertifikatsanfragen](#)
- [Fehlerbehebung bei der Zertifikatsvalidierung](#)
- [Problembehandlung bei der verwalteten Zertifikatsverlä](#)
- [Beheben Sie andere Probleme](#)
- [Umgang mit Ausnahmen](#)

Problembehandlung bei Zertifikatsanfragen

Lesen Sie die folgenden Themen, falls Sie bei der Anforderung eines ACM Zertifikats auf Probleme stoßen.

Themen

- [Zeitüberschreitung bei der Zertifikatsanforderung](#)
- [Zertifikatsanforderung fehlgeschlagen](#)

Zeitüberschreitung bei der Zertifikatsanforderung

Bei ACM Zertifikatsanfragen läuft das Timeout ab, wenn sie nicht innerhalb von 72 Stunden validiert werden. Um diese Bedingung zu korrigieren, öffnen Sie die Konsole, suchen Sie den Datensatz für das Zertifikat, klicken Sie auf das Kontrollkästchen, wählen Sie **Aktionen**, und wählen Sie **Löschen** aus. Wählen Sie dann **Aktionen** und **Zertifikat anfordern**, um erneut zu beginnen. Weitere Informationen

finden Sie unter [AWS Certificate Manager DNSValidierung](#) oder [AWS Certificate Manager E-Mail-Validierung](#). Wir empfehlen Ihnen, wenn möglich, die DNS Validierung zu verwenden.

Zertifikatsanforderung fehlgeschlagen

Wenn Ihre Anfrage fehlschlägt ACM und Sie eine der folgenden Fehlermeldungen erhalten, folgen Sie den vorgeschlagenen Schritten, um das Problem zu beheben. Sie können eine fehlgeschlagene Zertifikatsanforderung nicht erneut übermitteln. Senden Sie nach Behebung des Problems eine neue Anforderung.

Themen

- [Fehlermeldung: Keine verfügbaren Kontakte](#)
- [Fehlermeldung: Zusätzliche Überprüfung erforderlich](#)
- [Fehlermeldung: Ungültige öffentliche Domain](#)
- [Fehlermeldung: Andere](#)

Fehlermeldung: Keine verfügbaren Kontakte

Sie haben bei der Anforderung eines Zertifikats die E-Mail-Validierung ausgewählt, ACM konnten aber keine E-Mail-Adresse finden, die Sie für die Validierung eines oder mehrerer der Domainnamen in der Anfrage verwenden könnten. Um dieses Problem zu beheben, können Sie einen der folgenden Schritte ausführen:

- Stellen Sie sicher, dass Ihre Domain so konfiguriert ist, dass sie E-Mails empfangen kann. Der Nameserver Ihrer Domain muss über einen Mail-Exchanger-Datensatz (MX-Eintrag) verfügen, damit ACM die E-Mail-Server wissen, wohin die [E-Mail zur Domainvalidierung](#) gesendet werden muss.

Es reicht aus, nur eine der vorstehenden Aufgaben auszuführen, um dieses Problem zu beheben. Sie müssen nicht beide durchführen. Nachdem Sie das Problem behoben haben, fordern Sie ein neues Zertifikat an.

Weitere Informationen darüber, wie Sie sicherstellen können, dass Sie E-Mails zur Domainvalidierung erhalten ACM, finden Sie unter [AWS Certificate Manager E-Mail-Validierung](#) oder [Kein Empfang der Validierungs-E-Mail](#). Wenn Sie diese Schritte befolgen und weiterhin die Meldung „Keine verfügbaren Kontakte“ erhalten, [melden Sie dies an AWS](#) damit wir es untersuchen können.

Fehlermeldung: Zusätzliche Überprüfung erforderlich

ACMbenötigt zusätzliche Informationen, um diese Zertifikatsanforderung zu bearbeiten. Dies geschieht als Betrugsschutzmaßnahme, z. B. wenn Ihre Domain unter den [Top 1 000 Websites von Alexa](#) rangiert. Um die erforderlichen Informationen bereitzustellen, wenden Sie sich über das [Support Center](#) an AWS Support. Wenn du keinen Supportplan hast, poste einen neuen Thread im [ACMDiskussionsforum](#).

Note

Sie können kein Zertifikat für Amazon-eigene Domainnamen, wie solche, die mit amazonaws.com, cloudfront.net oder elasticbeanstalk.com enden, anfordern.

Fehlermeldung: Ungültige öffentliche Domain

Ein oder mehrere Domainnamen in der Zertifikatsanforderung sind ungültig. Dies liegt in der Regel daran, dass ein Domainname in der Anforderung keine gültige Domain der obersten Ebene ist. Versuchen Sie erneut, ein Zertifikat anzufordern, korrigieren Sie sämtliche Rechtschreib- oder Tippfehler in der fehlgeschlagenen Anforderung und prüfen Sie, ob alle Domainnamen in der Anforderung für Domains der obersten Ebene gültig sind. Sie können beispielsweise kein ACM Zertifikat für example.invalidpublicdomain anfordern, da „invalidpublicdomain“ keine gültige Top-Level-Domain ist. Wenn Sie diesen Fehlergrund weiterhin erhalten, kontaktieren Sie das [Support-Center](#). [Wenn du keinen Supportplan hast, poste einen neuen Thread im Diskussionsforum. ACM](#)

Fehlermeldung: Andere

Dieser Fehler tritt in der Regel auf, wenn ein Tippfehler in einem oder mehreren Domainnamen in der Zertifikatsanforderung zu finden ist. Versuchen Sie erneut, ein Zertifikat anzufordern, und korrigieren Sie sämtliche Rechtschreib- oder Tippfehler in der fehlgeschlagenen Anforderung. Wenn Sie diese Fehlermeldung weiterhin erhalten, wenden Sie sich über das [Support Center](#) an AWS Support. Wenn du keinen Supportplan hast, poste einen neuen Thread im [ACMDiskussionsforum](#).

Fehlerbehebung bei der Zertifikatsvalidierung

Wenn der Status der ACM Zertifikatsanforderung „Überprüfung ausstehend“ lautet, wartet die Anfrage auf eine Bearbeitung durch Sie. Wenn Sie bei der Anforderung die E-Mail-Validierung ausgewählt haben, müssen Sie oder ein autorisierter Stellvertreter auf die E-Mail-Nachrichten bei der Validierung

reagieren. Diese Nachrichten wurden an die gängigen E-Mail-Adressen für die angeforderte Domain gesendet. Weitere Informationen finden Sie unter [AWS Certificate Manager E-Mail-Validierung](#). Wenn Sie sich für die DNS Validierung entschieden haben, müssen Sie den CNAME Datensatz, der für Sie ACM erstellt wurde, in Ihre DNS Datenbank schreiben. Weitere Informationen finden Sie unter [AWS Certificate Manager DNSValidierung](#).

Important

Sie müssen prüfen, ob Sie jeden der Domainnamen, den Sie in Ihre Zertifikatanforderung aufgenommen haben, besitzen oder kontrollieren. Wenn Sie die E-Mail-Validierung wählen, erhalten Sie E-Mail-Nachrichten für die Validierung jeder Domain. Ist dies nicht der Fall, lesen Sie nach unter [Kein Empfang der Validierungs-E-Mail](#). Wenn Sie sich für die DNS Validierung entschieden haben, müssen Sie für jede Domain einen CNAME Datensatz erstellen.

