



Guida per l'utente

# AWS Certificate Manager



Version 1.0

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

# AWS Certificate Manager: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

---

# Table of Contents

Che cos'è AWS Certificate Manager? .....	1
ACM è il servizio giusto per me? .....	1
Caratteristiche dei certificati ACM .....	2
Regioni supportate .....	8
Servizi integrati .....	8
Simboli di sito protetto e loghi di affidabilità .....	13
Quote .....	13
Quote generali .....	14
Quote tariffarie API .....	16
Prezzi .....	18
Sicurezza .....	19
Protezione dei dati .....	19
Sicurezza per le chiavi private dei certificati .....	20
Identity and Access Management .....	21
Destinatari .....	22
Autenticazione con identità .....	23
Gestione dell'accesso con policy .....	26
Funzionamento di AWS Certificate Manager con IAM .....	29
Esempi di policy basate su identità .....	36
Riferimento alle autorizzazioni dell'API ACM .....	41
Policy gestite da AWS .....	43
Utilizzo delle chiavi di condizione .....	46
Utilizzo di ruoli collegati ai servizi .....	51
Risoluzione dei problemi .....	55
Resilienza .....	57
Sicurezza dell'infrastruttura .....	57
Concessione dell'accesso programmatico ad ACM .....	58
Best practice .....	59
AWS CloudFormation .....	60
Associazione dei certificati .....	60
Convalida del dominio .....	61
Aggiunta o eliminazione di nomi di dominio .....	61
Annullamento della registrazione della trasparenza del certificato. ....	62
Attiva AWS CloudTrail .....	64

Configurazione .....	65
Registrarsi per creare un Account AWS .....	65
Creazione di un utente amministratore .....	66
Registrare un nome di dominio .....	67
(Facoltativo) Configurazione dell'e-mail .....	67
Database WHOIS .....	68
Registro MX .....	68
(Opzionale) Configurazione di una CAA .....	69
Emissione e gestione dei certificati .....	72
Richiesta di un certificato pubblico .....	73
Richiedere un certificato pubblico utilizzando la console .....	74
Richiesta di un certificato pubblico utilizzando CLI .....	76
Richiesta di un certificato PKI privato .....	77
Configurazione dell'accesso a una CA privata .....	78
Richiesta di un certificato PKI privato utilizzando la console ACM .....	79
Richiesta di un certificato PKI privato utilizzando la CLI .....	81
Convalidare la proprietà del dominio .....	82
Convalida DNS .....	84
Convalida e-mail .....	89
Elenco dei certificati .....	94
Descrivere i certificati .....	97
Eliminazione dei certificazioni .....	100
Installazione dei certificati ACM .....	101
Rinnovo gestito .....	103
Certificati pubblicamente attendibili .....	104
Convalida DNS .....	105
Convalida e-mail .....	105
Certificati PKI privati .....	106
Automatizzazione dell'esportazione dei certificati rinnovati .....	107
Testa il rinnovo gestito .....	109
Verifica dello stato di rinnovo .....	110
Controllo dello stato (console) .....	111
Controllo dello stato (API) .....	112
Controllo dello stato (CLI) .....	112
Controlla lo stato utilizzando Personal Health Dashboard (PHD) .....	112
Automatizzare la convalida via e-mail .....	114

Modelli di e-mail di convalida .....	114
Convalida di un nuovo certificato .....	114
Convalida di un certificato per il rinnovo .....	115
Flusso di lavoro di convalida .....	116
Importazione di certificati .....	118
Prerequisiti .....	119
Formato del certificato .....	120
Importa certificato .....	122
Importazione (console) .....	122
Importa (AWS CLI) .....	123
Reimportazione di un certificato .....	124
Reimportazione (console) .....	124
Reimportazione (AWS CLI) .....	125
Esportazione di un certificato .....	127
Esportazione di un certificato privato (console) .....	127
Esportazione di un certificato privato (CLI) .....	128
Aggiunta di tag ai certificati ACM .....	130
Limitazioni applicate ai tag .....	130
Gestione dei tag .....	131
Gestione dei tag (Console) .....	131
Gestione dei tag (CLI) .....	133
Gestione dei tag .....	133
Monitoraggio e registrazione .....	134
Amazon EventBridge .....	134
Eventi supportati .....	134
Esempio di azioni .....	139
CloudTrail .....	149
Operazioni API supportate .....	150
Chiamate API per servizi integrati .....	164
CloudWatch metriche .....	169
Utilizzo dell'API (esempi Java) .....	171
AddTagsToCertificate .....	171
DeleteCertificate .....	173
DescribeCertificate .....	175
ExportCertificate .....	178
GetCertificate .....	181

ImportCertificate .....	183
ListCertificates .....	187
RenewCertificate .....	189
ListTagsForCertificate .....	191
RemoveTagsFromCertificate .....	193
RequestCertificate .....	195
ResendValidationEmail .....	198
Risoluzione dei problemi .....	201
Richieste di certificati .....	201
Timeout della richiesta .....	201
Richiesta non riuscita .....	202
Convalida dei certificati .....	203
Convalida DNS .....	204
Convalida e-mail .....	207
Rinnovo del certificato .....	212
Preparazione per la convalida automatica dei domini .....	212
Gestione degli errori relativi al rinnovo gestito dei certificati .....	213
Altri problemi .....	215
Registri CAA .....	216
Importazione di certificati .....	217
Associazione dei certificati .....	217
API Gateway .....	218
Errore imprevisto .....	218
Problemi con il ruolo collegato al servizio ACM .....	219
Gestione delle eccezioni .....	7
Gestione delle eccezioni per i certificati privati .....	219
Concetti .....	223
Certificato ACM .....	223
ACM Root CA .....	225
Dominio Apex .....	226
Crittografia delle chiavi asimmetrica .....	226
Certificate Authority (Autorità di certificazione) .....	227
Registrazione della trasparenza del certificato .....	227
Domain Name System .....	228
Nomi di dominio .....	228
Crittografia e decrittografia .....	230

---

Nome di dominio completo (FQDN) .....	230
Infrastruttura a chiave pubblica .....	230
Certificato root .....	230
Secure Sockets Layer (SSL) .....	230
HTTPS sicuro .....	231
Certificati del server SSL .....	231
Crittografia delle chiavi simmetrica .....	231
Transport Layer Security (TLS) .....	231
Trust .....	231
Cronologia dei documenti .....	232
.....	ccxxxix

# Che cos'è AWS Certificate Manager?

AWS Certificate Manager (ACM) gestisce la complessità della creazione, dell'archiviazione e del rinnovo dei certificati e delle chiavi SSL/TLS X.509 pubblici e privati che proteggono i siti Web e le applicazioni. AWS Puoi fornire i certificati per i tuoi [servizi AWS integrati](#) emettendoli direttamente con ACM o [importando](#) certificati di terze parti nel sistema di gestione ACM. I certificati ACM possono proteggere nomi di dominio singoli, più nomi di dominio specifici, domini con caratteri jolly o combinazioni di questi. I certificati jolly ACM possono proteggere un numero illimitato di sottodomini. Puoi anche [esportare](#) i certificati ACM firmati da e utilizzarli ovunque nella tua PKI interna. CA privata AWS

## Note

ACM non è destinato all'uso con un server Web autonomo. Se desideri configurare un server sicuro autonomo su un'istanza Amazon EC2, il seguente tutorial contiene le istruzioni: [Configura SSL/TLS su Amazon Linux 2023](#).

## Argomenti

- [ACM è il servizio giusto per me?](#)
- [Caratteristiche dei certificati ACM](#)
- [Regioni supportate](#)
- [Servizi integrati con AWS Certificate Manager](#)
- [Simboli di sito protetto e loghi di affidabilità](#)
- [Quote](#)
- [Prezzi per AWS Certificate Manager](#)

## ACM è il servizio giusto per me?

AWS offre due opzioni ai clienti che implementano certificati X.509 gestiti. Scegli quello migliore per le tue esigenze.

1. AWS Certificate Manager (ACM): questo servizio è destinato ai clienti aziendali che necessitano di una presenza Web sicura tramite TLS. I certificati ACM vengono distribuiti tramite Elastic Load



Balancing, CloudFront Amazon, Amazon API Gateway e [AWS](#) altri servizi integrati. L'applicazione più comune di questo tipo è un sito pubblico sicuro con requisiti di traffico significativi. ACM semplifica inoltre la gestione della sicurezza automatizzando il rinnovo dei certificati in scadenza. Sei nel posto giusto per questo servizio.

2. CA privata AWS—Questo servizio è destinato ai clienti aziendali che creano un'infrastruttura a chiave pubblica (PKI) all'interno del AWS cloud e destinato all'uso privato all'interno di un'organizzazione. Con CA privata AWS, puoi creare la tua gerarchia di autorità di certificazione (CA) ed emettere certificati con essa per autenticare utenti, computer, applicazioni, servizi, server e altri dispositivi. I certificati emessi da una CA privata non possono essere utilizzati su Internet. Per ulteriori informazioni, consulta la [CA privata AWS Guida per l'utente](#).

## Caratteristiche dei certificati ACM

I certificati pubblici forniti da ACM hanno le caratteristiche descritte in questa sezione.

### Note

Queste caratteristiche si applicano solo ai certificati forniti da ACM. Potrebbero non essere applicate per i [certificati importati su ACM](#).

### Autorità e gerarchia dei certificati

I certificati pubblici richiesti tramite ACM sono concessi da [Amazon Trust Services](#), un'[autorità di certificazione \(CA\)](#) pubblica gestita da Amazon. Le CA Amazon Root da 1 a 4 sono firmati trasversalmente da una root precedente denominata Starfield G2 Root Certificate Authority - G2. Starfield root è considerato affidabile sui dispositivi Android a partire dalle versioni successive di Gingerbread e da iOS a partire dalla versione 4.1. Le root di Amazon sono considerate affidabili da iOS a partire dalla versione 11. Qualsiasi browser, applicazione o sistema operativo che include le root Amazon o Starfield considererà attendibili i certificati pubblici ottenuti da ACM.

I certificati leaf o end-entity che ACM rilascia ai clienti acquisiscono la loro autorità da una CA root di Amazon Trust Services tramite una delle diverse CA intermedie. ACM assegna casualmente una CA intermedia in base al tipo di certificato (RSA o ECDSA) richiesto. Dal momento che la CA intermedia viene selezionata casualmente dopo la generazione della richiesta, ACM non fornisce informazioni sulla CA intermedia.

## Attendibilità browser e applicazione

I certificati ACM sono ritenuti attendibili da tutti i principali browser, tra cui Google Chrome, Microsoft Internet Explorer e Microsoft Edge, Mozilla Firefox e Apple Safari. Quando sono connessi tramite SSL/TLS a siti che utilizzano certificati ACM, i browser che ritengono attendibili i certificati ACM mostrano un'icona di un lucchetto nella loro barra di stato o nella barra degli indirizzi. I certificati ACM sono ritenuti attendibili anche da Java.

## Rotazione CA intermedia e root

Per mantenere un'infrastruttura di certificati resiliente e agile, Amazon può in qualsiasi momento scegliere di interrompere la fornitura di una CA intermedia senza preavviso. Modifiche di questo tipo non hanno alcun impatto sui clienti. Per ulteriori informazioni, consulta il post di blog [“Amazon introduce autorità di certificazione intermedie dinamiche”](#).

Nell'improbabile caso in cui Amazon interrompa la fornitura di una CA root, la modifica avverrà con la rapidità necessaria alle circostanze. A causa del grande impatto di tale cambiamento, Amazon utilizzerà tutti i meccanismi disponibili per avvisare AWS i clienti, tra cui l'AWS Health Dashboard e-mail ai proprietari degli account e il contatto con i responsabili tecnici degli account.

## Accesso al firewall per la revoca

Se un certificato end-entity non è più affidabile, verrà revocato. OCSP e CRL sono i meccanismi standard utilizzati per verificare se un certificato è stato revocato o meno. OCSP e CRL sono i meccanismi standard utilizzati per pubblicare le informazioni sulla revoca. Alcuni firewall dei clienti potrebbero richiedere regole aggiuntive per consentire il funzionamento di questi meccanismi.

I seguenti modelli di caratteri jolly URL possono essere utilizzati per identificare il traffico di revoca. Un asterisco (\*) rappresenta uno o più caratteri alfanumerici, un punto interrogativo (?) rappresenta un singolo carattere alfanumerico e un cancelletto (#) rappresenta un numero.

- OCSP

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

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

- CRL

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

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

## Convalida del dominio (DV)

I certificati ACM sono convalidati dal dominio. Ciò significa che il campo dell'oggetto di un certificato ACM identifica un nome di dominio e nulla di più. Quando si richiede un certificato ACM, è necessario che l'utente convalidi la proprietà o il controllo di tutti i domini specificati nella richiesta. È possibile convalidare la proprietà tramite e-mail o DNS. Per ulteriori informazioni, consultare [Convalida e-mail](#) e [Convalida DNS](#).

## Periodo di validità

Il periodo di validità dei certificati ACM è di 13 mesi (395 giorni).

## Distribuzione e rinnovo gestito

ACM gestisce il processo del rinnovo dei certificati ACM e del loro provisioning una volta che vengono rinnovati. Il rinnovo automatico consente di evitare tempi di inattività causati da certificati non configurati in modo corretto, revocati o scaduti. Per ulteriori informazioni, consulta [Rinnovo gestito per i certificati ACM](#).

## Nomi di dominio multipli

Ogni certificato ACM deve includere almeno un nome di dominio completo (FQDN) ed è possibile aggiungere ulteriori nomi se si desidera. Ad esempio, al momento della creazione di un certificato ACM per `www.example.com`, è possibile aggiungere anche il nome `www.example.net` se i clienti possono raggiungere il sito utilizzando entrambi i nomi. Ciò vale anche per domini essenziali (noti anche come apex di zona o domini nudi). Ciò significa che è possibile richiedere un certificato ACM per `www.example.com` e aggiungere il nome `example.com`. Per ulteriori informazioni, consulta [Richiesta di un certificato pubblico](#).

## Nomi jolly

ACM consente di utilizzare un asterisco (\*) nel nome di dominio per creare un certificato ACM contenente un nome jolly in grado di proteggere diversi siti nello stesso dominio. Ad esempio, `*.example.com` protegge `www.example.com` e `images.example.com`.

### Note

Quando si fa richiesta di un certificato jolly, l'asterisco (\*) deve essere nella posizione più a sinistra nel nome di dominio e può proteggere solo un livello di sottodominio. Ad esempio, `*.example.com` può proteggere `login.example.com` e `test.example.com`, ma non può proteggere `test.login.example.com`. Si noti inoltre come `*.example.com` protegga solo i sottodomini di `example.com` e non il

dominio essenziale o apex (**example.com**). Ad ogni modo, è possibile richiedere un certificato che protegga un dominio essenziale o apex e i relativi sottodomini specificando nomi di dominio multipli nella richiesta. Ad esempio, è possibile richiedere un certificato che protegga **example.com** e **\*.example.com**.

## Algoritmi chiave

Un certificato deve specificare un algoritmo e la dimensione della chiave di accesso. Al momento, i seguenti algoritmi della chiave pubblica RSA e Elliptic Curve Digital Signature Algorithm (ECDSA) sono supportati da ACM. ACM può richiedere l'emissione di nuovi certificati utilizzando algoritmi contrassegnati da un asterisco (\*). Gli algoritmi rimanenti sono supportati solo per i certificati [importati](#).

### Note

Quando richiedi un certificato PKI privato firmato da una CA presso AWS Private CA, la famiglia di algoritmi di firma specificata (RSA o ECDSA) deve corrispondere alla famiglia di algoritmi della chiave segreta della CA.

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

Le chiavi ECDSA sono più piccole e offrono una sicurezza paragonabile alle chiavi RSA ma con una maggiore efficienza di elaborazione. Tuttavia, ECDSA non è supportato da tutti i client di rete. La seguente tabella, adattata dal [NIST](#), mostra la forza di sicurezza rappresentativa di RSA ed ECDSA con chiavi di varie dimensioni. Tutti i valori sono in bit.

## Confronto della sicurezza per algoritmi e chiavi

Forza di sicurezza	Dimensione della chiave RSA	Dimensione della chiave ECDSA
128	3072	256
192	7680	384
256	15360	512

La forza di sicurezza, intesa come potenza di 2, è correlata al numero di tentativi necessari per violare la crittografia. Ad esempio, sia una chiave RSA a 3072 bit che una chiave ECDSA a 256 bit possono essere recuperate con non più di  $2^{128}$  tentativi.

Per informazioni su come scegliere un algoritmo, consulta il post AWS sul blog [Come valutare e utilizzare i certificati ECDSA](#) in AWS Certificate Manager

### Important

Si noti come i [servizi integrati](#) permettano solo agli algoritmi e alle dimensioni della chiave di accesso supportati di essere associati alle loro risorse. Inoltre il loro supporto varia a seconda che il certificato venga importato su IAM o su ACM. Per ulteriori informazioni, consultare la documentazione di ogni servizio.

- Per Elastic Load Balancing, consultare [Listener HTTPS per Application Load Balancer](#).
- Per CloudFront, consulta [Protocolli e cifrari SSL/TLS supportati](#).

## Punycode

I seguenti requisiti [Punycode](#) relativi a [Nomi di dominio internazionalizzati](#) devono essere soddisfatti:

1. I nomi di dominio che iniziano con il modello "<character><character>--" devono corrispondere a "xn--".
2. Anche i nomi di dominio che iniziano con "xn--" devono essere nomi di dominio internazionalizzati validi.

## Esempi di punycode

Nome dominio	Soddisfa #1	Soddisfa #2	Conse o	Nota
esempio.com	N/A	n/a	✓	Non inizia con "<character><character>--"
a--esempio.com	N/A	n/a	✓	Non inizia con "<character><character>--"
abc—esempio.com	N/A	n/a	✓	Non inizia con "<character><character>--"
xn—xyz.com	Sì	Sì	✓	Nome di dominio internazionalizzato valido (si risolve su 简.com)
xn--esempio.com	Sì	No	✗	Nome di dominio internazionalizzato non valido
ab--esempio.com	No	No	✗	Deve iniziare con "xn--"

## Eccezioni

Tieni presente quanto segue:

- ACM non fornisce certificati di convalida estesa (Extended validation, EV) né certificati di convalida dell'organizzazione (Organization validation, OV).
- ACM fornisce certificati solo per i protocolli SSL/TLS.
- Non è possibile utilizzare certificati ACM per la crittografia delle e-mail.
- ACM attualmente non consente di annullare il [rinnovo del certificato gestito](#) per i certificati ACM. Inoltre, il rinnovo gestito non è disponibile per i certificati importati su ACM.
- Non è possibile richiedere certificati per nomi di dominio appartenenti a Amazon, ad esempio quelli che finiscono con such amazonaws.com, cloudfront.net o elasticbeanstalk.com.
- Non è possibile scaricare la chiave di accesso privata per un certificato ACM.
- Non puoi installare direttamente i certificati ACM nel sito Web o nell'applicazione Amazon Elastic Compute Cloud (Amazon EC2). È possibile comunque utilizzare il proprio certificato

con qualsivoglia servizio integrato. Per ulteriori informazioni, consulta [Servizi integrati con AWS Certificate Manager](#).

## Regioni supportate

Vedi l'argomento relativo a [Regioni ed endpoint AWS](#) nella Riferimenti generali di AWS oppure la [Tabella delle Regioni AWS](#) per informazioni sulla disponibilità regionale di ACM.

I certificati in ACM sono risorse regionali. Per utilizzare un certificato con Elastic Load Balancing per lo stesso nome di dominio completo (FQDN) o set di FQDN in più di una AWS regione, devi richiedere o importare un certificato per ogni regione. Per i certificati forniti da ACM, questo significa che è necessario convalidare nuovamente ogni nome di dominio nel certificato per ogni regione. Non è possibile copiare un certificato tra regioni.

Per utilizzare un certificato ACM con Amazon CloudFront, devi richiedere o importare il certificato nella regione Stati Uniti orientali (Virginia settentrionale). I certificati ACM in questa regione associati a una CloudFront distribuzione vengono distribuiti in tutte le aree geografiche configurate per tale distribuzione.

## Servizi integrati con AWS Certificate Manager

AWS Certificate Manager supporta un numero crescente di AWS servizi. Non è possibile installare il certificato ACM o il CA privata AWS certificato privato direttamente sul sito Web o sull'applicazione di AWS base.

### Note

I certificati ACM pubblici possono essere installati su istanze Amazon EC2 connesse a un'[Enclave Nitro](#), ma non su altre istanze di Amazon EC2. Per informazioni sulla configurazione di un server Web autonomo su un'istanza Amazon EC2 non connessa a Nitro Enclave, vedi [Tutorial: Installa un server Web LAMP su Amazon Linux 2](#) o [Tutorial: installa un server Web LAMP con Amazon Linux AMI](#).

I certificati ACM sono supportati dai seguenti servizi:

## Sistema di bilanciamento del carico elastico

Elastic Load Balancing distribuisce automaticamente il traffico in entrata delle applicazioni su più istanze Amazon EC2. Rileva le istanze non integre e re-instrada il traffico alle istanze integre finché quelle non integre non vengono ripristinate. Elastic Load Balancing ridimensiona automaticamente la sua capacità di gestione delle richieste in risposta al traffico in entrata. Per ulteriori informazioni su Elastic Load Balancing, consulta la [Guida per l'utente di Elastic Load Balancing](#).

In generale, per distribuire contenuti protetti su SSL/TLS, i bilanciatori del carico richiedono l'installazione dei certificati SSL/TLS sul load balancer o sull'istanza Amazon EC2 di back-end. ACM è integrato con Elastic Load Balancing per la distribuzione di certificati ACM sul load balancer. Per ulteriori informazioni, consultare l'articolo relativo alla [creazione di un Application Load Balancer](#).

## Amazon CloudFront

Amazon CloudFront è un servizio web che accelera la distribuzione dei tuoi contenuti web dinamici e statici agli utenti finali distribuendo i tuoi contenuti da una rete mondiale di edge location. Quando un utente finale richiede il contenuto attraverso il quale stai distribuendo CloudFront, viene indirizzato verso la edge location che offre la latenza più bassa. In questo modo i contenuti vengono distribuiti con massimi livelli di prestazioni. Se il contenuto si trova attualmente in quella posizione periferica, lo CloudFront consegna immediatamente. Se il contenuto non si trova attualmente in quella posizione periferica, lo CloudFront recupera dal bucket o dal server Web Amazon S3 che hai identificato come fonte di contenuto definitiva. Per ulteriori informazioni CloudFront, consulta l'[Amazon CloudFront Developer Guide](#).

Per fornire contenuti sicuri tramite SSL/TLS, è CloudFront necessario che i certificati SSL/TLS siano installati sulla distribuzione o sulla fonte di contenuto supportata CloudFront . ACM è integrato con per distribuire i certificati ACM sulla distribuzione. CloudFront CloudFront Per ulteriori informazioni, consultare l'articolo [Per ottenere un certificato SSL/TLS](#).

### Note

Per utilizzare un certificato ACM con CloudFront, è necessario richiedere o importare il certificato nella regione Stati Uniti orientali (Virginia settentrionale).



## Amazon Cognito

Amazon Cognito fornisce autenticazione, autorizzazione e gestione degli utenti per le applicazioni Web e per dispositivi mobili. Gli utenti possono accedere direttamente con Account AWS le tue credenziali o tramite terze parti come Facebook, Amazon, Google o Apple. Per ulteriori informazioni su Amazon Cognito, consulta la [Guida per sviluppatori di Amazon Cognito](#).

Quando configuri un pool di utenti Cognito per utilizzare un CloudFront proxy Amazon, CloudFront puoi inserire un certificato ACM per proteggere il dominio personalizzato. In questo caso, tieni presente che devi rimuovere l'associazione del certificato con CloudFront prima di poterlo eliminare.

## AWS Elastic Beanstalk

Elastic Beanstalk ti aiuta a distribuire e gestire le applicazioni AWS nel cloud senza preoccuparti dell'infrastruttura che esegue tali applicazioni. AWS Elastic Beanstalk riduce la complessità della gestione. Basta caricare la tua applicazione perché Elastic Beanstalk gestisca automaticamente tutti i dettagli correlati a provisioning della capacità, bilanciamento del carico, dimensionamento e monitoraggio dello stato dell'applicazione. Elastic Beanstalk utilizza il servizio Elastic Load Balancing per creare un load balancer. Per ulteriori informazioni su Elastic Beanstalk, consulta la [Guida per sviluppatori di AWS Elastic Beanstalk](#).

Per scegliere un certificato, è necessario configurare il load balancer per l'applicazione nella console Elastic Beanstalk. Per ulteriori informazioni, consultare [Configurazione del load balancer dell'ambiente Elastic Beanstalk per terminare HTTPS](#).

## AWS App Runner

App Runner è un AWS servizio che offre un modo rapido, semplice ed economico per distribuire dal codice sorgente o da un'immagine del contenitore direttamente a un'applicazione Web scalabile e sicura nel cloud. AWS Non è necessario apprendere nuove tecnologie, decidere quale servizio di elaborazione utilizzare o sapere come fornire e configurare le risorse. AWS Per ulteriori informazioni su App Runner, consulta la [Guida per gli sviluppatori di AWS App Runner](#).

Quando si associano nomi di dominio personalizzati al servizio App Runner, App Runner crea internamente certificati che tengono traccia della validità del dominio. Sono memorizzati in ACM. App Runner non elimina questi certificati per sette giorni dopo la disassociazione di un dominio dal servizio o dopo l'eliminazione del servizio. L'intero processo è automatizzato e non è necessario aggiungere o gestire nessun certificato da soli. Per ulteriori informazioni, consulta [Gestione di nomi di dominio personalizzati per un servizio App Runner](#) nella Guida per gli sviluppatori di AWS App Runner .

## Amazon API Gateway

Con l'enorme diffusione di dispositivi mobili e la crescita dell'Internet of Things (IoT), è diventato sempre più comune creare API che possono essere utilizzate per accedere ai dati e interagire con i sistemi di back-end su AWS. È possibile utilizzare API Gateway per la pubblicazione, la manutenzione, il monitoraggio e la protezione delle API. Dopo aver distribuito l'API su API Gateway, è possibile [impostare un nome di dominio personalizzato](#) per semplificare l'accesso. Per impostare un nome di dominio personalizzato, è necessario fornire un certificato SSL/TLS. Puoi utilizzare ACM per generare o importare il certificato. Per ulteriori informazioni su Amazon API Gateway, consulta la [Guida per gli sviluppatori di Amazon API Gateway](#).

## AWS Enclavi Nitro

AWS Nitro Enclaves è una funzionalità di Amazon EC2 che consente di creare ambienti di esecuzione isolati, chiamati enclavi, da istanze Amazon EC2. Le enclave sono macchine virtuali separate, rinforzate e altamente vincolate. Forniscono solo connettività socket locale sicura con l'istanza principale. Non dispongono di archiviazione persistente, accesso interattivo o reti esterne. Gli utenti non possono stabilire SSH in un'enclave e i dati e le applicazioni all'interno dell'enclave non possono accedere ai processi, alle applicazioni o agli utenti dell'istanza principale (inclusi root o admin).

Le istanze EC2 connesse a Nitro Enclaves supportano i certificati ACM. Per ulteriori informazioni, consulta [AWS Certificate Manager per Nitro Enclaves](#).

### Note

Non è possibile associare certificati ACM a un'istanza EC2 non connessa a un Nitro Enclave.

## AWS CloudFormation

AWS CloudFormation ti aiuta a modellare e configurare le tue risorse Amazon Web Services. Crei un modello che descrive le AWS risorse che desideri utilizzare, come Elastic Load Balancing o API Gateway. Quindi AWS CloudFormation effettuerà il provisioning e la configurazione di tali risorse. Non è necessario creare e configurare singolarmente AWS le risorse e capire cosa dipende da cosa; AWS CloudFormation gestisce tutto questo. I certificati ACM sono inclusi come risorsa modello, il che significa che AWS CloudFormation è possibile richiedere certificati ACM da utilizzare con AWS i servizi per abilitare connessioni sicure. Inoltre, i certificati ACM sono inclusi in molte delle AWS risorse con cui è possibile eseguire la configurazione. AWS CloudFormation

Per informazioni generali su CloudFormation, consulta la [Guida per l'AWS CloudFormation utente](#). Per informazioni sulle risorse ACM supportate da CloudFormation, vedere [AWS::CertificateManager::Certificate](#).

Grazie alla potente automazione fornita da AWS CloudFormation, è facile superare la [quota dei certificati](#), soprattutto con nuovi AWS account. Ti consigliamo di seguire le [best practice](#) ACM per AWS CloudFormation.

#### Note

Se crei un certificato ACM con AWS CloudFormation, lo AWS CloudFormation stack rimane nello stato CREATE\_IN\_PROGRESS. Qualsiasi ulteriore operazione dello stack viene ritardata finché non procedi secondo le istruzioni presenti nell'e-mail di convalida del certificato. Per ulteriori informazioni, consultare la sezione relativa all'[impossibilità di stabilizzare una risorsa durante un'operazione di creazione, aggiornamento o eliminazione dello stack](#).