Note

Öffentliche ACM Zertifikate können auf EC2 Amazon-Instances installiert werden, die mit einer [Nitro Enclave](#) verbunden sind, aber nicht mit anderen EC2 Amazon-Instances. Informationen zum Einrichten eines eigenständigen Webserver auf einer EC2 Amazon-Instance, die nicht mit einer Nitro Enclave verbunden ist, finden [Sie unter Tutorial: Einen LAMP Webserver auf Amazon Linux 2 installieren oder Tutorial: Einen LAMP Webserver mit Amazon Linux installieren. AMI](#)

Wir empfehlen, dass Sie die DNS Validierung anstelle der E-Mail-Validierung verwenden.

Lesen Sie die folgenden Themen, falls Sie Probleme mit der Validierung haben.

Themen

- [Beheben Sie DNS Validierungsprobleme](#)
- [Beheben von E-Mail-Validierungsproblemen](#)

Beheben Sie DNS Validierungsprobleme

Lesen Sie die folgenden Anleitungen, wenn Sie Probleme bei der Validierung eines Zertifikats mit haben. DNS

Der erste Schritt bei der DNS Fehlerbehebung besteht darin, den aktuellen Status Ihrer Domain mit Tools wie den folgenden zu überprüfen:

- dig — [Linux](#), [Windows](#)
- nslookup — [Linux](#), [Windows](#)
- whois — [Linux](#), [Windows](#)

Themen

- [Vom Anbieter verbotene Unterstriche DNS](#)
- [Vom Anbieter hinzugefügter Standardzeitraum DNS](#)
- [DNSDie Validierung bei schlägt GoDaddy fehl](#)
- [ACMIn der Konsole wird die Schaltfläche „Datensätze in Route 53 erstellen“ nicht angezeigt](#)
- [Route-53-Validierung schlägt in privaten \(nicht vertrauenswürdigen\) Domains fehl](#)
- [Die Validierung ist erfolgreich, aber die Ausstellung oder Verlängerung schlägt fehl](#)
- [Die Validierung schlägt für einen DNS Server auf einem fehl VPN](#)

Vom Anbieter verbotene Unterstriche DNS

Wenn Ihr DNS Anbieter führende Unterstriche in CNAME Werten verbietet, können Sie den Unterstrich aus dem ACM angegebenen Wert entfernen und Ihre Domain ohne ihn validieren. Zum Beispiel `_x2.acm-validations.aws` kann der CNAME Wert zu Validierungszwecken in geändert werden `x2.acm-validations.aws`. Der CNAME Namensparameter muss jedoch immer mit einem führenden Unterstrich beginnen.

Sie können einen der Werte auf der rechten Seite der Tabelle unten verwenden, um eine Domain zu validieren.

Name	Typ	Wert
<code>_<random value>.example.com.</code>	CNAME	<code>_<random value>.acm-validations.aws.</code>
<code><random value>.example.com.</code>	CNAME	<code><random value>.acm-validations.aws.</code>

Vom Anbieter hinzugefügter Standardzeitraum DNS

Einige DNS Anbieter fügen dem von Ihnen angegebenen CNAME Wert standardmäßig einen Nachzeitraum hinzu. Infolgedessen verursacht das Hinzufügen des Zeitraums selbst einen Fehler. Zum Beispiel "`<random_value>.acm-validations.aws.`" wird abgelehnt, während "`<random_value>.acm-validations.aws`" akzeptiert wird.

DNS Die Validierung bei schlägt GoDaddy fehl

DNS Die Validierung von Domains, die bei Godaddy und anderen Registrys registriert sind, schlägt möglicherweise fehl, sofern Sie die von angegebenen CNAME Werte nicht ändern. ACM Unter Verwendung von `example.com` als Domainname hat der ausgestellte CNAME Datensatz die folgende Form:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:
_cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

Sie können einen CNAME Datensatz erstellen, der kompatibel mit ist, GoDaddy indem Sie die Apex-Domain (einschließlich des Punkts) am Ende des NAME Felds wie folgt abschneiden:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:
_cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

ACM In der Konsole wird die Schaltfläche „Datensätze in Route 53 erstellen“ nicht angezeigt

Wenn Sie Amazon Route 53 als Ihren DNS Anbieter auswählen, AWS Certificate Manager kann direkt mit ihm interagieren, um Ihre Domain-Inhaberschaft zu bestätigen. Unter bestimmten Umständen ist die Schaltfläche Datensätze in Route 53 erstellen möglicherweise nicht verfügbar, wenn Sie es erwarten. Wenn dies der Fall ist, prüfen Sie auf folgende mögliche Ursachen.

- Sie verwenden Route 53 nicht als Ihren DNS Anbieter.
- Sie sind über verschiedene Konten bei Route 53 angemeldet ACM.
- Sie sind nicht IAM berechtigt, Datensätze in einer von Route 53 gehosteten Zone zu erstellen.
- Sie oder eine andere Person haben die Domain bereits validiert.
- Die Domain ist nicht öffentlich adressierbar.

Route-53-Validierung schlägt in privaten (nicht vertrauenswürdigen) Domains fehl

ACMSucht während der DNS Überprüfung nach einer CNAME in einer öffentlich gehosteten Zone. Wenn es keinen findet, wird eine Zeitüberschreitung nach 72 Stunden mit dem Status Validation timed out (Validierung abgelaufen) angezeigt. Sie können es nicht verwenden, um DNS Datensätze für private Domains zu hosten, einschließlich Ressourcen in einer VPC [privaten von Amazon gehosteten Zone](#), nicht vertrauenswürdigen Domains in Ihren privaten PKI Domänen und selbstsignierten Zertifikaten.

AWS bietet Unterstützung für öffentlich nicht vertrauenswürdige Domains über [AWS Private CA](#)Dienst.

Die Validierung ist erfolgreich, aber die Ausstellung oder Verlängerung schlägt fehl

Schlägt die Zertifikatsausstellung mit der Meldung „Ausstehende Validierung“ fehl, obwohl dies korrekt DNS ist, überprüfen Sie, ob die Ausstellung nicht durch einen Autorisierungsdatensatz der Zertifizierungsstelle () CAA blockiert wird. Weitere Informationen finden Sie unter [\(Optional\) Konfigurieren Sie einen Datensatz CAA](#).

Die Validierung schlägt für einen DNS Server auf einem fehl VPN

Wenn Sie einen DNS Server auf einem finden VPN und ein Zertifikat ACM nicht anhand dieses Zertifikats validieren können, überprüfen Sie, ob der Server öffentlich zugänglich ist. Die öffentliche Ausstellung von Zertifikaten mithilfe von ACM DNS Validierung setzt voraus, dass die Domaineinträge über das öffentliche Internet aufgelöst werden können.

Beheben von E-Mail-Validierungsproblemen

Lesen Sie bei Schwierigkeiten mit der Überprüfung einer Zertifikats-Domain per E-Mail die folgenden Hinweise.

Themen

- [Kein Empfang der Validierungs-E-Mail](#)
- [Persistenter anfänglicher Zeitstempel für die E-Mail-](#)
- [Ich kann nicht zur DNS Validierung wechseln](#)

Kein Empfang der Validierungs-E-Mail

Wenn Sie ein Zertifikat von anfordern ACM und sich für die E-Mail-Validierung entscheiden, wird eine E-Mail zur Domainvalidierung an die fünf gängigen Verwaltungsadressen gesendet. Weitere Informationen finden Sie unter [AWS Certificate Manager E-Mail-Validierung](#). Wenn Sie Probleme mit dem Empfang von Validierungs-E-Mails haben, sehen Sie sich folgende Vorschläge an.

Wo suchen ich nach der E-Mail?

ACMsendet Bestätigungs-E-Mail-Nachrichten an den von Ihnen angeforderten Domainnamen. Sie können auch eine Superdomain als Validierungsdomain angeben, wenn Sie diese E-Mails stattdessen unter dieser Domain erhalten möchten. Jede Subdomain bis zur minimalen Website-Adresse ist gültig und wird als Domain für die E-Mail-Adresse als Suffix nach @ verwendet. Sie können beispielsweise eine E-Mail an admin@example.com erhalten, wenn Sie example.com als Validierungsdomain für subdomain.example.com angeben. Sehen Sie sich die Liste der E-Mail-Adressen an, die in der ACM Konsole angezeigt werden (oder von oder zurückgegeben werdenAPI), um zu ermitteln, wo Sie nach der CLI Bestätigungs-E-Mail suchen sollten. Zum Anzeigen der Liste klicken Sie auf das Symbol neben dem Domainnamen im Textfeld mit der Bezeichnung Validation not complete.

Die E-Mail wird als Spam markiert

Überprüfen Sie, ob sich die Validierungs-E-Mail in Ihrem Spam-Ordner befindet.

GMailsortiert Ihre E-Mail automatisch

Wenn Sie verwendenGMail, wurde die Bestätigungs-E-Mail möglicherweise automatisch in die Tabs Updates oder Werbeaktionen sortiert.

Der Domainanbieter zeigt keine Kontaktinformationen an oder der Datenschutz ist aktiviert

Für Domains, die bei Route 53 erworben wurden, ist der Datenschutz standardmäßig aktiviert und Ihre E-Mail-Adresse wird einer whoisprivacyservice.org-, contact.gandi.net- oder identity-protect.org-E-Mail-Adresse zugeordnet. Stellen Sie sicher, dass Ihre beim Domainanbieter hinterlegte Registrant-E-Mail auf dem neuesten Stand ist, sodass die E-Mail, die an diese verdeckten E-Mail-Adressen gesendet wird, an eine E-Mail-Adresse weitergeleitet wird, die Sie kontrollieren können.

Note

Der Datenschutz für einige Domains, die Sie bei Route 53 kaufen, wird auch dann aktiviert, wenn Sie Ihre Kontaktdaten veröffentlichen möchten. So kann beispielsweise der

Datenschutz für die Top-Level-Domain `.ca` nicht programmatisch von Route 53 deaktiviert werden. Sie müssen sich an den [AWS Support Center](#) und fordern Sie an, dass der Datenschutz deaktiviert wird.

Nach der Bereitstellung mindestens einer der acht E-Mail-Adressen, an die AWS sendet eine Bestätigungs-E-Mail und bestätigt, dass Sie eine E-Mail für diese Adresse erhalten können. Sie sind bereit, über diese Adresse ein Zertifikat anzufordern ACM. Nachdem Sie eine Zertifikatsanforderung gestellt haben, stellen Sie sicher, dass die vorgesehene E-Mail-Adresse in der Liste der E-Mail-Adressen in der AWS Management Console. Solange sich das Zertifikat im Status „Überprüfung ausstehend“ befindet, können Sie die Liste erweitern, um es anzuzeigen, indem Sie auf das Symbol neben dem Domainnamen im Feld „Überprüfung nicht abgeschlossen“ klicken. Sie können die Liste auch unter Schritt 3: Validierung des Assistenten zum ACM Anfordern eines Zertifikats aufrufen. Die angezeigten E-Mail-Adressen sind diejenigen, an die E-Mail-Adresse gesendet wurde.

Wenden Sie sich an das Support-Center

Wenn Sie nach der Lektüre der obigen Hinweise immer noch keine E-Mail zur Domaininvalidierung erhalten, besuchen Sie bitte die [AWS Support Zentrieren Sie](#) und erstellen Sie einen Fall. Wenn Sie keine Support-Vereinbarung haben, posten Sie eine Nachricht im [ACMDiskussionsforum](#).

Persistenter anfänglicher Zeitstempel für die E-Mail-

Der Zeitstempel der ersten E-Mail-Validierungsanforderung eines Zertifikats bleibt über spätere Anforderungen für die Validierungsverlängerung bestehen. Dies ist kein Hinweis auf einen ACM Betriebsfehler.

Ich kann nicht zur DNS Validierung wechseln

Nachdem Sie ein Zertifikat mit E-Mail-Validierung erstellt haben, können Sie nicht zur Validierung mit DNS wechseln. Um die DNS Validierung zu verwenden, löschen Sie das Zertifikat und erstellen Sie dann ein neues Zertifikat, das DNS Validierung verwendet.

Problembehandlung bei der verwalteten Zertifikatsverlän

ACM versucht, Ihre ACM Zertifikate automatisch zu verlängern, bevor sie ablaufen, sodass Sie nichts unternehmen müssen. Wenn Sie Probleme mit [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#) haben, sehen Sie sich folgende Themen an.

Vorbereitung auf die automatische Domainvalidierung

Bevor ACM Sie Ihre Zertifikate automatisch verlängern können, muss Folgendes zutreffen:

- Ihr Zertifikat muss mit einem verknüpft sein AWS Dienst, der in integriert ist ACM. Informationen zu den Ressourcen, die ACM unterstützt werden, finden Sie unter [In ACM integrierte Services](#).
- Für per E-Mail validierte Zertifikate ACM muss es möglich sein, Sie unter einer Administrator-E-Mail-Adresse für jede in Ihrem Zertifikat aufgeführte Domain zu erreichen. Die E-Mail-Adressen, die ausprobiert werden, sind in [AWS Certificate Manager E-Mail-Validierung](#) gelistet.
- Stellen Sie DNS bei validierten Zertifikaten sicher, dass Ihre DNS Konfiguration die richtigen CNAME Datensätze enthält, wie unter beschrieben. [AWS Certificate Manager DNSValidierung](#)

Behandlung von Fehlern bei der Erneuerung verwalteter Zertifikate

Wenn das Zertifikat bald abläuft (60 Tage für DNS, 45 Tage für EMAIL und 60 Tage für Privat), wird ACM versucht, das Zertifikat zu verlängern, sofern es die [Zulassungskriterien](#) erfüllt. Möglicherweise müssen Sie Maßnahmen ergreifen, damit die Verlängerung erfolgreich ist. Weitere Informationen finden Sie unter [Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#).

Erneuerung verwalteter Zertifikate für per E-Mail validierte Zertifikate

ACMZertifikate sind 13 Monate (395 Tage) gültig. Die Verlängerung eines Zertifikats erfordert Maßnahmen des Domaininhabers. ACM beginnt 45 Tage vor Ablauf mit dem Senden von Verlängerungsmitteilungen an die mit der Domain verknüpften E-Mail-Adressen. Die Benachrichtigungen enthalten einen Link, auf den der Domaininhaber zur Verlängerung klicken kann. Sobald alle aufgelisteten Domains validiert sind ACM, wird ein erneuertes Zertifikat mit demselben ausgestellt ARN.

Unter [Per E-Mail validieren](#) finden Sie Anleitungen dazu, wie Sie die Domains identifizieren, die sich im Status PENDING_VALIDATION befinden, und wie Sie den Validierungsprozess für diese Domains wiederholen.