## AWS Amplify

Amplify è un set di strumenti e funzionalità appositamente progettati che consente agli sviluppatori web e mobili front-end di creare applicazioni complete in modo rapido e semplice. AWS Amplify fornisce due servizi: Amplify Hosting e Amplify Studio. Amplify Hosting fornisce un flusso di lavoro basato su git per l'hosting di app web full-stack serverless con distribuzione continua. Amplify Studio è un ambiente di sviluppo visivo che semplifica la creazione di app web e mobili scalabili e full-stack. Usa Studio per creare l'interfaccia utente front-end con un set di componenti dell'interfaccia utente, creare un backend per app e ready-to-use quindi connettere i due elementi. Per ulteriori informazioni su Amplify, consulta la [Guida per l'utente di AWS Amplify](#).

Se colleghi un dominio personalizzato all'applicazione, la console Amplify emette un certificato ACM per proteggerlo.

## OpenSearch Servizio Amazon

Amazon OpenSearch Service è un motore di ricerca e analisi per casi d'uso come analisi dei log, monitoraggio delle applicazioni in tempo reale e analisi del flusso di clic. Per ulteriori informazioni, consulta l'[Amazon OpenSearch Service Developer Guide](#).

Quando si crea un cluster di OpenSearch servizi che contiene un [dominio e un endpoint personalizzati](#), è possibile utilizzare ACM per fornire un certificato all'Application Load Balancer associato.

## AWS Network Firewall

AWS Network Firewall è un servizio gestito che semplifica l'implementazione delle protezioni di rete essenziali per tutti i tuoi Amazon Virtual Private Cloud (VPC). Per ulteriori informazioni su Firewall di rete, consulta la [Guida per gli sviluppatori di AWS Network Firewall](#).

Il firewall di Firewall di rete si integra con ACM per l'ispezione TLS. Se si utilizza l'ispezione TLS in Firewall di rete, è necessario configurare un certificato ACM per la decrittografia e la ricrittografia del traffico SSL/TLS che attraversa il firewall. Per informazioni su come funziona Firewall di rete con ACM per l'ispezione TLS, consulta [Requisiti per l'utilizzo di certificati SSL/TLS con configurazioni di ispezione TLS](#) nella Guida per gli sviluppatori di AWS Network Firewall .

## Simboli di sito protetto e loghi di affidabilità

Amazon non fornisce alcun simbolo di sito protetto e non permette di utilizzare il suo marchio come tale:

- AWS Certificate Manager (ACM) non fornisce un sigillo sicuro da utilizzare sul tuo sito Web. Se desideri utilizzare un simbolo di questo tipo, puoi ottenerne uno da un fornitore di terze parti. Consigliamo di scegliere un fornitore che valuti e confermi la sicurezza del sito Web o delle prassi aziendali.
- Amazon non permette di utilizzare il suo marchio o logo come badge del certificato, simbolo di sito protetto o logo di affidabilità. Simboli e badge di questo tipo possono essere copiati da altri siti che non utilizzano il servizio ACM e quindi essere impiegati in modo improprio per dare una falsa impressione di affidabilità. Per proteggere i nostri clienti e la reputazione di Amazon, non consentiamo l'utilizzo del nostro marchio e del nostro logo per questo scopo.

## Quote

Le seguenti quote di servizio AWS Certificate Manager (ACM) si applicano a ciascuna AWS regione per ogni account. AWS

Per vedere quali quote possono essere regolate, vedere la [tabella quote ACM](#) nella AWS Guida generale di riferimento. Per richiedere aumenti delle quote, creare un caso nel [Centro AWS Support](#).

## Quote generali

Elemento	Quota predefinita
<p>Numero di certificati ACM</p> <p>I certificati scaduti e revocati continuano a contare ai fini del totale.</p> <p>I certificati firmati da una CA di CA privata AWS non vengono conteggiati ai fini di questo totale.</p>	2500
<p>Numero di certificati ACM all'anno (ultimi 365 giorni)</p> <p>Puoi richiedere fino al doppio della tua quota di certificati ACM per anno, regione e account. Ad esempio, se la quota è 2.500, è possibile richiedere fino a 5.000 certificati ACM all'anno in una determinata regione e account. È possibile avere solo 2.500 certificati in qualsiasi momento. Se si richiedono 5.000 certificati in un anno, è necessario eliminare 2.500 certificati durante l'anno per rimanere entro la quota. Se sono necessari più di 2.500 certificati in qualsiasi momento, è necessario contattare il <a href="#">Centro AWS Support</a>.</p> <p>I certificati firmati da una CA di CA privata AWS non vengono conteggiati ai fini di questo totale.</p>	Il doppio della quota dell'account
Numero di certificati importati	2.500
Numero di certificati importati all'anno (ultimi 365 giorni)	Il doppio della quota dell'account
Numero di nomi di dominio per certificato ACM	10

Elemento	Quota predefinita
<p>La quota predefinita è 10 nomi di dominio per ciascun certificato ACM. La tua quota potrebbe essere maggiore.</p> <p>Il primo nome di dominio inviato è incluso come nome comune (CN) dell'oggetto del certificato. Tutti i nomi sono inclusi nell'estensione Nome oggetto alternativo.</p> <p>È possibile richiedere fino a 100 nomi di dominio. Per richiedere un aumento della quota, crea una richiesta nella console Service Quotas per il servizio ACM. Prima di creare un caso, tuttavia, assicurarsi di comprendere come l'aggiunta di altri nomi di dominio può generare più lavoro amministrativo se si utilizza la convalida e-mail. Per ulteriori informazioni, consulta <a href="#">Convalida del dominio</a>.</p> <p>La quota per il numero di nomi di dominio per il certificato ACM si applica solo per i certificati forniti da ACM. Questa quota non si applica ai certificati importati in ACM. Le seguenti sezioni si applicano solo ai certificati ACM.</p>	

Elemento	Quota predefinita
<p>Numero di CA private</p> <p>ACM è integrato con AWS Private Certificate Authority ().CA privata AWSÈ possibile utilizzare la console ACM o l'API ACM per richiedere e certificati privati a un'autorità di certificazione (CA) privata esistente ospitata da. AWS CLI CA privata AWS Tali certificati vengono gestiti all'interno dell'ambiente e presentano le stesse limitazioni dei certificati pubblici emessi da ACM. Per ulteriori informazioni, consulta <a href="#">Richiesta di un certificato PKI privato</a>. Puoi anche emettere certificati privati utilizzando il servizio autonomo CA privata AWS . Per ulteriori informazioni, consulta <a href="#">Emissione di un certificato privato</a>.</p> <p>Un CA privato eliminato verrà conteggiato ai fini della quota fino alla fine del periodo di ripristino. Per ulteriori informazioni consulta <a href="#">Eliminazione del CA privato</a>.</p>	200
Numero di certificati privati per CA (durata)	1.000.000

## Quote tariffarie API

Le seguenti quote di servizio si applicano all'API ACM per ciascuna Regione e ciascun account. ACM limita le richieste API a diverse quote a seconda dell'operazione API. Limitare significa che ACM rifiuta una richiesta valida perché la richiesta supera la quota dell'operazione stabilita di richieste al secondo. Quando una richiesta è soggetta a limitazione, ACM restituisce un errore di `ThrottlingException`. La tabella seguente elenca ciascuna operazione API e la quota a cui ACM limita le richieste per tale operazione.

**Note**

Oltre alle operazioni API elencate nella tabella seguente, ACM può anche chiamare l'operazione `IssueCertificate` esterna da CA privata AWS. Per informazioni sulle quote up-to-date tariffarie su `IssueCertificate`, consulta gli [endpoint e le quote](#) per CA privata AWS

requests-per-second Quota R per ogni operazione API ACM

Chiamata API	Richieste al secondo
<code>AddTagsToCertificate</code>	5
<code>DeleteCertificate</code>	10
<code>DescribeCertificate</code>	10
<code>ExportCertificate</code>	5
<code>GetAccountConfiguration</code>	1
<code>GetCertificate</code>	10
<code>ImportCertificate</code>	1
<code>ListCertificates</code>	8
<code>ListTagsForCertificate</code>	10
<code>PutAccountConfiguration</code>	1
<code>RemoveTagsFromCertificate</code>	5
<code>RenewCertificate</code>	5
<code>RequestCertificate</code>	5
<code>ResendValidationEmail</code>	1
<code>UpdateCertificateOptions</code>	5



Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API AWS Certificate Manager](#).

## Prezzi per AWS Certificate Manager

Non si è soggetti a un costo aggiuntivo per i certificati SSL/TLS gestiti con AWS Certificate Manager. Pagi solo per AWS le risorse che crei per far funzionare il tuo sito Web o la tua applicazione. Per le informazioni più recenti sui prezzi di ACM, consulta la pagina [dei prezzi dei AWS Certificate Manager servizi](#) sul AWS sito Web.

# Sicurezza in AWS Certificate Manager

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS Certificate Manager, consulta [AWS Servizi nell'ambito del programma di conformitàAWS](#) .
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Certificate Manager (ACM). I seguenti argomenti illustrano come configurare ACM per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse ACM.

## Argomenti

- [Protezione dei dati in AWS Certificate Manager](#)
- [Identity and Access Management per AWS Certificate Manager](#)
- [Resilienza in AWS Certificate Manager](#)
- [Sicurezza dell'infrastruttura nell' AWS Certificate Manager](#)
- [Best practice](#)

## Protezione dei dati in AWS Certificate Manager

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati in AWS Certificate Manager. Come descritto in questo modello, AWS è responsabile della protezione

dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con ACM o altri utenti Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

## Sicurezza per le chiavi private dei certificati

Quando [richiedi un certificato pubblico](#), AWS Certificate Manager (ACM) genera una coppia di chiavi pubblica/privata. Per i [certificati importati](#) viene generata la coppia di chiavi di accesso. La chiave di accesso pubblica diventa parte del certificato. ACM archivia il certificato e la chiave privata

corrispondente e utilizza AWS Key Management Service (AWS KMS) per proteggere la chiave privata. Il processo avviene in questo modo:

1. La prima volta che richiedi o importi un certificato in una AWS regione, ACM ne crea uno gestito AWS KMS key con l'alias `aws/acm`. Questa chiave KMS è unica in ogni account e in ogni regione. AWS AWS
2. ACM utilizza questa chiave KMS per crittografare la chiave di accesso privata del certificato. ACM archivia solo una versione crittografata della chiave di accesso privata (ACM non archivia la chiave di accesso privata sotto forma di testo crittografato). ACM utilizza la stessa chiave KMS per crittografare le chiavi private di tutti i certificati in un AWS account specifico e in una regione specifica. AWS
3. Quando si associa il certificato a un servizio integrato con AWS Certificate Manager, ACM invia il certificato e la chiave privata crittografata al servizio. Viene inoltre creata una concessione AWS KMS che consente al servizio di utilizzare la chiave KMS per decrittografare la chiave privata del certificato. Per ulteriori informazioni sulle autorizzazioni, consulta [Utilizzo delle autorizzazioni](#) nella guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni sui servizi supportati da ACM, consultare [Servizi integrati con AWS Certificate Manager](#).

#### Note

Hai il controllo sulla concessione creata automaticamente. AWS KMS Se si elimina questa concessione per qualsiasi motivo, si perde la funzionalità ACM per il servizio integrato.

4. I servizi integrati utilizzano la chiave KMS per decrittografare la chiave privata. In seguito il servizio utilizza il certificato e la chiave di accesso privata decrittografata (testo non crittografato) per stabilire canali di comunicazione sicura (sessioni SSL/TLS) con i suoi client.
5. Quando il certificato viene disassociato da un servizio integrato, l'autorizzazione concessa nella fase 3 viene ritirata. Ciò significa che il servizio non può più utilizzare la chiave KMS per decrittografare la chiave di accesso privata.

## Identity and Access Management per AWS Certificate Manager

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse ACM. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

## Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Funzionamento di AWS Certificate Manager con IAM](#)
- [Esempi di policy basate su identità per AWS Certificate Manager](#)
- [Autorizzazioni API ACM: operazioni e riferimento alle risorse](#)
- [AWS Policy gestite da per AWS Certificate Manager](#)
- [Utilizzo delle chiavi di condizione con ACM](#)
- [Utilizzo di un ruolo collegato ai servizi \(SLR\) con ACM](#)
- [Risoluzione dei problemi di identità e accesso in AWS Certificate Manager](#)

## Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in ACM.

**Utente del servizio:** se utilizzi il servizio ACM per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità ACM utilizzate per il processo, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non è possibile accedere a una funzionalità in ACM, consulta [Risoluzione dei problemi di identità e accesso in AWS Certificate Manager](#).

**Amministratore del servizio:** se sei il responsabile delle risorse ACM presso la tua azienda, probabilmente disponi dell'accesso completo ad ACM. Il tuo compito è determinare le funzionalità e le risorse di ACM a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con ACM, consulta [Funzionamento di AWS Certificate Manager con IAM](#).

**Amministratore IAM:** un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso ad ACM. Per visualizzare policy basate sulle identità

ACM di esempio che puoi utilizzare in IAM, consulta [Esempi di policy basate su identità per AWS Certificate Manager](#).

## Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione [Come accedere al tuo Account AWS](#) nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia della linea di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consultare [Firma delle richieste AWS](#) nella Guida per l'utente di IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#) nella Guida per l'utente di IAM.

## Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco

completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Tasks that require root user credentials](#) (Attività che richiedono le credenziali dell'utente root) nella Guida per l'utente di IAM.

## Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ad Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono ad Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center.

## Utenti e gruppi IAM

Un [utente IAM](#) è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente di IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un utente IAM \(invece di un ruolo\)](#) nella Guida per l'utente di IAM.

## Ruoli IAM

Un [ruolo IAM](#) è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo [scambio di ruoli](#). È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Creazione di un ruolo per un provider di identità di terza parte](#) nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso multi-servizio:** alcuni Servizi AWS utilizzano funzionalità che in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.



- **Inoltro delle sessioni di accesso (FAS):** quando utilizzi un ruolo o un utente IAM per eseguire azioni in AWS, sei considerato un principale. Quando utilizzi alcuni servizi, puoi eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altre risorse o Servizi AWS per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Inoltro sessioni di accesso](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLI o dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

## Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione

ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWS sotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

## Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente di IAM.

## Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali

condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

## Liste di controllo accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

## Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Policy di controllo dei servizi (SCP):** le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS multipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un

utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente di IAM.

## Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare [Logica di valutazione delle policy](#) nella Guida per l'utente di IAM.