Verwaltete Zertifikatserneuerung für DNS -validierte Zertifikate

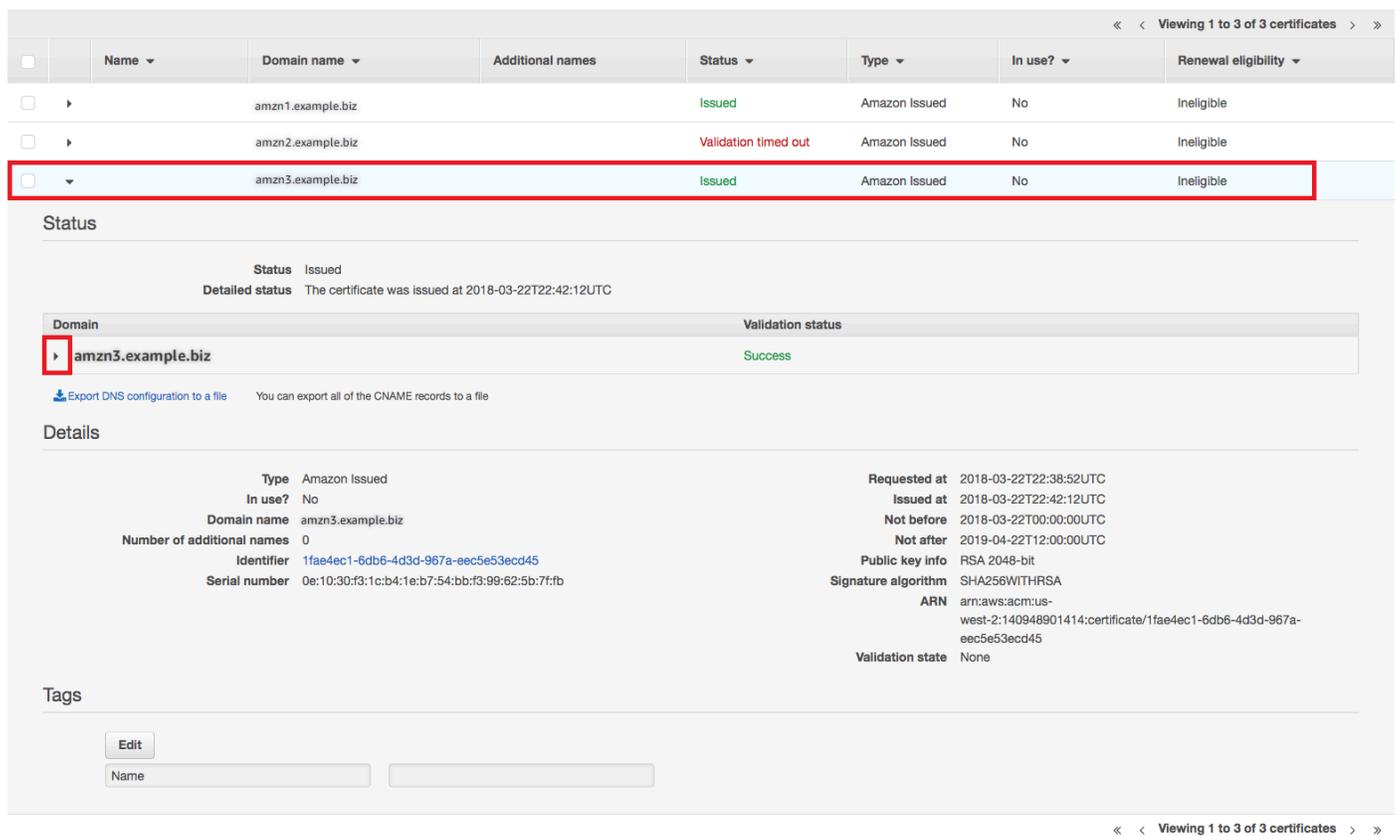
ACM versucht nicht, Zertifikate mit TLS DNS -validierter Gültigkeit zu validieren. Wenn ein ACM Zertifikat, das Sie mit DNS Validierung validiert haben, nicht erneuert werden kann, liegt das höchstwahrscheinlich an fehlenden oder ungenauen CNAME Datensätzen in Ihrer DNS

Konfiguration. In diesem Fall werden Sie ACM darüber informiert, dass das Zertifikat nicht automatisch erneuert werden konnte.

Important

Sie müssen die richtigen CNAME Datensätze in Ihre DNS Datenbank einfügen. Befragen Sie Ihren Domain-Registrierer, um dies zu tun.

Sie können die CNAME Datensätze für Ihre Domains finden, indem Sie Ihr Zertifikat und die zugehörigen Domaineinträge in der ACM Konsole erweitern. Details hierzu finden Sie in den folgenden Abbildungen. Sie können CNAME Datensätze auch abrufen, indem Sie den [DescribeCertificate](#) Vorgang in ACM API oder den Befehl `describe-certificate` in der verwenden. ACM CLI Weitere Informationen finden Sie unter [AWS Certificate Manager DNSValidierung](#).



The screenshot shows the AWS Certificate Manager console. At the top, there is a table listing certificates. The third row, for the certificate named 'amzn3.example.biz', is highlighted with a red border. Below the table, the 'Status' section shows the certificate is 'Issued' with a detailed status of 'The certificate was issued at 2018-03-22T22:42:12UTC'. The 'Domain' section shows 'amzn3.example.biz' with a 'Validation status' of 'Success'. The 'Details' section provides various metadata including 'Type: Amazon Issued', 'In use?: No', 'Domain name: amzn3.example.biz', 'Number of additional names: 0', 'Identifier: 1fae4ec1-6db6-4d3d-967a-ee5e53ecd45', 'Serial number: 0e:10:30:f3:1c:b4:1e:b7:54:bb:f3:99:62:5b:7f:fb', 'Requested at: 2018-03-22T22:38:52UTC', 'Issued at: 2018-03-22T22:42:12UTC', 'Not before: 2018-03-22T00:00:00UTC', 'Not after: 2019-04-22T12:00:00UTC', 'Public key info: RSA 2048-bit', 'Signature algorithm: SHA256WITHRSA', 'ARN: arn:aws:acm:us-west-2:140948901414:certificate/1fae4ec1-6db6-4d3d-967a-ee5e53ecd45', and 'Validation state: None'. At the bottom, there is a 'Tags' section with an 'Edit' button and a 'Name' input field.

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
amzn1.example.biz			Issued	Amazon Issued	No	Ineligible
amzn2.example.biz			Validation timed out	Amazon Issued	No	Ineligible
amzn3.example.biz			Issued	Amazon Issued	No	Ineligible

Status

Status: Issued
Detailed status: The certificate was issued at 2018-03-22T22:42:12UTC

Domain	Validation status
amzn3.example.biz	Success

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

Details

Type	Amazon Issued	Requested at	2018-03-22T22:38:52UTC
In use?	No	Issued at	2018-03-22T22:42:12UTC
Domain name	amzn3.example.biz	Not before	2018-03-22T00:00:00UTC
Number of additional names	0	Not after	2019-04-22T12:00:00UTC
Identifier	1fae4ec1-6db6-4d3d-967a-ee5e53ecd45	Public key info	RSA 2048-bit
Serial number	0e:10:30:f3:1c:b4:1e:b7:54:bb:f3:99:62:5b:7f:fb	Signature algorithm	SHA256WITHRSA
		ARN	arn:aws:acm:us-west-2:140948901414:certificate/1fae4ec1-6db6-4d3d-967a-ee5e53ecd45
		Validation state	None

Tags

Edit

Name

Wählen Sie in der Konsole das Zielzertifikat aus.

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

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

Erweitern Sie das Zertifikatsfenster, um die CNAME Informationen zum Zertifikat zu finden.

Wenn das Problem weiterhin besteht, nehmen Sie Kontakt mit dem [Support Center](#) auf.

Informationen zum Zeitpunkt der Erneuerung

[Verwaltete Zertifikatserneuerung in AWS Certificate Manager](#) ist ein asynchroner Prozess. Das bedeutet, dass die Schritte nicht unmittelbar hintereinander auftreten. Nachdem alle Domainnamen in einem ACM Zertifikat validiert wurden, kann es zu einer Verzögerung kommen, bis ACM das neue Zertifikat ausgestellt wird. Zwischen dem Erhalt des erneuerten ACM Zertifikats und der Bereitstellung des Zertifikats für AWS Ressourcen, die es verwenden. Daher kann es mehrere Stunden dauern, bis Änderungen am Zertifikatsstatus in der Konsole angezeigt werden.

Beheben Sie andere Probleme

Dieser Abschnitt enthält Anleitungen für Probleme, die nichts mit der Ausstellung oder Validierung von ACM Zertifikaten zu tun haben.

Themen

- [Probleme mit der Autorisierung durch die Zertifizierungsstelle \(CAA\)](#)
- [Zertifikatsimport](#)
- [Zertifikatsimport](#)
- [APIProbleme mit dem Gateway](#)
- [Was zu tun ist, wenn ein Arbeitszertifikat unerwartet fehlschlägt](#)
- [Probleme mit der ACM serviceverknüpften Rolle \(\) SLR](#)

Probleme mit der Autorisierung durch die Zertifizierungsstelle (CAA)

Sie können CAA DNS Datensätze verwenden, um anzugeben, dass die Amazon-Zertifizierungsstelle (CA) ACM Zertifikate für Ihre Domain oder Subdomain ausstellen kann. Wenn Sie bei der Zertifikatsausstellung eine Fehlermeldung erhalten, die besagt, dass ein oder mehrere Domainnamen aufgrund eines Autorisierungsfehlers (CAA) bei der Zertifizierungsstelle nicht validiert wurden, überprüfen Sie Ihre CAA DNS Aufzeichnungen. Wenn Sie diese Fehlermeldung erhalten, nachdem Ihre ACM Zertifikatsanforderung erfolgreich validiert wurde, müssen Sie Ihre CAA Daten aktualisieren und erneut ein Zertifikat anfordern. Das Wertfeld in Ihrem CAA Datensatz muss einen der folgenden Domainnamen enthalten:

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

Weitere Informationen zum Erstellen eines CAA Datensatzes finden Sie unter [\(Optional\) Konfigurieren Sie einen Datensatz CAA](#).

Note

Sie können sich dafür entscheiden, keinen CAA Eintrag für Ihre Domain zu konfigurieren, wenn Sie die CAA Überprüfung nicht aktivieren möchten.

Zertifikatsimport

Sie können Zertifikate von Drittanbietern in [integrierte Dienste](#) importieren ACM und sie diesen zuordnen. Wenn Probleme auftreten, lesen Sie in den Themen [Voraussetzungen](#) und [Zertifikatformat](#) nach. Beachten Sie insbesondere Folgendes:

- Sie können nur X.509 Version SSL TLS 3/-Zertifikate importieren.
- Ihr Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle (CA, Certificate Authority) signiert sein.
- Wenn Ihr Zertifikat von einer Zertifizierungsstelle signiert ist, müssen Sie eine Zwischenzertifikatkette einschließen, die einen Pfad zum Root of Authority bereitstellt.
- Wenn Ihr Zertifikat selbstsigniert ist, müssen Sie den privaten Schlüssel in Klartext einschließen.
- Jedes Zertifikat in der Kette muss jeweils direkt das vorhergehende Zertifikat zertifizieren.
- Fügen Sie Ihr Endentitätszertifikat nicht in die Zwischenzertifikatkette ein.
- Ihr Zertifikat, Ihre Zertifikatskette und Ihr privater Schlüssel (falls vorhanden) müssen PEM — codiert sein. Im Allgemeinen besteht die PEM Kodierung aus Base64-codierten Textblöcken, die mit ASCII Klartext-Kopf- und Fußzeilen beginnen und enden. Sie dürfen beim Kopieren oder Hochladen keine Zeilen oder Leerzeichen hinzufügen oder andere Änderungen an einer PEM Datei vornehmen. Sie können Zertifikatsketten mit dem [Open SSL Verify Utility überprüfen](#).
- Ihr privater Schlüssel (sofern vorhanden) darf nicht verschlüsselt sein. (Tipp: Wenn es eine Passphrase hat, ist sie verschlüsselt.)
- Dienste, die [in integriert](#) sind, ACM müssen Algorithmen und Schlüsselgrößen verwenden, die ACM unterstützt werden. Sehen Sie sich das an AWS Certificate Manager Das Benutzerhandbuch und die Dokumentation für jeden Dienst, um sicherzustellen, dass Ihr Zertifikat funktioniert.
- Die Unterstützung von Zertifikaten durch integrierte Dienste kann unterschiedlich sein, je nachdem, ob das Zertifikat in IAM oder in importiert wird ACM.
- Das Zertifikat muss gültig sein, wenn es importiert wird.
- Detaillierte Informationen über alle Ihre Zertifikate werden in der Konsole angezeigt. Standardmäßig jedoch, wenn Sie die [ListCertificates](#) API oder die [List-Zertifikate](#) aufrufen AWS CLI Befehl ohne Angabe des keyTypes Filters, es werden nur RSA_1024 oder RSA_2048 -Zertifikate angezeigt.

Zertifikatsimport

ACMGeneriert ein neues öffentlich-privates key pair, um ein Zertifikat zu erneuern. Wenn in Ihrer Anwendung ein [Zertifikat-Pinning](#) ACM Zertifikat angeheftet wird (manchmal auch als SSL Pinning bezeichnet), kann die Anwendung danach möglicherweise keine Verbindung zu Ihrer Domain herstellen AWS erneuert das Zertifikat. Aus diesem Grund empfehlen wir, dass Sie kein ACM Zertifikat anheften. Wenn Ihre Anwendung ein Zertifikat pinnen muss, können Sie folgende Schritte ausführen:

- [Importieren Sie Ihr eigenes Zertifikat in ACM](#) und heften Sie dann Ihre Anwendung an das importierte Zertifikat. ACMbietet keine verwaltete Verlängerung für importierte Zertifikate.
- Wenn Sie ein öffentliches Zertifikat verwenden, heften Sie Ihre Anwendung an alle verfügbaren [Amazon-Stammzertifikate](#) an. Wenn Sie ein privates Zertifikat verwenden, heften Sie Ihre Anwendung an das Stammzertifikat der Zertifizierungsstelle an.

APIProbleme mit dem Gateway

Wenn Sie einen Edge-optimierten API Endpunkt bereitstellen, richtet API Gateway eine CloudFront Verteilung für Sie ein. Die CloudFront Distribution gehört API Gateway, nicht Ihrem Konto. Die Distribution ist an das ACM Zertifikat gebunden, das Sie bei der Bereitstellung Ihres verwendet habenAPI. Um die Bindung zu entfernen und Ihr Zertifikat löschen ACM zu können, müssen Sie die benutzerdefinierte API Gateway-Domäne entfernen, die dem Zertifikat zugeordnet ist.