## Funzionamento di AWS Certificate Manager con IAM

Prima di utilizzare IAM per gestire l'accesso ad ACM, scopri quali funzionalità di IAM sono disponibili per l'uso con ACM.

Funzionalità IAM che è possibile utilizzare con AWS Certificate Manager

Funzionalità IAM	Supporto ACM
<a href="#">Policy basate su identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Operazioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione della policy (specifica del servizio)</a>	Sì
<a href="#">Liste di controllo degli accessi</a>	No
<a href="#">ABAC (tag nelle policy)</a>	Parziale
<a href="#">Credenziali temporanee</a>	Sì
<a href="#">Autorizzazioni del principale</a>	Sì

Funzionalità IAM	Supporto ACM
<a href="#">Ruoli di servizio</a>	No
<a href="#">Ruoli collegati al servizio</a>	Sì

Per ottenere un quadro generale del funzionamento di ACM e altri servizi AWS con la maggior parte delle funzionalità di IAM, consulta [Servizi AWS supportati da IAM](#) nella Guida per l'utente di IAM.

## Policy basate su identità per ACM

Supporta le policy basate su identità	Sì
---------------------------------------	----

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

## Esempi di policy basate su identità per ACM

Per visualizzare esempi di policy basate sulle identità ACM, consulta [Esempi di policy basate su identità per AWS Certificate Manager](#).

## Policy basate sulle risorse all'interno di ACM

Supporta le policy basate su risorse	No
--------------------------------------	----

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust dei ruoli IAM e le policy dei

bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata su risorse rappresenta solo una parte della relazione di attendibilità. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

## Operazioni di policy per ACM

Supporta le azioni di policy

Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più azioni in una policy. Queste azioni aggiuntive sono denominate azioni dipendenti.

Includi le azioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di operazioni ACM, consulta [Operazioni definite da AWS Certificate Manager](#) nella Guida di riferimento per l'autorizzazione del servizio.

Le operazioni delle policy in ACM utilizzano il seguente prefisso prima dell'operazione:

```
acm
```

Per specificare più azioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di policy basate sulle identità ACM, consulta [Esempi di policy basate su identità per AWS Certificate Manager](#).

## Risorse di policy per ACM

Supporta le risorse di policy

Si

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (\*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco di tipi di risorse ACM e dei relativi ARN, consulta [Risorse definite da AWS Certificate Manager](#) nella Guida di riferimento per l'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione [Operazioni definite da AWS Certificate Manager](#).

Per visualizzare esempi di policy basate sulle identità ACM, consulta [Esempi di policy basate su identità per AWS Certificate Manager](#).

## Chiavi di condizione delle policy per ACM

Supporta le chiavi di condizione delle policy specifiche del servizio Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione OR logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta [Chiavi di contesto delle condizioni globali di AWS](#) nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione ACM, consulta [Chiavi di condizione per AWS Certificate Manager](#) nella Guida di riferimento per l'autorizzazione del servizio. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta la sezione [Operazioni definite da AWS Certificate Manager](#).

Per visualizzare esempi di policy basate sulle identità ACM, consulta [Esempi di policy basate su identità per AWS Certificate Manager](#).



## ACL in ACM

Supporta le ACL

No

Le policy di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

## ABAC con ACM

Supporta ABAC (tag nelle policy)

Parziale

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Partial (Parziale).

Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con le fasi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

## Utilizzo di credenziali temporanee con ACM

Supporta le credenziali temporanee

Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta [Servizi AWS supportati da IAM](#) nella Guida per l'utente di IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi alla AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Cambio di un ruolo \(console\)](#) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWS consiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

## Autorizzazioni del principale tra servizi per ACM

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì
--	----

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un'entità principale. Quando utilizzi alcuni servizi, puoi eseguire un'operazione che attiva un'altra operazione in un servizio differente. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altre risorse o Servizi AWS per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Inoltro sessioni di accesso](#).

## Ruoli di servizio per ACM

Supporta i ruoli di servizio	No
------------------------------	----

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per

ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.

#### Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di ACM. Modifica i ruoli di servizio solo quando ACM fornisce le indicazioni per farlo.

## Ruoli collegati ai servizi per ACM

Supporta i ruoli collegati ai servizi	Si
---------------------------------------	----

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta [Servizi AWS supportati da IAM](#). Trova un servizio nella tabella che include un Yes nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Esempi di policy basate su identità per AWS Certificate Manager

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse di ACM. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da ACM, incluso il formato degli ARN per ogni tipo di risorsa, consulta [Operazioni, risorse e chiavi di condizione per AWS Certificate Manager](#) nella Guida di riferimento per l'autorizzazione del servizio.

## Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console ACM](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Elenco dei certificati](#)
- [Recupero di un certificato](#)
- [Importazione di un certificato](#)
- [Eliminazione di un certificato](#)

## Best practice per le policy

Le policy basate sulle identità determinano se qualcuno può creare, accedere o eliminare risorse di ACM nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di

servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per IAM Access Analyzer](#) nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Configurazione dell'accesso alle API protetto con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

## Utilizzo della console ACM

Per accedere alla console AWS Certificate Manager è necessario disporre di un insieme di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario che concedi le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per essere certi che gli utenti e i ruoli possano continuare a utilizzare la console ACM, collega alle entità anche la policy gestita da AWS *AWSCertificateManagerReadOnly* ACM. Per ulteriori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente IAM.

## Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le

autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API AWS.

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

## Elenco dei certificati

La policy seguente permette all'utente di elencare tutti i certificati ACM sull'account dell'utente.

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

```
{
  "Effect": "Allow",
  "Action": "acm:ListCertificates",
  "Resource": "*"
}
```

### Note

Questa autorizzazione è obbligatoria affinché i certificati ACM compaiano sulle console Elastic Load Balancing e CloudFront.

## Recupero di un certificato

La policy seguente permette all'utente di recuperare uno specifico certificato ACM.

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

## Importazione di un certificato

La policy seguente permette all'utente di importare un certificato.

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

## Eliminazione di un certificato

La policy seguente permette all'utente di cancellare uno specifico certificato ACM.

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

## Autorizzazioni API ACM: operazioni e riferimento alle risorse

Quando si configura il controllo degli accessi e si scrivono policy di autorizzazione che possono essere collegate a un utente o ruolo IAM, è possibile utilizzare la tabella seguente come riferimento. La prima colonna della tabella elenca ogni operazione API AWS Certificate Manager. È possibile specificare le operazioni nell'elemento `Action` di una policy. Le restanti colonne forniscono ulteriori informazioni:

Per esprimere le condizioni, è possibile usare gli elementi di policy IAM nelle policy ACM. Per un elenco completo, consulta [Chiavi disponibili](#) nella guida per l'utente di IAM.

### Note

Per specificare un'operazione, utilizza il prefisso `acm:` seguito dal nome dell'operazione API (ad esempio, `acm:RequestCertificate`).

### Autorizzazioni e operazioni dell'API ACM

Operazioni dell'API ACM	Autorizzazioni obbligatorie (Operazioni API)	Risorse
<a href="#">AddTagsToCertificate</a>	<code>acm:AddTagsToCertificate</code>	<code>arn:aws:acm:<i>region</i>:<i>account</i>:certificate/<i>certificate_ID</i></code>



Operazioni dell'API ACM	Autorizzazioni obbligatorie (Operazioni API)	Risorse
<a href="#">DeleteCertificate</a>	acm:DeleteCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">DescribeCertificate</a>	acm:DescribeCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">ExportCertificate</a>	acm:ExportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">GetAccountConfiguration</a>	acm:GetAccountConfiguration	*
<a href="#">GetCertificate</a>	acm:GetCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">ImportCertificate</a>	acm:ImportCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/*  oppure  *
<a href="#">ListCertificates</a>	acm:ListCertificates	*
<a href="#">ListTagsForCertificate</a>	acm:ListTagsForCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">PutAccountConfiguration</a>	acm:PutAccountConfiguration	*

Operazioni dell'API ACM	Autorizzazioni obbligatorie (Operazioni API)	Risorse
<a href="#">RemoveTagsFromCertificate</a>	acm:RemoveTagsFromCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">RequestCertificate</a>	acm:RequestCertificate	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/*  oppure  *
<a href="#">ResendValidationEmail</a>	acm:ResendValidationEmail	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>
<a href="#">UpdateCertificateOptions</a>	acm:UpdateCertificateOptions	arn:aws:acm: <i>region</i> : <i>account</i> :certificate/ <i>certificate_ID</i>

## AWS Policy gestite da per AWS Certificate Manager

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni

una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

## AWSCertificateManagerReadOnly

Questa policy fornisce accesso in sola lettura ai certificati ACM e consente agli utenti di descrivere, elencare e recuperare certificati ACM.

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

Per visualizzare la policy gestita da AWS nella console, consulta <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly>.

## AWSCertificateManagerFullAccess

Questa policy fornisce accesso completo a tutte le operazioni e risorse ACM.

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

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

Per visualizzare questa policy gestita da AWS nella console, consulta <https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess>.

## Aggiornamenti di ACM alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per ACM da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina [Cronologia dei documenti](#) di ACM

Modifica	Descrizione	Data
Aggiunta del supporto <code>GetAccountConfiguration</code> per la policy <a href="#">AWSCertificateManagerReadOnly</a> .	La policy <code>AWSCertificateManagerReadOnly</code> ora include l'autorizzazione per chiamare l'azione dell'API <code>GetAccountConfiguration</code> .	3 marzo 2021
ACM avvia il monitoraggio delle modifiche	ACM inizia a monitorare le modifiche per le policy gestite da AWS.	3 marzo 2021

## Utilizzo delle chiavi di condizione con ACM

AWS Certificate Manager utilizza le [chiavi di condizione](#) di AWS Identity and Access Management (IAM) per limitare l'accesso alle richieste di certificati. Con le chiavi di condizione delle policy IAM o delle policy di controllo dei servizi (SCP) puoi creare richieste di certificati conformi alle linee guida della tua organizzazione.

### Note

Combina le chiavi di condizione ACM con le [chiavi di condizione globali](#) di AWS, ad esempio `aws:PrincipalArn`, per limitare ulteriormente le azioni a utenti o ruoli specifici.

## Condizioni supportate per ACM

### Operazioni API ACM e condizioni supportate

Chiave di condizione	Operazioni API ACM supportate	Type (Tipo)	Descrizione
<code>acm:ValidationMethod</code>	<a href="#">RequestCertificate</a>	Stringa (EMAIL, DNS)	Filtra le richieste in base al <a href="#">metodo di convalida</a> ACM

Chiave di condizione	Operazioni API ACM supportate	Type (Tipo)	Descrizione
acm:DomainNames	<a href="#">RequestCertificate</a>	ArrayOfString	Filtra in base ai <a href="#">nomi di dominio</a> nella richiesta ACM
acm:KeyAlgorithm	<a href="#">RequestCertificate</a>	Stringa	Filtra le richieste in base all' <a href="#">algoritmo della chiave e alle dimensioni</a> ACM
acm:CertificateTransparencyLogging	<a href="#">RequestCertificate</a>	Stringa (ENABLED, DISABLED)	Filtra le richieste in base alle <a href="#">preferenze di registrazione della trasparenza del certificato</a> ACM
acm:CertificateAuthority	<a href="#">RequestCertificate</a>	ARN	Filtra le richieste in base alle <a href="#">autorità di certificazione</a> nella richiesta ACM

## Esempio 1: limitazione del metodo di convalida

La seguente policy nega nuove richieste di certificati utilizzando il metodo di [convalida e-mail](#) tranne che per una richiesta effettuata utilizzando il ruolo `arn:aws:iam::123456789012:role/AllowedEmailValidation`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "acm:RequestCertificate",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acm:ValidationMethod": "EMAIL"
        }
      }
    }
  ]
}
```

```

    },
    "ArnNotLike": {
      "aws:PrincipalArn": [ "arn:aws:iam::123456789012:role/
AllowedEmailValidation" ]
    }
  }
}
}

```

## Esempio 2: prevenzione dei domini jolly

La seguente policy nega qualsiasi nuova richiesta di certificato ACM che utilizza domini jolly.

```

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

```

## Esempio 3: limitazione dei domini dei certificati

La seguente policy nega qualsiasi nuova richiesta di certificato ACM per i domini che non terminano con \*.amazonaws.com

```

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

```

```

    "Action": "acm:RequestCertificate",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringNotLike": {
        "acm:DomainNames": ["*.amazonaws.com"]
      }
    }
  }
}

```

La politica potrebbe essere ulteriormente limitata a sottodomini specifici. Questa policy consentirebbe solo le richieste in cui ogni dominio corrisponde ad almeno uno dei nomi di dominio condizionali.

```

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

```

#### Esempio 4: limitazione dell'algoritmo della chiave

La seguente policy utilizza la chiave di condizione `StringNotLike` per consentire solo i certificati richiesti con l'algoritmo della chiave ECDSA a 384 bit (`EC_secp384r1`).

```

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

```



```

    "Condition":{
      "StringNotLike" : {
        "acm:KeyAlgorithm":"EC_secp384r1"
      }
    }
  }
}

```

La seguente policy utilizza la combinazione di chiave di condizione `StringLike` e carattere jolly `*` per impedire richieste di nuovi certificati in ACM con qualsiasi algoritmo della chiave RSA.

```

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

```

## Esempio 5: limitazione dell'autorità di certificazione

La seguente policy consentirebbe solo le richieste di certificati privati utilizzando l'ARN dell'autorità di certificazione privata (PCA) fornito.

```

{
  "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"
    }
}
}
}

```

Questa policy utilizza la condizione `acm:CertificateAuthority` per consentire solo le richieste di certificati pubblicamente attendibili emessi da Amazon Trust Services. L'impostazione dell'ARN dell'autorità di certificazione su `false` impedisce le richieste di certificati privati da parte della PCA.