Wenn Sie einen regionalen API Endpunkt bereitstellen, erstellt API Gateway in Ihrem Namen einen Application Load Balancer (ALB). Der Load Balancer gehört API Gateway und ist für Sie nicht sichtbar. Das ALB ist an das ACM Zertifikat gebunden, das Sie bei der Bereitstellung Ihres API verwendet haben. Um die Bindung zu entfernen und das Löschen Ihres Zertifikats ACM zu ermöglichen, müssen Sie die benutzerdefinierte API Gateway-Domäne entfernen, die dem Zertifikat zugeordnet ist.

Was zu tun ist, wenn ein Arbeitszertifikat unerwartet fehlschlägt

Wenn Sie ein ACM Zertifikat erfolgreich einem integrierten Dienst zugeordnet haben, das Zertifikat aber nicht mehr funktioniert und der integrierte Dienst anfängt, Fehler zurückzugeben, kann dies an einer Änderung der Berechtigungen liegen, die der Dienst benötigt, um ein ACM Zertifikat verwenden zu können.

Elastic Load Balancing (ELB) benötigt beispielsweise die Erlaubnis zum Entschlüsseln eines AWS KMS key das wiederum entschlüsselt den privaten Schlüssel des Zertifikats. Diese Berechtigung wird durch eine ressourcenbasierte Richtlinie gewährt, die ACM gilt, wenn Sie ein Zertifikat mit verknüpfen. ELB Wenn die Erteilung für diese Berechtigung ELB verloren geht, schlägt sie beim nächsten Versuch, den Zertifikatsschlüssel zu entschlüsseln, fehl.

Um das Problem zu untersuchen, überprüfen Sie den Status Ihrer Zuschüsse mithilfe der AWS KMS Konsole unter <https://console.aws.amazon.com/kms>. Führen Sie dann eine der folgenden Aktionen durch:

- Wenn Sie der Meinung sind, dass Berechtigungen, die einem integrierten Dienst gewährt wurden, widerrufen wurden, besuchen Sie die Konsole des integrierten Dienstes, trennen Sie die Zuordnung des Zertifikats vom Dienst und verknüpfen Sie es dann erneut. Dadurch wird die ressourcenbasierte Politik erneut angewendet und ein neuer Zuschuss eingeführt.
- Wenn Sie der Meinung sind, dass erteilte Berechtigungen widerrufen ACM wurden, wenden Sie sich an AWS Support zu <https://console.aws.amazon.com/support/> Hause#/.

Probleme mit der ACM serviceverknüpften Rolle () SLR

Wenn Sie ein von einer privaten Zertifizierungsstelle signiertes Zertifikat ausstellen, das von einem anderen Konto mit Ihnen geteilt wurde, ACM versucht es beim ersten Mal, eine dienstverknüpfte Rolle (SLR) einzurichten, um als Principal mit einem zu interagieren AWS Private CA [ressourcenbasierte Zugriffsrichtlinie](#). Wenn Sie ein privates Zertifikat von einer gemeinsam genutzten Zertifizierungsstelle ausstellen und dieses nicht vorhanden SLR ist, ACM kann dieses Zertifikat nicht automatisch für Sie erneuert werden.

ACM weist Sie möglicherweise darauf hin, dass nicht festgestellt werden kann, ob auf Ihrem Konto ein SLR vorhanden ist. Wenn die erforderliche `iam:GetRole` Genehmigung ACM SLR für Ihr Konto bereits erteilt wurde, wird die Warnung nach der Erstellung des Kontos nicht erneut SLR angezeigt. Wenn sie erneut auftritt, müssen Sie oder Ihr Kontoadministrator möglicherweise die `iam:GetRole` Genehmigung für die von Ihnen verwaltete ACM Richtlinie erteilen oder Ihr Konto mit dieser verknüpfen ACM. `AWSCertificateManagerFullAccess`

Weitere Informationen finden Sie im Benutzerhandbuch unter [Berechtigungen für dienstbezogene Rollen](#). IAM

Umgang mit Ausnahmen

Importieren in `&S3`; AWS Certificate Manager Der Befehl kann aus verschiedenen Gründen fehlschlagen. Weitere Informationen zu den einzelnen Ausnahmen finden Sie in der folgenden Tabelle.

Umgang mit Ausnahmen bei privaten Zertifikaten

Die folgenden Ausnahmen können auftreten, wenn Sie versuchen, ein privates PKI Zertifikat zu erneuern, das ausgestellt wurde von AWS Private CA.

Note

AWS Private CA wird in den Regionen China (Peking) und China (Ningxia) nicht unterstützt.

ACM-Fehlercode	Kommentar
PCA_ACCESS_DENIED	<p>Die private Zertifizierungsstelle hat keine ACM Berechtigungen erteilt. Dies löst eine aus AWS Private CA AccessDeniedException Fehlercode.</p> <p>Um das Problem zu beheben, gewähren Sie dem ACM Dienstprinzipal die erforderlichen Berechtigungen mithilfe der AWS Private CA CreatePermission Betrieb.</p>
PCA_INVALID_DURATION	<p>Die Gültigkeitsdauer des angeforderten Zertifikats überschreitet die Gültigkeitsdauer der ausstellenden privaten CA. Dies löst eine aus AWS Private CA ValidationException Fehlercode.</p> <p>Um das Problem zu beheben, installieren Sie ein neues CA-Zertifikat mit einem entsprechenden Gültigkeitszeitraum.</p>

ACM-Fehlercode	Kommentar
PCA_INVALID_STATE	<p>Die aufgerufene private Zertifizierungsstelle befindet sich nicht im richtigen Zustand, um den angeforderten ACM Vorgang auszuführen. Dies löst eine <code>AWS Private CA InvalidStateException</code> Fehlercode.</p> <p>Beheben Sie das Problem wie folgt:</p> <ul style="list-style-type: none">• Wenn die Zertifizierungsstelle den Status <code>CREATING</code> angenommen hat, warten Sie, bis die Erstellung abgeschlossen ist, und installieren Sie das CA-Zertifikat.• Wenn die Zertifizierungsstelle den Status <code>PENDING_CERTIFICATE</code> angenommen hat, installieren Sie das CA-Zertifikat.• Wenn die Zertifizierungsstelle den Status <code>DISABLED</code> angenommen hat, aktualisieren Sie sie auf den Status <code>ACTIVE</code>.• Wenn die Zertifizierungsstelle den Status <code>DELETED</code> angenommen hat, stellen Sie sie wieder her.• Wenn die Zertifizierungsstelle den Status <code>EXPIRED</code> angenommen hat, installieren Sie ein neues Zertifikat• Wenn die CA den Status <code>FAILED</code> hat und Sie das Problem nicht lösen können, wenden Sie sich an AWS Support.

ACM-Fehlercode	Kommentar
PCA_LIMIT_EXCEEDED	<p>Die private Zertifizierungsstelle hat das Ausgabekontingent erreicht. Dies löst eine aus AWS Private CA <code>LimitExceededException</code> Fehlercode. Versuchen Sie, Ihre Anfrage zu wiederholen, bevor Sie mit dieser Hilfe fortfahren.</p> <p>Wenn der Fehler weiterhin besteht, wenden Sie sich an AWS Support um eine Erhöhung der Quote zu beantragen.</p>
PCA_REQUEST_FAILED	<p>Ein Netzwerk- oder Systemfehler ist aufgetreten. Dies löst eine aus AWS Private CA <code>RequestFailedException</code> Fehlercode. Versuchen Sie, Ihre Anfrage zu wiederholen, bevor Sie mit dieser Hilfe fortfahren.</p> <p>Wenn der Fehler weiterhin besteht, wenden Sie sich an AWS Support.</p>
PCA_RESOURCE_NOT_FOUND	<p>Die private Zertifizierungsstelle wurde endgültig gelöscht. Dies löst eine aus AWS Private CA <code>ResourceNotFoundException</code> Fehlercode. Stellen Sie sicher, dass Sie den richtigen <code>ARN</code> verwendet haben. Wenn dies fehlschlägt, können Sie diese Zertifizierungsstelle nicht verwenden.</p> <p>Um das Problem zu beheben, erstellen Sie eine neue Zertifizierungsstelle.</p>

ACM-Fehlercode	Kommentar
SLR_NOT_FOUND	<p>Um ein Zertifikat zu erneuern, das von einer privaten Zertifizierungsstelle signiert wurde, die sich in einem anderen Konto befindet, ist eine dienstverknüpfte Rolle (SLR) für das Konto ACM erforderlich, auf dem sich das Zertifikat befindet. Wenn Sie ein SLR gelöscht Objekt erneut erstellen müssen, finden Sie weitere Informationen unter. Erstellen des für SLR ACM</p>

Kontingente

Die folgenden AWS Certificate Manager (ACM) Servicekontingente gelten für jede AWS Region und jedes AWS Konto.

Welche Kontingente angepasst werden können, finden Sie in der [Tabelle mit den ACM Kontingenten](#) im AWS Allgemeinen Referenzhandbuch. Um Kontingenterhöhungen anzufordern, erstellen Sie einen Fall im [AWS Support Center](#).

Allgemeine Kontingente

Item	Standardkontingent
Anzahl der ACM-Zertifikate	2500
Abgelaufene und gesperrte Zertifikate werden weiterhin auf diese Summe angerechnet.	
Zertifikate, die von einer Zertifizierungsstelle von signiert wurden, zählen AWS Private CA nicht zu dieser Summe.	
Anzahl der ACM Zertifikate pro Jahr (letzte 365 Tage)	5,000
Sie können bis zu doppelt so viele ACM Zertifikate pro Jahr, Region und Konto anfordern. Wenn Ihr Kontingent beispielsweise 2.500 beträgt, können Sie bis zu 5.000 ACM Zertifikate pro Jahr in einer bestimmten Region und einem bestimmten Konto anfordern. Sie können zu einem Zeitpunkt nur 2.500 Zertifikate haben. Um 5.000 Zertifikate in einem Jahr anzufordern, müssen Sie im Verlauf des Jahres 2.500 löschen, damit Sie das Kontingent nicht überschreiten. Wenn Sie mehr als 2.500 Zertifikate zu einem bestimmten	

Item	Standardkontingent
<p>Zeitpunkt benötigen, müssen Sie sich an das AWS Support -Center wenden.</p> <p>Zertifikate, die von einer Zertifizierungsstelle von signiert wurden, zählen AWS Private CA nicht zu dieser Gesamtzahl.</p>	
Anzahl importierter Zertifikate	2.500
Anzahl der importierten Zertifikate pro Jahr (in den letzten 365 Tagen)	5,000

Item	Standardkontingent
<p data-bbox="110 222 753 260">Anzahl der Domainnamen pro ACM Zertifikat</p> <p data-bbox="110 302 792 436">Das Standardkontingent beträgt 10 Domainnamen für jedes ACM Zertifikat. Ihr Kontingent kann größer sein.</p> <p data-bbox="110 478 737 705">Der erste Domainname, den Sie einreichen, ist als der Subject Common Name (CN) des Zertifikats enthalten. Alle Namen sind in der Erweiterung "Subject Alternative Name" enthalten.</p> <p data-bbox="110 747 792 1264">Sie können bis zu 100 Domainnamen anfordern. Um eine Erhöhung Ihres Kontingents zu beantragen, erstellen Sie in der Service Quotas Quotas-Konsole eine Anfrage für den ACM Service. Bevor Sie einen Fall erstellen, stellen Sie sicher, dass Sie verstehen, wie durch das Hinzufügen weiterer Domainnamen mehr administrativer Aufwand für Sie entstehen kann, falls Sie eine E-Mail-Validierung verwenden. Weitere Informationen finden Sie unter Domaininvalidierung.</p> <p data-bbox="110 1306 776 1583">Das Kontingent für die Anzahl der Domainnamen pro ACM Zertifikat gilt nur für Zertifikate, die von bereitgestellt werdenACM. Dieses Kontingent gilt nicht für Zertifikate, in die Sie importierenACM. Die folgenden Abschnitte gelten nur für ACM Zertifikate.</p>	10

Item	Standardkontingent
<p>Anzahl der privaten CAs</p> <p>ACM ist in AWS Private Certificate Authority (AWS Private CA) integriert. Sie können die ACM Konsole oder verwenden AWS CLI, ACM API um private Zertifikate von einer bestehenden privaten Zertifizierungsstelle (CA) anzufordern, die von gehostet wird AWS Private CA. Diese Zertifikate werden innerhalb der ACM Umgebung verwaltet und unterliegen denselben Einschränkungen wie öffentliche Zertifikate, die von ausgestellt wurden ACM. Weitere Informationen finden Sie unter Fordern Sie ein privates Zertifikat an in AWS Certificate Manager. Mithilfe des eigenständigen AWS Private CA Dienstes können Sie auch private Zertifikate ausstellen. Weitere Informationen finden Sie unter Ausstellen eines privaten Endentitätszertifikats.</p> <p>Eine private CA, die gelöscht wurde, wird bis zum Ende ihres Wiederherstellungszeitraums auf Ihr Kontingent angerechnet. Weitere Informationen finden Sie unter Löschen Ihrer privaten CA.</p>	200
<p>Anzahl der privaten Zertifikate pro CA (Lebenszeit)</p>	1 000 000

APIKontingente bewerten

Die folgenden Kontingente gelten ACM API für jede Region und jedes Konto. ACM drosselt API Anfragen je nach Vorgang auf unterschiedliche Kontingente. API Drosselung bedeutet, dass eine ansonsten gültige Anfrage ACM zurückgewiesen wird, weil die Anforderung das Kontingent des Vorgangs für die Anzahl der Anfragen pro Sekunde überschreitet. Wenn eine Anforderung gedrosselt

wird, wird ein Fehler zurückgegeben. `ACM ThrottlingException` In der folgenden Tabelle sind die einzelnen API Operationen und das Kontingent aufgeführt, bei dem Anfragen für diesen Vorgang ACM gedrosselt werden.

 Note

Zusätzlich zu den in der Tabelle unten aufgeführten API Aktionen ACM kann die externe `IssueCertificate` Aktion auch von aufgerufen werden. AWS Private CA Informationen zu up-to-date Preiskontingenten finden Sie unter [Endpunkte und Kontingente](#) für AWS Private CA. `IssueCertificate`

Requests-per-second Kontingent für jeden Vorgang ACM API

API aufrufen	Anforderungen pro Sekunde
<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

API aufrufen	Anforderungen pro Sekunde
RequestCertificate	5
ResendValidationEmail	1
UpdateCertificateOptions	5

Weitere Informationen finden Sie unter [AWS Certificate Manager API Referenz](#).

Dokumentverlauf

In der folgenden Tabelle wird der Versionsverlauf der Dokumentation von beschriebenen AWS Certificate Manager ab 2018.