```

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

```

## Utilizzo di un ruolo collegato ai servizi (SLR) con ACM

AWS Certificate Manager utilizza un [ruolo collegato al servizio AWS Identity and Access Management](#) (IAM) per consentire il rinnovo automatico dei certificati ACM gestiti. Un ruolo collegato ai servizi (SLR) è un tipo univoco di ruolo IAM collegato direttamente a un servizio ACM. I SLR sono definiti automaticamente da ACM e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Il SLR semplifica la configurazione di ACM perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie per la firma automatica del certificato. ACM definisce le autorizzazioni di questo SLR e, salvo diversamente definito, solo ACM potrà assumere tale ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i SLR, consulta [ServiziAWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli un link Yes (Sì) per visualizzare la documentazione relativa al SLR per tale servizio.

## Autorizzazioni SLR per ACM

ACM utilizza una SLR denominata policy sui ruoli di servizio Certificate Manager di Amazon.

La `AWSServiceRoleForCertificateManager` SLR si affida ai seguenti servizi per l'assunzione del ruolo:

- `acm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad ACM di eseguire le seguenti operazioni sulle risorse specificate:

- Operazioni: `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` su ""

Per permettere a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un SLR devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

### Important

ACM potrebbe avvisarti che non è in grado di determinare se esiste un SLR sul tuo account. Se l'autorizzazione `iam:GetRole` richiesta è già stata concessa ad ACM SLR per il tuo account, l'avviso non si ripeterà dopo la creazione del SLR. In caso di ripetizione, l'utente o l'amministratore dell'account potrebbe essere necessario concedere l'autorizzazione `iam:GetRole` ad ACM o associare il proprio account con il `AWSCertificateManagerFullAccess` della policy gestito da ACM.

## Creazione del SLR per ACM

Non devi creare manualmente il SLR utilizzato da ACM. Quando emetti un certificato ACM utilizzando l'AWS Management Console, la o l'AWS API AWS CLI, ACM crea la SLR per te la prima volta che scegli una CA privata per firmare il tuo certificato.

Se ricevi messaggi che indicano che ACM non è in grado di determinare se esiste una reflex sul tuo account, è possibile che il tuo account non abbia concesso l'autorizzazione di lettura necessaria. CA privata AWS Ciò non impedirà l'installazione del SLR e sarà comunque possibile emettere certificati, ma ACM non sarà in grado di rinnovare automaticamente i certificati finché non verrà risolto il problema. Per ulteriori informazioni, consulta [Problemi con il ruolo collegato al servizio ACM](#).

#### Important

Questo SLR può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Inoltre, se utilizzavi il servizio ACM prima del 1° gennaio 2017, quando ha iniziato a supportare le reflex, ACM ha creato il ruolo nel tuo account. `AWSServiceRoleForCertificateManager` Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo SLR e quindi devi crearlo di nuovo, puoi utilizzare uno dei seguenti metodi:

- Nella console IAM, scegli Role, Create role, Certificate Manager per creare un nuovo ruolo con lo `CertificateManagerServiceRolePolicy` use case.
- Utilizzando l'API IAM [CreateServiceLinkedRole](#) o il AWS CLI comando corrispondente [create-service-linked-role](#), crea una SLR con il nome del `acm.amazonaws.com` servizio.

Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Modifica del SLR per ACM

ACM non consente di modificare il ruolo collegato al `AWSServiceRoleForCertificateManager` servizio. Dopo aver creato il SLR, non puoi modificare il relativo ruolo perché varie entità possono farvi riferimento. Tuttavia, utilizzando IAM è possibile modificarne la descrizione. Per ulteriori informazioni, consulta la sezione [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Eliminazione del SLR per ACM

In genere non è necessario eliminare la reflex. `AWSServiceRoleForCertificateManager` Tuttavia, puoi eliminare il ruolo manualmente utilizzando la console IAM, AWS CLI o l' AWS API. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Regioni supportate per i SLR ACM

ACM supporta l'utilizzo di reflex in tutte le regioni in cui sono disponibili sia ACM che ACM. CA privata AWS Per ulteriori informazioni, consulta [AWS Regioni ed endpoint di](#) .

Nome Regione	Identità della regione	Supporto in ACM
US East (N. Virginia)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
US West (N. California)	us-west-1	Sì
US West (Oregon)	us-west-2	Sì
Asia Pacific (Mumbai)	ap-south-1	Sì
Asia Pacifico (Osaka-Locale)	ap-northeast-3	Sì
Asia Pacifico (Seul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Canada (Central)	ca-central-1	Sì
Europe (Frankfurt)	eu-central-1	Sì
Europa (Zurigo)	eu-central-2	Sì
Europa (Irlanda)	eu-west-1	Sì
Europe (London)	eu-west-2	Sì
Europe (Paris)	eu-west-3	Sì
Sud America (São Paulo)	sa-east-1	Sì
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	Sì

Nome Regione	Identità della regione	Supporto in ACM
AWS GovCloud (Stati Uniti orientali) Est	us-gov-east-1	Sì

## Risoluzione dei problemi di identità e accesso in AWS Certificate Manager

Utilizza le seguenti informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di ACM e IAM.

### Argomenti

- [Non sono autorizzato a eseguire un'operazione in ACM](#)
- [Non sono autorizzato a richiedere un certificato in ACM](#)
- [Non sono autorizzato a eseguire iam:PassRole](#)
- [Desidero consentire alle persone esterne al mio Account AWS di accedere alle mie risorse ACM](#)

### Non sono autorizzato a eseguire un'operazione in ACM

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni `acm:GetWidget` fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione `acm:GetWidget`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

### Non sono autorizzato a richiedere un certificato in ACM

Se ricevi questo errore, significa che l'amministratore ACM o PKI ha impostato delle regole che impediscono di richiedere il certificato nello stato attuale.

Il seguente errore di esempio si verifica quando un utente IAM prova a utilizzare la console per richiedere un certificato utilizzando opzioni configurate con DENY dall'amministratore dell'organizzazione.

```
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 questo caso, la richiesta deve essere effettuata nuovamente in modo conforme alle policy impostate dall'amministratore. Oppure la policy deve essere aggiornata per consentire la richiesta del certificato.

## Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo ad ACM.

Alcuni Servizi AWS consentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in ACM. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Desidero consentire alle persone esterne al mio Account AWS di accedere alle mie risorse ACM

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se ACM supporta queste funzionalità, consulta [Funzionamento di AWS Certificate Manager con IAM](#).
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di proprietà dell'utente](#) nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta [Fornire l'accesso agli Account AWS di proprietà di terze parti](#) nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

## Resilienza in AWS Certificate Manager

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

## Sicurezza dell'infrastruttura nell' AWS Certificate Manager

In quanto servizio gestito, AWS Certificate Manager è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.



Utilizzate chiamate API AWS pubblicate per accedere ad ACM attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

## Concessione dell'accesso programmatico ad ACM

Gli utenti necessitano di un accesso programmatico se desiderano interagire con l' AWS esterno di AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente</a>.AWS Command Line Interface</li> <li>• Per AWS SDK, strumenti e AWS API, consulta <a href="#">l'autenticazione IAM Identity Center</a> nella Guida di</li> </ul>

Quale utente necessita dell'accesso programmatico?	Per	Come
		riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporanee e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in <a href="#">Uso delle credenziali temporanee con AWS risorse</a> nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Autenticazione tramite credenziali utente IAM nella Guida per l'utente</a>.AWS Command Line Interface</li> <li>• Per gli AWS SDK e gli strumenti, consulta <a href="#">Autenticazione tramite credenziali a lungo termine</a> nella Guida di riferimento agli SDK e agli AWS strumenti.</li> <li>• Per le AWS API, consulta <a href="#">Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM</a>.</li> </ul>

## Best practice

Le best practice sono consigli che possono aiutarti a utilizzare AWS Certificate Manager (AWS Certificate Manager) in modo più efficace. Le seguenti best practice sono basate sull'esperienza pratica dei clienti ACM attuali.

## Argomenti

- [AWS CloudFormation](#)
- [Associazione dei certificati](#)
- [Convalida del dominio](#)
- [Aggiunta o eliminazione di nomi di dominio](#)
- [Annullamento della registrazione della trasparenza del certificato.](#)
- [Attiva AWS CloudTrail](#)

## AWS CloudFormation

Con AWS CloudFormation puoi creare un modello che descriva le AWS risorse che desideri utilizzare. AWS CloudFormation quindi effettua il provisioning e configura tali risorse per te. AWS CloudFormation può fornire risorse supportate da ACM come Elastic Load Balancing, Amazon e CloudFront Amazon API Gateway. Per ulteriori informazioni, consulta [Servizi integrati con AWS Certificate Manager](#).

Se lo utilizzi AWS CloudFormation per creare ed eliminare rapidamente più ambienti di test, ti consigliamo di non creare un certificato ACM separato per ogni ambiente. In questo modo il limite di certificato si esaurirà in breve tempo. Per ulteriori informazioni, consulta [Quote](#). Al contrario, è necessario creare un certificato jolly che copra tutti i nomi di dominio utilizzati per il test. Ad esempio, se si creano ripetutamente certificati ACM per nomi di dominio che hanno una variazione solo nel numero della versione, come `<version>.service.example.com`, creare invece un singolo certificato jolly per `<*>.service.example.com`. Includi il certificato wildcard nel modello AWS CloudFormation utilizzato per creare il tuo ambiente di test.

## Associazione dei certificati

Il processo di associazione del certificato, conosciuto anche come associazione del SSL, può essere utilizzato nella propria applicazione per convalidare un host remoto, associando tale host direttamente con il suo certificato X.509 o con una chiave di accesso pubblica anziché con una gerarchia di certificato. L'applicazione quindi utilizza l'associazione per bypassare la convalida della catena di certificato SSL/TLS. Il processo di convalida di un SSL tipico verifica le firme in tutta la catena di certificato dall'autorità di certificazione (CA) della root tramite il certificato CA subordinato eventuale. Verifica inoltre il certificato per l'host remoto in fondo alla gerarchia. L'applicazione può invece bloccare il certificato per l'host remoto dicendo che solo quel certificato è attendibile, non il

certificato root né tantomeno altri certificati nella catena. È possibile aggiungere il certificato dell'host remoto o la chiave di accesso pubblica per l'applicazione durante la fase di sviluppo. In alternativa, l'applicazione è in grado di aggiungere il certificato o la chiave di accesso quando si connette al primo host.

#### Warning

È consigliabile che l'applicazione non associ un certificato ACM. ACM esegue [Rinnovo gestito per i certificati ACM](#) per rinnovare automaticamente i certificati SSL/TLS emessi da Amazon prima della loro scadenza. Per rinnovare un certificato, ACM genera una nuova coppia di chiavi di accesso pubblica-privata. Se l'applicazione associa il certificato ACM e il certificato viene rinnovato correttamente con una nuova chiave di accesso pubblica, l'applicazione potrebbe non essere in grado di stabilire una connessione con il dominio.

Se decidi di associare un certificato, le seguenti opzioni non ostacoleranno l'applicazione nella connessione al tuo dominio:

- [Importa il tuo certificato](#) in ACM, quindi associa l'applicazione al certificato importato. ACM non prova a rinnovare automaticamente i certificati importati.
- Se stai utilizzando un certificato pubblico, aggiungi la tua applicazione a tutti i [certificati root Amazon](#) disponibili. Se stai utilizzando un certificato privato, aggiungi la tua applicazione a un certificato root CA.

## Convalida del dominio

Prima che l'autorità di certificazione Amazon (CA) possa emettere un certificato per il tuo sito, AWS Certificate Manager (ACM) deve verificare che tu possieda o controlli tutti i domini che hai specificato nella richiesta. È possibile eseguire la verifica tramite e-mail o DNS. Per ulteriori informazioni, consultare [Convalida DNS](#) e [Convalida e-mail](#).

## Aggiunta o eliminazione di nomi di dominio

Non è possibile aggiungere né rimuovere i nomi di dominio da un certificato ACM esistente. Invece è necessario richiedere un nuovo certificato con l'elenco rivisto dei nomi di dominio. Ad esempio, se il certificato ha cinque nomi di dominio e si desidera aggiungerne altri quattro, è necessario richiedere un nuovo certificato con tutti i nove nomi di dominio. Così come per qualsiasi nuovo

certificato, è necessario convalidare la proprietà di tutti i nomi di dominio nella richiesta, inclusi i nomi precedentemente convalidati per il certificato originale.

Se utilizzi la convalida e-mail, riceverai fino a 8 messaggi e-mail di convalida per ogni dominio, almeno 1 dei quali deve essere coinvolto entro 72 ore. Ad esempio, quando si richiede un certificato con cinque nomi di dominio, si riceveranno fino a 40 messaggi di convalida, almeno 5 dei quali dovranno essere coinvolti entro 72 ore. All'aumentare del numero di nomi di dominio nella richiesta di certificato, aumenterà anche il lavoro necessario per l'utilizzo di e-mail per convalidare la proprietà del dominio.

Se utilizzi la convalida del DNS invece, è necessario scrivere un nuovo record DNS al database per l'FQDN da convalidare. ACM invia il registro per creare e per richiedere in un secondo momento il database per determinare se il registro è stato aggiunto. L'aggiunta del record conferma che controlli il dominio e che questo ti appartiene. In questo esempio, se si richiede un certificato con cinque nomi di dominio, è necessario creare cinque record DNS. È consigliabile utilizzare la convalida del DNS quando possibile.

## Annullamento della registrazione della trasparenza del certificato.

### Important

Indipendentemente dalle operazioni eseguite per annullare la registrazione della trasparenza del certificato, quest'ultimo potrebbe comunque essere annullato da qualsiasi client o singolo dotato di accesso a endpoint pubblici o privati a cui si vincola il certificato. Tuttavia, il certificato non conterrà una marca temporale di certificato firmato (Signed Certificate Timestamp, SCT). Solo la CA emittente è in grado di incorporare un SCT in un certificato.

A partire dal 30 aprile 2018, Google Chrome interromperà la concessione di fiducia ai certificati SSL/TLS pubblici che non verranno registrati in un registro di trasparenza del certificato. Pertanto, a partire dal 24 aprile 2018, la CA di Amazon inizierà a pubblicare tutti i nuovi certificati e i rinnovi per almeno due log pubblici. Una volta che un certificato è stato registrato, non può essere rimosso. Per ulteriori informazioni, consulta [Registrazione della trasparenza del certificato](#).

La registrazione viene eseguita automaticamente quando si richiede un certificato o quando un certificato viene rinnovato, ma è possibile scegliere di annullarlo. I motivi più comuni per l'annullamento sono legati alla sicurezza e alla privacy. Ad esempio, la registrazione di nomi di dominio di un host interno offre ai potenziali aggressori informazioni relative alle reti interne che

altrimenti non sarebbero pubbliche. Inoltre, la registrazione potrebbe perdere i nomi di prodotti e siti Web nuovi o non ancora rilasciati.

Per disattivare la registrazione in trasparenza quando richiedi un certificato, utilizza il `options` parametro del comando [request-certificate](#) o l'operazione API AWS CLI . [RequestCertificate](#)  
Se il certificato è stato emesso prima del 24 aprile 2018 e vuoi assicurarti che non venga registrato durante il rinnovo, puoi utilizzare il [update-certificate-options](#) comando o l'operazione [UpdateCertificateOptions](#) API per disattivarlo.

## Limitazioni

- Non puoi utilizzare la console per abilitare o disabilitare la registrazione della trasparenza.
- Non è possibile modificare lo stato di registrazione dopo che un certificato ha immesso il periodo di rinnovo, in genere 60 giorni prima della scadenza del certificato. Se una modifica dello stato non riesce, non viene generato alcun messaggio di errore.