Änderung	Beschreibung	Datum
Die E-Mail-Validierung von Mail Exchanger (MX) wurde eingestellt	Die ACM Konsole unterstützt Mail Exchanger (MX) nicht mehr.	11. Juli 2024
Hinzufügung von Best Practices rund um die Trennung auf Kontoebene	Verwenden Sie in Ihren Richtlinien, wo immer dies möglich ist, eine Trennung auf Kontoebene. Falls nicht möglich, können Sie die Berechtigungen auf Kontoebene oder mithilfe von Bedingungsschlüsseln für den Verschlüsselungskontext in Ihren Richtlinien einschränken.	11. Juni 2024
Bevorstehende Einstellung der E-Mail-Verifizierung WHOIS	Es wurde ein Hinweis hinzugefügt, dass die WHOIS E-Mail-Verifizierung ab Juni 2024 nicht mehr unterstützt wird.	5. Februar 2024
Unterstützung für Bedingungsschlüssel hinzugefügt	Unterstützung für IAM Bedingungsschlüssel bei der Anforderung von ACM Zertifikaten wurde hinzugefügt. Eine Liste mit unterstützten Bedingungen finden Sie unter https://docs.aws.amazon.com/acm/latest/userguide/acm-	24. August 2023

<u>ECDSAUnterstützung hinzugefügt</u>	<u>conditions.html#acm-con ditions-supported.</u> Unterstützung für den Elliptic Curve Digital Signature Algorithm (ECDSA) wurde hinzugefügt, wenn ein öffentlic hes ACM Zertifikat angefordert wird. Eine Liste der gegenwärt ig unterstützten Schlüssel algorithmen finden Sie unter <u>https://docs.aws.amazon.com/ acm/latest/userguide/acm-certi ficate.html#algorithms.</u>	08. November 2022
<u>Neue Ereignisse CloudWatch</u>	Es wurden die Ereignisse „ACMZertifikat abgelaufen“, „ACMZertifikat verfügbar“ und „Aktion zur ACM Zertifika tserneuerung erforderlich“ hinzugefügt. Eine Liste der unterstützten CloudWate h Ereignisse finden Sie unter <u>https://docs.aws. amazon.com/acm/latest/us erguide/cloudwatch-events. html.</u>	27. Oktober 2022

[Aktualisieren von Schlüsselalgorithmustypen für den Import](#)

Zertifikate, in die importiert wurden, verfügen jetzt ACM möglicherweise über Schlüssel mit zusätzlichen Algorithmen RSA und Algorithmen für elliptische Kurven. Eine Liste der gegenwärtig unterstützten Schlüsselalgorithmen finden Sie unter <https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html> aus.

14. Juli 2021

[„Überwachen und Protokollieren“ wurde zu einem separaten Kapitel hochgestuft.](#)

Überwachungs- und Protokollierungsdokumentation in ein eigenes Kapitel verschoben. Diese Änderung umfasst CloudWatch Metriken, CloudWatch Events/ EventBridge und CloudTrail. Weitere Informationen finden Sie unter <https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html>.

23. März 2021

[Unterstützung für CloudWatch Metriken und Ereignisse hinzugefügt](#)

DaysToExpiry Metrik, Ereignis und Unterstützung hinzugefügt APIs. Weitere Informationen erhalten Sie unter <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html> und <https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html>.

3. März 2021

Unterstützung des kontoübergreifenden Support	Kontenübergreifende Unterstützung für die Verwendung von Private CAs From hinzugefügt AWS Private CA. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html .	17. August 2020
Zusätzlicher Support für Regionen	Unterstützung für Regionen hinzugefügt für AWS Regionen China (Peking und Ningxia). Eine vollständige Liste der unterstützten Regionen finden Sie unter https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region .	4. März 2020
Workflow-Tests zur Verlängerung	Kunden können die Konfiguration ihres ACM verwalteten Verlängerungsworkflows jetzt manuell testen. Weitere Informationen finden Sie unter Konfiguration für ACM verwaltete Verlängerungen von Testing .	14. März 2019
Protokollierung der Zertifikatstransparenz jetzt standardmäßig	Es wurde die Möglichkeit hinzugefügt, ACM öffentliche Zertifikate standardmäßig in Zertifikatstransparenzprotokollen zu veröffentlichen.	24. April 2018

[Wird gestartet AWS Private CA](#)

Einführung von ACM Private Certificate Manager (CM) und Erweiterung von AWS Certificate Manager Damit können Benutzer eine sichere verwaltete Infrastruktur für die Ausstellung und den Widerruf privater digitaler Zertifikate einrichten. Weitere Informationen finden Sie unter [AWS Private Zertifizierungsstelle](#).

4. April 2018

[Protokollierung der Zertifikatstransparenz](#)

Protokollierung der Zertifikatstransparenz unter „Bewährte Methoden“ wurde hinzugefügt.

27. März 2018

In der folgenden Tabelle wird der Versionsverlauf der Dokumentation von beschrieben AWS Certificate Manager vor 2018.

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer Inhalt	DNSValidierung hinzugefügt zu AWS Certificate Manager DNSValidierung .	21. November 2017
Neuer Inhalt	Verwenden Sie AWS Certificate Manager mit dem SDK für Java enthält neue Java-Code-Beispiele.	12. Oktober 2017
Neuer Inhalt	Es wurden Informationen zu CAA Datensätzen hinzugefügt (Optional Konfigurieren Sie einen Datensatz CAA).	21. September 2017
Neuer Inhalt	Informationen über .IO-Domains zu Probleme beheben mit	07. Juli 2017

Änderung	Beschreibung	Veröffentlichungsdatum
	AWS Certificate Manager hinzugefügt.	
Neuer Inhalt	Informationen über das erneute Importieren eines Zertifikats zu Importieren Sie ein Zertifikat erneut hinzugefügt.	07. Juli 2017
Neuer Inhalt	Informationen über das Zertifikat-Pinning zu Bewährte Methoden und zu Probleme beheben mit AWS Certificate Manager hinzugefügt.	07. Juli 2017
Neuer Inhalt	Hinzugefügt AWS CloudFormation zu In ACM integrierte Services .	27. Mai 2017
Aktualisierung	Weitere Informationen zu Kontingente hinzugefügt.	27. Mai 2017
Neuer Inhalt	Dokumentation zu Identity and Access Management für AWS Certificate Manager hinzugefügt.	28. April 2017
Aktualisierung	Eine Grafik wurde hinzugefügt, um anzuzeigen, wohin die Validierungs-E-Mail gesendet wird. Siehe AWS Certificate Manager E-Mail-Validierung .	21. April 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung	Informationen zum Einrichten von E-Mail für Ihre Domain hinzugefügt. Siehe AWS Certificate Manager E-Mail-Validierung .	6. April 2017
Aktualisierung	Informationen zum Prüfen des Zertifikatserneuerungs-Status in der Konsole hinzugefügt. Siehe Überprüfen des Erneuerungsstatus eines Zertifikats .	28. März 2017
Aktualisierung	Die Dokumentation zur Verwendung von Elastic Load Balancing wurde aktualisiert.	21. März 2017
Neuer Inhalt	Unterstützung hinzugefügt für AWS Elastic Beanstalk und Amazon API Gateway. Siehe In ACM integrierte Services .	21. März 2017
Aktualisierung	Dokumentation über Verwaltete Zertifikatserneuerung aktualisiert.	20. Februar 2017
Neuer Inhalt	Dokumentation zu Importierte Zertifikate hinzugefügt.	13. Oktober 2016
Neuer Inhalt	Hinzugefügt AWS CloudTrail Unterstützung für ACM Aktionen. Siehe Verwenden CloudTrail mit AWS Certificate Manager .	25. März 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neues Handbuch	Diese Version stellt vor AWS Certificate Manager.	21. Januar 2016

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.