Una volta che un certificato è stato registrato, non può essere rimosso dal log. A quel punto l'annullamento non avrà alcun effetto. Se si annulla la registrazione al momento della richiesta del certificato e si sceglie poi di ripristinarlo, il certificato non sarà registrato fino al suo rinnovo. Se si desidera che il certificato venga registrato subito, è preferibile emetterne uno nuovo.

L'esempio seguente mostra come utilizzare il comando [request-certificate](#) per disabilitare la trasparenza di certificato al momento della richiesta di un nuovo certificato.

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

```

Il comando precedente emette l'ARN del nuovo certificato.

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

Se disponi già di un certificato e non desideri che venga registrato al momento del rinnovo, usa il [update-certificate-options](#) comando. Il comando non restituisce un valore.

```
aws acm update-certificate-options \  

```

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

## Attiva AWS CloudTrail

Attiva CloudTrail la registrazione prima di iniziare a utilizzare ACM. CloudTrail ti consente di monitorare le tue AWS implementazioni recuperando una cronologia delle chiamate AWS API per il tuo account, incluse le chiamate API effettuate tramite la Console di AWS gestione, gli AWS SDK e Amazon Web Services di livello superiore. AWS Command Line Interface È anche possibile inoltre identificare quali utenti e quali account hanno chiamato le API ACM, da quale indirizzo IP di origine sono state effettuate le chiamate e quando sono avvenute. Puoi integrarti CloudTrail nelle applicazioni utilizzando l'API, automatizzare la creazione di percorsi per la tua organizzazione, controllare lo stato dei percorsi e controllare come gli amministratori attivano e disattivano l'accesso. CloudTrail Per ulteriori informazioni, consultare l'articolo relativo alla [Creazione di un trail](#). Visita [Utilizzo con CloudTrail AWS Certificate Manager](#) per visualizzare i trail di esempio per le operazioni ACM.

# Configurazione

Con AWS Certificate Manager (ACM) è possibile eseguire il provisioning e gestire i certificati SSL/TLS per i siti Web e le applicazioni basati su AWS. Utilizzi ACM per creare o importare e successivamente gestire un certificato. È necessario utilizzare altri servizi AWS per distribuire il certificato sul sito Web o sull'applicazione. Per ulteriori informazioni sui servizi integrati con ACM, consulta [Servizi integrati con AWS Certificate Manager](#). Le sezioni seguenti illustrano i passaggi da eseguire prima di utilizzare ACM.

## Argomenti

- [Registrarsi per creare un Account AWS](#)
- [Creazione di un utente amministratore](#)
- [Registrare un nome di dominio](#)
- [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#)
- [\(Opzionale\) Configurazione di un registro CAA](#)

## Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

### Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, [assegna l'accesso amministrativo a un utente amministrativo](#) e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo <https://aws.amazon.com/> e selezionando Il mio account.



# Creazione di un utente amministratore

Dopo aver effettuato la registrazione di un Account AWS, proteggi l'utente root dell'account AWS, abilita AWS IAM Identity Center e crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

## Protezione dell'utente root dell'account AWS

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo l'utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Accesso come utente root](#) della Guida per l'utente di Accedi ad AWS.

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per ricevere istruzioni, consulta [Abilitazione di un dispositivo MFA virtuale per l'utente root dell'Account AWS \(console\)](#) nella Guida per l'utente IAM.

## Creazione di un utente amministratore

1. Abilita Centro identità IAM.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center.

2. In Centro identità IAM, assegna l'accesso amministrativo a un utente amministratore.

Per un tutorial sull'utilizzo di IAM Identity Center directory come origine di identità, consulta [Configure user access with the default IAM Identity Center directory](#) nella Guida per l'utente di AWS IAM Identity Center.

## Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [Accedere al portale di accesso AWS](#) nella Guida per l'utente Accedi ad AWS.

## Registrazione un nome di dominio

Un nome di dominio completo (FQDN) è il nome univoco di un'organizzazione o di un singolo su Internet seguito da un'estensione di dominio di primo livello, ad esempio .com o .org. Se non hai ancora registrato un nome di dominio, è possibile registrarne uno tramite Amazon Route 53 o tramite uno dei registrar commerciali. In genere, è possibile visitare il sito Web del registrar e richiedere un nome di dominio. Il registrar richiede al WHOIS di determinare se l'FQDN richiesto è disponibile. In tal caso, il registrar in genere elenca i nomi correlati che differiscono dall'estensione del dominio e offre la possibilità di acquisire uno dei nomi disponibili. La registrazione di solito dura un periodo di tempo determinato, ad esempio uno o due anni prima che debba essere rinnovata.

Per ulteriori informazioni sulla registrazione dei nomi di dominio con Amazon Route 53, vedi [Registrazione di nomi di dominio con Amazon Route 53](#) nella Guida per sviluppatori di Amazon Route 53 Developer.

## (Facoltativo) Configurazione dell'e-mail per il dominio in uso

### Note

Le seguenti fasi sono necessarie solo se si utilizza la convalida e-mail per la conferma della proprietà o del controllo del nome di dominio completo (FQDN) specificato nella richiesta di certificato. Prima dell'emissione di un certificato, in ACM devi convalidare la tua proprietà o il tuo controllo. È possibile utilizzare la convalida dell'email o la convalida del DNS. Per ulteriori informazioni sulla convalida e-mail, consultare [Convalida e-mail](#).

Se si è in grado di modificare la configurazione DNS, si consiglia di utilizzare la convalida del dominio DNS anziché la convalida email. La convalida DNS evita la necessità di configurare l'email per il nome di dominio. Per ulteriori informazioni sulla convalida DNS, consulta [Convalida DNS](#).

Usare il sito Web del registrar di riferimento per associare gli indirizzi di contatto con il nome di dominio. Il registrar aggiunge gli indirizzi e-mail di contatto al database WHOIS e aggiunge uno o più server di posta elettronica ai record Mail Exchanger (MX) di un server DNS. Se scegli di utilizzare la convalida e-mail, ACM invia e-mail agli indirizzi di contatto e a cinque indirizzi di amministrazione comuni formati dal tuo registro MX. ACM invia fino a otto messaggi e-mail di convalida ogni volta che crei un nuovo certificato, rinnovi un certificato o richiedi una nuova e-mail di convalida. L'e-mail di convalida contiene le istruzioni per confermare che il proprietario del dominio o un rappresentante

designato approva il certificato ACM. Per ulteriori informazioni, consulta [Convalida e-mail](#). In caso di problemi relativi alla convalida e-mail, vedere [Risoluzione dei problemi di convalida e-mail](#).

## Database WHOIS

Il database WHOIS contiene informazioni di contatto per il dominio in uso. Per convalidare la tua identità, ACM invia un'e-mail ai seguenti tre indirizzi in WHOIS. È necessario accertarsi che le informazioni di contatto siano pubbliche o che l'email inviata a un indirizzo offuscato venga inoltrata all'indirizzo effettivo.

- Registrant del dominio
- Contatto tecnico
- Contatto amministrativo

## Registro MX

Quando l'utente registra il proprio dominio, il registrar invia i record di Mail Exchanger (MX) a un server Domain Name System (DNS). Un record MX indica quali server accettano mail per il dominio in uso. Il record contiene un nome di dominio completo (FQDN). È possibile richiedere un certificato per domini o sottodomini apex.

Ad esempio, se utilizzi la console per richiedere un certificato per `abc.xyz.example.com`, ACM prima cerca di individuare il registro MX per tale sottodominio. Se il registro non viene trovato, ACM esegue una ricerca MX per `xyz.example.com`. Se tale registro non viene trovato, ACM esegue una ricerca MX per `example.com`. Se tale registro non viene trovato o se non vi è alcun registro MX, ACM sceglie il dominio originale per il quale il certificato è stato richiesto (`abc.xyz.example.com` in questo esempio). ACM invia quindi l'e-mail ai seguenti cinque indirizzi di amministrazione di sistema comuni per il dominio o il sottodominio:

- `amministratore@nome-del-dominio`
- `hostmaster@nome-del-dominio`
- `postmaster@nome-del-dominio`
- `webmaster@nome-del-dominio`
- `admin@nome-del-dominio`

**Tip**

È possibile sostituire il dominio a cui vengono inviati i messaggi di convalida. Se si utilizza l'operazione [ResendValidationEmailAPI](#) o il [resend-validation-email](#) AWS CLI comando, AWS non esegue una ricerca MX. Al contrario, si fornisce il nome di dominio registrato e il nome di un dominio di convalida personalizzato e AWS invia i precedenti cinque messaggi e-mail al dominio di convalida, anziché al dominio registrato dell'utente.

ACM invia sempre le e-mail di convalida ai cinque indirizzi comuni elencati in precedenza, indipendentemente dal fatto che si stia utilizzando la console, l'API o la AWS CLI. Tuttavia, AWS esegue una ricerca MX solo quando si utilizza la console per richiedere un certificato.

Se non si riceve l'e-mail di convalida, vedere [Mancata ricezione dell'e-mail di convalida](#) per informazioni su possibili cause e soluzioni alternative.

## (Opzionale) Configurazione di un registro CAA

È possibile configurare facoltativamente un record DNS di tipo CAA (Certification Authority Authorization) per specificare che il servizio AWS Certificate Manager (ACM) è autorizzato a emettere un certificato per il tuo dominio o sottodominio. Dopo aver convalidato il dominio, ACM verifica la presenza di un registro CAA per accertarsi che può emettere un certificato. Puoi scegliere di non configurare un record CAA per il dominio se non vuoi consentire il controllo CAA.

Un record CAA contiene i seguenti campi dati:

### flags

Specifica se il valore del campo tag è supportato da ACM. Impostare questo valore su 0.

### tag

Il campo tag può essere uno dei seguenti valori. Si noti che il campo iodef è attualmente ignorato.

### issue

Indica che la CA ACM specificata nel campo value è autorizzata a emettere un certificato per il dominio o sottodominio.

## issuewild

Indica che la CA ACM specificata nel campo value è autorizzata a emettere un certificato jolly per il dominio o sottodominio. Un certificato jolly si applica al dominio o sottodominio e a tutti i suoi sottodomini.

## value

Il valore di questo campo dipende dal valore del campo tag. È necessario racchiudere questo valore tra virgolette ("").

Quando tag è issue

Il campo value contiene il nome di dominio CA. Il campo può contenere il nome di una CA diversa dalla CA Amazon. Tuttavia, se non disponi di un registro CAA che specifichi una delle seguenti quattro CA Amazon, ACM non può emettere un certificato per il dominio o sottodominio:

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

Il campo value può anche contenere un punto e virgola (;) per indicare che nessuna CA deve essere autorizzata a emettere un certificato per il dominio o sottodominio. Utilizzare questo campo se si decide in un secondo momento che un certificato non deve più essere emesso per un determinato dominio.

Quando tag è issuewild

Il campo value è lo stesso di quando tag è issue ad eccezione del fatto che il valore si applica a certificati con caratteri jolly.

Quando è presente un registro CAA issuewild che non include un valore ACM CA, non è possibile emettere caratteri jolly mediante ACM. Se non è presente issuewild ma è presente un registro CAA issue per ACM, i caratteri jolly possono essere emessi mediante ACM.

## Example Esempi di record CAA

Negli esempi seguenti, il nome di dominio è il primo elemento, seguito dal tipo di record (CAA). Il campo flags è sempre 0. Il campo tags può essere issue o issuewild. Se il campo è issue e il tipo

di nome di dominio è un server CA nel campo value, il record CAA indica che il server specificato è autorizzato a emettere il certificato richiesto. Se si digita un punto e virgola (;) nel campo value, il record CAA indica che nessuna CA è autorizzata a emettere un certificato. La configurazione dei record CAA varia a seconda del provider DNS.

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

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

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

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

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

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

Per ulteriori informazioni su come aggiungere o modificare record DNS, consultare il provider DNS. Route 53 supporta i registri CAA. Se il provider DNS è Route 53, consulta [Formato CAA Format](#) per ulteriori informazioni su come creare un registro.

# Rilascio e gestione dei certificati

I certificati ACM possono essere utilizzati per stabilire comunicazioni protette su Internet o su una rete interna. È possibile richiedere un certificato pubblicamente attendibile direttamente da ACM (un "certificato ACM") o importare un certificato pubblicamente attendibile emesso da una terza parte. Sono supportati anche i certificati autofirmati. Per eseguire il provisioning della PKI interna dell'organizzazione, puoi emettere certificati ACM firmati da un'autorità di certificazione (CA) privata creata e gestita da [CA privata AWS](#). La CA può essere dere nel tuo account o essere condivisa con te da un altro account.

## Note

I certificati ACM pubblici possono essere installati su istanze Amazon EC2 connesse a un'[Enclave Nitro](#), ma non su altre istanze di Amazon EC2. Per informazioni sulla configurazione di un server Web autonomo su un'istanza Amazon EC2 non connessa a Nitro Enclave, vedi [Tutorial: Installa un server Web LAMP su Amazon Linux 2](#) o [Tutorial: installa un server Web LAMP con Amazon Linux AMI](#).

## Note

Poiché i certificati firmati da una CA privata non sono considerati attendibili per impostazione predefinita, gli amministratori devono installarli in archivi client attendibili.

[Per iniziare a emettere certificati, accedi alla console di AWS gestione e apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/home>](#). Se viene visualizzata la pagina introduttiva, scegli Get Started (Inizia). In caso contrario, scegli Certificate Manager o Private CAs (CA private) nel pannello di navigazione a sinistra.

## Argomenti

- [Richiesta di un certificato pubblico](#)
- [Richiesta di un certificato PKI privato](#)
- [Convalida della proprietà del dominio](#)
- [Elenco dei certificati gestiti da ACM](#)
- [Descrizione dei certificati ACM](#)

- [Eliminazione di certificati gestiti da ACM](#)
- [Installazione dei certificati ACM](#)

## Richiesta di un certificato pubblico

Nelle sezioni seguenti viene illustrato come utilizzare la console ACM o AWS CLI richiedere un certificato ACM pubblico. Dopo aver richiesto un certificato pubblico, è necessario completare una delle procedure descritte in [Convalida della proprietà del dominio](#).

I certificati ACM pubblici sono conformi allo standard X.509 e sono soggetti alle seguenti restrizioni:

- **Nomi:** è necessario utilizzare nomi di soggetti conformi al DNS. Per ulteriori informazioni, consulta [Nomi di dominio](#).
- **Algoritmo:** per la crittografia, l'algoritmo della chiave privata del certificato deve essere RSA a 2048 bit, ECDSA a 256 bit o ECDSA a 384 bit.
- **Scadenza:** ogni certificato è valido per 13 mesi (395 giorni).
- **Rinnovo:** ACM tenta di rinnovare automaticamente un certificato privato dopo 11 mesi.

Se si verificano problemi durante la richiesta di un certificato, consulta [Risoluzione dei problemi relativi alle richieste di certificato](#).

Per richiedere un certificato per l'utilizzo CA privata AWS di una PKI privata, consulta [Richiesta di un certificato PKI privato](#)

### Note

Gli amministratori possono utilizzare le [policy delle chiavi di condizione](#) ACM per controllare il modo in cui gli utenti finali emettono nuovi certificati. Queste chiavi di condizione consentono di applicare restrizioni su domini, metodi di convalida e altri attributi relativi a una richiesta di certificato.

### Note

Se non si sceglie di annullare, i certificati ACM pubblicamente attendibili vengono automaticamente registrati in almeno due database di trasparenza di certificati. Al momento, non è possibile utilizzare la console per annullare. È necessario utilizzare AWS CLI o l'API



ACM. Per ulteriori informazioni, consulta [Annullamento della registrazione della trasparenza del certificato](#). Per informazioni generali sui log di trasparenza, consulta [Registrazione della trasparenza del certificato](#).

## Argomenti

- [Richiedere un certificato pubblico utilizzando la console](#)
- [Richiesta di un certificato pubblico utilizzando CLI](#)

## Richiedere un certificato pubblico utilizzando la console

Per richiedere un certificato pubblico ACM (console)

1. [Accedi alla console di AWS gestione e apri la console ACM all'indirizzo `https://console.aws.amazon.com/acm/home`](https://console.aws.amazon.com/acm/home).

Scegli Request a certificate (Richiedi un certificato).

2. Nella sezione Domain names (Nomi di dominio) digitare il nome di dominio.

È possibile utilizzare un nome di dominio completo (FQDN) come **www.example.com** o un nome di dominio essenziale o apex come **example.com**. È inoltre possibile utilizzare un asterisco (\*) come carattere jolly nella posizione più a sinistra per proteggere diversi nomi di siti nello stesso dominio. Ad esempio, **\*.example.com** protegge **corp.example.com** e **images.example.com**. Il nome del carattere jolly apparirà nel campo Subject (Oggetto) e nell'estensione Subject Alternative Name (Nome oggetto alternativo) del certificato ACM.

Quando si fa richiesta di un certificato jolly, l'asterisco (\*) deve essere nella posizione più a sinistra nel nome di dominio e può proteggere solo un livello di sottodominio. Ad esempio, **\*.example.com** può proteggere **login.example.com** e **test.example.com**, ma non può proteggere **test.login.example.com**. Si noti inoltre come **\*.example.com** protegga solo i sottodomini di **example.com** e non il dominio essenziale o apex (**example.com**). Per proteggere entrambi, consulta la fase successiva.

### Note

In conformità con [RFC 5280](#), la lunghezza del nome di dominio (tecnicamente, il nome comune) immesso in questo passaggio non può superare i 64 ottetti (caratteri), compresi

i punti. Ogni successivo nome alternativo soggetto (SAN), tuttavia, può contenere fino a 253 ottetti.

Per aggiungere un altro nome, scegli **Aggiungi un altro nome** al certificato e digita il nome nella casella di testo. Questo è utile per proteggere sia un dominio essenziale o apex (ad esempio **example.com**) che i relativi sottodomini (**\*.example.com**).

3. Nella sezione **Validation method** (Metodo di convalida), scegli **DNS validation – recommended** (Convalida del DNS – consigliata) o **Email validation** (Convalida dell'e-mail), a seconda delle esigenze.

#### Note

Se si è in grado di modificare la configurazione DNS, si consiglia di utilizzare la convalida del dominio DNS anziché la convalida email. La convalida del DNS offre diversi vantaggi rispetto alla convalida dell'email. Per informazioni, consulta [Convalida DNS](#).

Prima di emettere un certificato, ACM convalida la proprietà e il controllo dei nomi di dominio nella richiesta di certificato. È possibile utilizzare la convalida dell'email o la convalida del DNS.

Se scegli la convalida tramite email, ACM invia un'e-mail di convalida a tre indirizzi di contatto registrati nel database WHOIS e a cinque indirizzi comuni di amministrazione del sistema per ciascun nome di dominio. L'utente o un rappresentante autorizzato deve rispondere a uno di questi messaggi e-mail. Per ulteriori informazioni, consulta [Convalida e-mail](#).

Se usi la convalida DNS, è sufficiente aggiungere un registro CNAME fornito da ACM nella configurazione DNS. Per ulteriori informazioni sulla convalida DNS, consulta [Convalida DNS](#).

4. Nella sezione **Key algorithm** (Algoritmo chiave), scegli uno dei tre algoritmi disponibili:
  - RSA 2048 (impostazione predefinita)
  - ECDSA P 256
  - ECDSA P 384

Per informazioni su come scegliere un algoritmo, consulta [Algoritmi chiave](#) il post AWS sul blog [Come valutare e utilizzare i certificati ECDSA](#) in *AWS Certificate Manager*

5. Nella pagina Tags (Tag) è possibile taggare facoltativamente il certificato. I tag sono coppie chiave-valore che fungono da metadati per identificare e organizzare le risorse. AWS Per un elenco dei parametri dei tag ACM e per istruzioni su come aggiungere tag ai certificati dopo la creazione, consulta [Tagging di certificati AWS Certificate Manager](#).

Al termine dell'aggiunta di tag, scegli Request (Richiesta).

6. Dopo l'elaborazione della richiesta, la console ti riporta all'elenco dei certificati, dove vengono visualizzate le informazioni relative al nuovo certificato.

Un certificato entra nello stato Convalida in attesa al momento della richiesta, a meno che non abbia esito negativo per uno dei motivi indicati nell'argomento di risoluzione dei problemi [Errore nella richiesta di certificato](#). ACM effettua ripetuti tentativi di convalidare un certificato per 72 ore, dopodiché va in time out. Se un certificato mostra lo stato Failed (Non riuscito) o Validation timed out (Convalida scaduta), elimina la richiesta, correggi l'errore con [DNS validation](#) (Convalida DNS) o [Email validation](#) (Convalida e-mail) e riprova. Se la convalida ha esito positivo, il certificato entra nello stato Issued (Emesso).

#### Note

A seconda di come hai ordinato l'elenco, un certificato che stai cercando potrebbe non essere immediatamente visibile. È possibile fare clic sul triangolo nero a destra per modificare l'ordine. È inoltre possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra.

## Richiesta di un certificato pubblico utilizzando CLI

Utilizza il comando [request-certificate](#) per richiedere un nuovo certificato ACM pubblico sulla riga di comando. I valori facoltativi per il metodo di convalida sono DNS ed EMAIL. I valori facoltativi per l'algoritmo chiave sono RSA\_2048 (l'impostazione predefinita se il parametro non viene fornito esplicitamente), EC\_Prime256v1 ed EC\_secp384r1.

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

Questo comando restituisce l'Amazon Resource Name (ARN) del nuovo certificato pubblico.

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

## Richiesta di un certificato PKI privato

Se hai accesso a una CA privata esistente creata da CA privata AWS, ACM può richiedere un certificato adatto all'uso nella tua PKI privata. La CA può essere dere nel tuo account o essere condivisa con te da un altro account. Per ulteriori informazioni sulla creazione di una CA privata, consulta [Creazione di una Private Certificate Authority](#).

Per impostazione predefinita, i certificati privati formati da una CA privata non sono considerati attendibili per impostazione predefinita. Di conseguenza, un amministratore deve intervenire per installarli negli archivi attendibili dei clienti dell'organizzazione.

I certificati ACM privati sono conformi allo standard X.509 e sono soggetti alle seguenti restrizioni:

- **Nomi:** è necessario utilizzare nomi di soggetti conformi al DNS. Per ulteriori informazioni, consulta [Nomi di dominio](#).
- **Algoritmo:** per la crittografia, l'algoritmo della chiave privata del certificato deve essere RSA a 2048 bit, ECDSA a 256 bit o ECDSA a 384 bit.

### Note

La famiglia di algoritmi di firma specificata (RSA o ECDSA) deve corrispondere alla famiglia di algoritmi della chiave segreta della CA.

- **Scadenza:** ogni certificato è valido per 13 mesi (395 giorni). La data di fine del certificato CA deve essere successiva alla data di fine del certificato richiesto o la richiesta del certificato non andrà a buon fine.
- **Rinnovo:** ACM tenta di rinnovare automaticamente un certificato privato dopo 11 mesi.

La CA privata utilizzata per firmare i certificati dell'entità finale è soggetta alle proprie restrizioni:

- Lo stato della CA deve essere Attivo.
- L'algoritmo a chiave privata CA deve essere RSA 2048 o RSA 4096.

### Note

A differenza dei certificati pubblicamente attendibili, i certificati firmati da una CA privata non richiedono una convalida.

## Argomenti

- [Configurazione dell'accesso a una CA privata](#)
- [Richiesta di un certificato PKI privato utilizzando la console ACM](#)
- [Richiesta di un certificato PKI privato utilizzando la CLI](#)

## Configurazione dell'accesso a una CA privata

Puoi utilizzare CA privata AWS per firmare i tuoi certificati ACM in uno dei due casi seguenti:

- Account singolo: la CA firmataria e il certificato ACM emesso risiedono nello stesso account. AWS

Per abilitare l'emissione e i rinnovi di account singoli, l'amministratore di CA privata AWS deve concedere l'autorizzazione al principale del servizio ACM per creare, recuperare ed elencare i certificati. [Questa operazione viene eseguita utilizzando l'azione CA privata AWS API CreatePermissiono il AWS CLI comando create-permission.](#) Il proprietario dell'account assegna queste autorizzazioni a un utente, gruppo o ruolo IAM responsabile del rilascio dei certificati.

- Cross-account: la CA che firma e il certificato ACM emesso risiedono in AWS account diversi e l'accesso alla CA è stato concesso all'account in cui risiede il certificato.

[Per consentire l'emissione e il rinnovo tra più account, l' CA privata AWS amministratore deve allegare alla CA una policy basata sulle risorse utilizzando l'azione API o il comando put-policy. CA privata AWSPutPolicyAWS CLI](#) La policy specifica le entità principali degli altri account a cui è consentito l'accesso limitato alla CA. Per ulteriori informazioni, consulta [Utilizzo di una policy basata sulle risorse con ACM Private CA.](#)

Lo scenario tra più account richiede inoltre che ACM configuri un ruolo collegato ai servizi (SLR) per interagire come entità principale con la policy PCA. ACM crea automaticamente il SLR durante il rilascio del primo certificato.

ACM potrebbe avvisarti che non è in grado di determinare se esiste un SLR sul tuo account. Se l'autorizzazione `iam:GetRole` richiesta è già stata concessa ad ACM SLR per il tuo account,

l'avviso non si ripeterà dopo la creazione del SLR. In caso di ripetizione, l'utente o l'amministratore dell'account potrebbe essere necessario concedere l'autorizzazione `iam:GetRole` ad ACM o associare il proprio account con il `AWSCertificateManagerFullAccess` della policy gestito da ACM.

Per ulteriori informazioni consulta [Utilizzo di un ruolo collegato ai servizi con ACM](#).

#### Important

Il certificato ACM deve essere associato attivamente a un servizio supportato prima di poter essere rinnovato automaticamente. AWS Per ulteriori informazioni sulle risorse supportate da ACM, consultare [Servizi integrati con AWS Certificate Manager](#).

## Richiesta di un certificato PKI privato utilizzando la console ACM

1. [Accedi alla console di AWS gestione e apri la console ACM all'indirizzo `https://console.aws.amazon.com/acm/home`](https://console.aws.amazon.com/acm/home).

Scegli Request a certificate (Richiedi un certificato).

2. Nella pagina Request certificate (Richiedi un certificato) scegli Request a private certificate (Richiedi un certificato privato) e Next (Avanti) per continuare.
3. Nella sezione Certificate authority details (Dettagli dell'autorità di certificazione), fai clic sul menu Certificate authority (Autorità di certificazione) e scegli una delle CA private disponibili. Se la CA è condivisa da un altro account, l'ARN precede le informazioni sulla proprietà.

Vengono visualizzate dettagli sulla CA per aiutarti a verificare di aver scelto la quella corretta:

- Proprietario
- Type (Tipo)
- Common name (CN) (Nome comune)
- Organizzazione (O)
- Organization unit (OU) (Unità organizzativa)
- Nome paese (C)
- State or province (Stato o provincia)
- Locality name (Nome località)

4. Nella sezione Domain names (Nomi di dominio) digita il nome di dominio. È possibile utilizzare un nome di dominio completo (FQDN) come **www.example.com** o un nome di dominio essenziale o apex come **example.com**. È inoltre possibile utilizzare un asterisco (\*) come carattere jolly nella posizione più a sinistra per proteggere diversi nomi di siti nello stesso dominio. Ad esempio, **\*.example.com** protegge **corp.example.com** e **images.example.com**. Il nome del carattere jolly apparirà nel campo Subject (Oggetto) e nell'estensione Subject Alternative Name (Nome oggetto alternativo) del certificato ACM.

#### Note

Quando si fa richiesta di un certificato jolly, l'asterisco (\*) deve essere nella posizione più a sinistra nel nome di dominio e può proteggere solo un livello di sottodominio. Ad esempio, **\*.example.com** può proteggere **login.example.com** e **test.example.com**, ma non può proteggere **test.login.example.com**. Si noti inoltre come **\*.example.com** protegga solo i sottodomini di **example.com** e non il dominio essenziale o apex (**example.com**). Per proteggere entrambi, consulta la fase successiva

Facoltativamente, puoi scegliere Aggiungi un altro nome al certificato e digitare il nome nella casella di testo. Questo è utile per autenticare sia un dominio essenziale o apex (ad esempio **example.com**) che i relativi sottodomini (**\*.example.com**).

5. Nella sezione Key algorithm (Algoritmo chiave), scegli uno dei tre algoritmi disponibili:
  - RSA 2048 (impostazione predefinita)
  - ECDSA P 256
  - ECDSA P 384

Per informazioni su come scegliere un algoritmo, consulta [Algoritmi chiave](#).

6. Nella sezione Tags (Tag) è possibile taggare facoltativamente il certificato. I tag sono coppie chiave-valore che fungono da metadati per identificare e organizzare le risorse. AWS Per un elenco dei parametri dei tag ACM e per istruzioni su come aggiungere tag ai certificati dopo la creazione, consulta [Tagging di certificati AWS Certificate Manager](#).
7. Nella sezione Certificate renewal permissions (Autorizzazioni di rinnovo dei certificati), riconosce l'avviso sulle autorizzazioni di rinnovo del certificato. Queste autorizzazioni consentono il rinnovo

automatico dei certificati PKI privati firmati con la CA selezionata. Per ulteriori informazioni consulta [Utilizzo di un ruolo collegato ai servizi con ACM](#).

8. Dopo aver fornito tutte le informazioni richieste, scegli Request (Richiesta). La console ti restituisce all'elenco dei certificati, dove puoi visualizzare il nuovo certificato.

#### Note

A seconda di come hai ordinato l'elenco, un certificato che stai cercando potrebbe non essere immediatamente visibile. È possibile fare clic sul triangolo nero a destra per modificare l'ordine. È inoltre possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra.

## Richiesta di un certificato PKI privato utilizzando la CLI

È possibile usare il comando [request-certificate](#) per richiedere un certificato privato in ACM.

#### Note

Quando si richiede un certificato PKI privato firmato da una CA presso AWS Private CA, la famiglia di algoritmi di firma specificata (RSA o ECDSA) deve corrispondere alla famiglia di algoritmi della chiave segreta della CA.

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

Questo comando restituisce l'Amazon Resource Name (ARN) del nuovo certificato privato.

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

Nella maggior parte dei casi, ACM assegna automaticamente un ruolo collegato ai servizi (SLR) all'account la prima volta che si utilizza una CA condivisa. Il SLR abilita il rinnovo automatico dei



certificati di entità finale rilasciati da te. Per verificare se il SLR è presente, è possibile eseguire una query IAM con il comando seguente:

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

Se il SLR è presente, l'output del comando dovrebbe essere simile al seguente:

```
{
  "Role":{
    "Path":"/aws-service-role/acm.amazonaws.com/",
    "RoleName":"AWSServiceRoleForCertificateManager",
    "RoleId":"AAAAAAA0000000BBBBBBB",
    "Arn":"arn:aws:iam::{account_no}:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager",
    "CreateDate":"2020-08-01T23:10:41Z",
    "AssumeRolePolicyDocument":{
      "Version":"2012-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"acm.amazonaws.com"
          },
          "Action":"sts:AssumeRole"
        }
      ]
    },
    "Description":"SLR for ACM Service for accessing cross-account Private CA",
    "MaxSessionDuration":3600,
    "RoleLastUsed":{
      "LastUsedDate":"2020-08-01T23:11:04Z",
      "Region":"ap-southeast-1"
    }
  }
}
```

Se manca il SLR, consulta [Utilizzo di un ruolo collegato ai servizi con ACM](#).

## Convalida della proprietà del dominio

Prima che l'autorità di certificazione (CA) di Amazon possa rilasciare un certificato per il tuo sito, AWS Certificate Manager (ACM) deve verificare che tu possieda o controlli tutti i nomi di dominio

specificati nella richiesta. Puoi scegliere di dimostrare la proprietà con la convalida Domain Name System (DNS) o con la convalida via e-mail al momento della richiesta di un certificato.

#### Note

La convalida si applica solo ai certificati pubblicamente attendibili rilasciati da ACM. ACM non convalida la proprietà del dominio per i [certificati importati](#) o per i certificati firmati da una CA privata. ACM non è in grado di convalidare le risorse in una [Zona ospitata privata](#) di Amazon VPC o qualsiasi altro dominio privato. Per ulteriori informazioni, consulta [Risoluzione dei problemi di convalida dei certificati](#).

In generale, consigliamo di utilizzare la convalida DNS tramite la convalida della posta elettronica per i seguenti motivi:

- Se utilizzi Amazon Route 53 per gestire i tuoi registri pubblici DNS, puoi aggiornarli direttamente tramite ACM.
- ACM rinnova automaticamente i certificati convalidati da DNS finché un certificato è in uso e il tuo registro CNAME rimane invariato.
- Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACM inizia a inviare avvisi di rinnovo 45 giorni prima della scadenza. Questi avvisi vanno agli indirizzi di posta elettronica WHOIS del dominio e a cinque indirizzi comuni di amministratore. Le notifiche contengono un link su cui il proprietario del dominio può cliccare per il rinnovo. Una volta convalidati tutti i domini elencati, ACM rilascia un certificato rinnovato con lo stesso ARN.

Se non hai l'autorizzazione per modificare il database DNS del tuo dominio, devi usare [convalida e-mail](#).

#### Note

Dopo aver creato un certificato con convalida e-mail, non è possibile passare alla convalida con DNS.

## Argomenti

- [Convalida DNS](#)

- [Convalida e-mail](#)

## Convalida DNS

Il Domain Name System (DNS) è un servizio di directory per le risorse connesso a una rete. Il provider DNS gestisce un database contenente registri cord che definiscono il dominio. Quando scegli la convalida DNS, ACM fornisce uno o più registri CNAME da essere aggiunti al database. Questi registri contengono una coppia chiave-valore univoca che serve come prova del controllo del dominio.

### Note

Dopo aver creato un certificato con convalida e-mail, non è possibile passare alla convalida con DNS.

Ad esempio, se richiedi un certificato per il dominio `example.com` con `www.example.com` come ulteriore nome, ACM crea due registri CNAME. Ogni record, creato in modo specifico per il tuo dominio e il tuo account, contiene un nome e un valore. Il valore è un alias che punta a un AWS dominio utilizzato da ACM per rinnovare automaticamente il certificato. Puoi aggiungere i registri CNAME al tuo database DNS solo una volta. ACM rinnova automaticamente il certificato finché il certificato è in uso e il tuo registro CNAME rimane invariato.

### Important

Se non usi Amazon Route 53 per gestire i tuoi registri pubblici DNS, contatta il tuo provider DNS per scoprire come aggiungere registri. Se non hai l'autorità per modificare il database DNS del tuo dominio, devi usare [convalida e-mail](#).

Senza la necessità di ripetere la convalida, puoi richiedere ulteriori certificati ACM per il nome di dominio completo (FQDN) finché il registro CNAME rimane al suo posto. Ciò significa che puoi creare certificati sostitutivi con lo stesso nome del dominio o certificati che coprono sottodomini diversi. Poiché il token di convalida CNAME funziona per qualsiasi AWS regione, puoi ricreare lo stesso certificato in più regioni. Puoi anche sostituire un certificato eliminato.

È possibile arrestare il rinnovo automatico rimuovendo il certificato dal servizio AWS associato o eliminando il registro CNAME. Se Route 53 non è il provider DNS, contatta il tuo provider per scoprire

come eliminare il registro. Se Route 53 è il tuo provider, consulta [Eliminazione di set di registri della risorsa](#) nella Guida per sviluppatori di Route 53. Per ulteriori informazioni sul rinnovo gestito del certificato, consulta [Rinnovo gestito per i certificati ACM](#).

#### Note

La risoluzione CNAME avrà esito negativo se più di cinque CNAME sono concatenati insieme nella configurazione DNS. Se hai bisogno di un concatenamento più lungo, ti consigliamo di usare [convalidaonvalida e-mail](#).

## Come funzionano i registri CNAME per ACM

#### Note

Questa sezione è destinata ai clienti che non utilizzano Route 53 come provider DNS.

Se non usi Route 53 come provider DNS, devi immettere manualmente i registri CNAME forniti da ACM nel database del provider, in genere tramite un sito Web. I registri CNAME vengono utilizzati per diversi scopi, tra cui come meccanismi di reindirizzamento e container per metadati specifici del fornitore. Per ACM, questi registri consentono la convalida iniziale della proprietà del dominio e il rinnovo automatico dei certificati.

La tabella riportata di seguito mostra un esempio di registri CNAME per sei nomi del dominio. Ogni coppia di registri Nome registro-Valore registro serve per autenticare la proprietà del nome di dominio.

Nella tabella, si noti che le prime due coppie Nome registro-Valore registro sono le stesse. Questo dimostra che per un dominio jolly, come \*.example.com, le stringhe create da ACM sono le stesse di quelle create per il suo dominio di base, example.com. In caso contrario, la coppia Nome registro e Valore registro differiscono per ciascun nome di dominio.

### Esempio di registri CNAME

Nome dominio	Nome registro	Valore registro	Commento
*.example.com	<u>_x1</u> .example.com.	<u>_x2</u> .acm-validations.a ws.	Identico

Nome dominio	Nome registro	Valore registro	Commento
esempio.com	<code>_x1.example.com.</code>	<code>_x2.acm-validations.aws.</code>	
www.example.com	<code>_x3.www.example.com.</code>	<code>_x4.acm-validations.aws.</code>	Unique
host.example.com	<code>_x5.host.example.com.</code>	<code>_x6.acm-validations.aws.</code>	Unique
sottodominio.esempio.com	<code>_x7.subdomain.example.com.</code>	<code>_x8.acm-validations.aws.</code>	Unique
host.subdomain.example.com	<code>_x9.host.subdomain.example.com.</code>	<code>_x10.acm-validations.aws.</code>	Unique

I valori `xN` che seguono un trattino basso ( `_` ) sono lunghe stringhe generate da ACM. Ad esempio,

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

è il rappresentante di un Nome registro risultante generato. Il Valore registro associato potrebbe essere

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

per lo stesso registro DNS.

#### Note

Se il provider DNS non supporta i valori CNAME con il trattino basso che li precede, vedi [Risoluzione dei problemi di convalida DNS](#).

Quando richiedi un certificato e specifichi la convalida DNS, ACM fornisce informazioni CNAME nel formato seguente:

Nome dominio	Nome registro	Tipo di registro	Valore registro
esempio. om	_a79865eb4cd1a6ab990a45779b 4e0b96.example.com.	CNAME	_424c7224e9b0146f9a8808af95 5727d0.acm-validations.aws.

Nome dominio è il nome FQDN associato al certificato. Nome registro identifica il registro in modo univoco, fungendo da chiave della coppia chiave-valore. Valore registro serve come valore della coppia chiave-valore.

Tutti e tre questi valori (Nome dominio, Nome registro, e Valore registro) devono essere immessi nei campi appropriati dell'interfaccia Web del provider DNS per l'aggiunta di registri DNS. I provider non hanno tutti lo stesso approccio nella gestione del campo nome registro (o semplicemente "nome"). In alcuni casi, dovrai fornire l'intera stringa come mostrato sopra. Altri provider aggiungono automaticamente il nome di dominio a qualsiasi stringa immessa, il che significa (in questo esempio) che dovresti inserire solo

```
_a79865eb4cd1a6ab990a45779b4e0b96
```

nel campo del nome. Se per errore immetti un nome di registro che contiene un nome di dominio (ad esempio *example.com*), potrebbe accadere quanto segue:

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

La convalida fallisce in questo caso. Di conseguenza, dovresti provare a stabilire in anticipo che tipo di input si aspetta il tuo provider.

## Configurazione della convalida DNS

In questa sezione viene descritto come configurare un certificato pubblico per utilizzare la convalida DNS.

## Per impostare la convalida DNS nella console

### Note

Questa procedura presuppone che tu abbia già creato almeno un certificato e che tu stia lavorando nella AWS regione in cui lo hai creato. Se provi ad aprire la console e visualizzi invece la schermata per il primo utilizzo oppure riesci ad aprire la console e non vedi il tuo certificato nell'elenco, conferma di aver specificato la regione corretta.

1. Apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/>.
2. Nell'elenco dei certificati, scegli Certificate ID (ID del certificato) di un certificato con lo stato Pending validation (Convalida in attesa) che intendi configurare. Viene visualizzata una pagina dei dettagli per il certificato.
3. Nella sezione Domains (Domini), completare una delle seguenti due procedure:
  - a. (Facoltativo) Convalida con Route 53.

Un pulsante attivo Create records in Route 53 (Crea registri in Route 53) viene visualizzato se le condizioni seguenti sono vere:

- Usi Route 53 come provider DNS.
- Hai l'autorizzazione per scrivere nella zona ospitata da Route 53.
- Il FQDN non è stato ancora convalidato.

### Note

Se usi Route 53 ma il pulsante Crea registri in Route 53 manca o è disattivato, consulta [La console ACM non visualizza il pulsante "Crea record in Route 53"](#).


Scegli il pulsante Create records in Route 53 (Crea registri in Route 53), quindi scegli Create records (Crea registri). La pagina Certificate status (Stato del certificato) dovrebbe essere aperta con un banner di stato che visualizza Successfully created DNS records (Registri DNS creati con successo).

Il nuovo certificato potrebbe ancora visualizzare lo stato Pending validation (Convalida in attesa) per un massimo di 30 minuti.

 Tip

Non è possibile richiedere a livello di programmazione che ACM crei automaticamente i registri in Route 53. Tuttavia, puoi effettuare una chiamata AWS CLI o una chiamata API a Route 53 per creare il record nel database DNS di Route 53. Per ulteriori informazioni sui set di registri di Route 53, consulta [Lavorare con set di registri della risorsa](#).

- b. (Facoltativo) Se non usi Route 53 come provider DNS, devi recuperare le informazioni CNAME e aggiungerle al database DNS. Nella pagina dei dettagli del nuovo certificato, è possibile farlo in due modi:
- Copia i componenti CNAME visualizzati nella sezione Domains (Domini). Queste informazioni devono ancora essere aggiunte manualmente al database DNS.
  - In alternativa, scegli Export to CSV (Esporta in CSV). Le informazioni contenute nel file risultante devono essere aggiunte manualmente al database DNS.

 Important

Per evitare problemi di convalida, consulta [Come funzionano i registri CNAME per ACM](#) prima di aggiungere informazioni al database del provider DNS. Se riscontri problemi, consulta [Risoluzione dei problemi di convalida DNS](#).

Se ACM non è in grado di convalidare il nome del dominio entro 72 ore dal momento in cui genera un valore CNAME per l'utente, ACM modifica lo stato del certificato su Validation timed out (Convalida scaduta). La ragione più probabile di questo risultato è che non è stata aggiornata la configurazione DNS con il valore generato da ACM. Per risolvere questo problema, è necessario richiedere un nuovo certificato dopo aver controllato le istruzioni CNAME.

## Convalida e-mail

Prima che l'autorità di certificazione Amazon (CA) possa emettere un certificato per il tuo sito, AWS Certificate Manager (ACM) deve verificare che tu possieda o controlli tutti i domini che hai specificato



nella richiesta. È possibile eseguire la verifica tramite e-mail o DNS. Questo argomento tratta la convalida tramite e-mail. Per informazioni sulla convalida DNS, consulta [Convalida DNS](#).

Osserva le seguenti considerazioni sulla convalida delle e-mail.

- Hai bisogno di un indirizzo email funzionante registrato nel tuo dominio per poter utilizzare la convalida dell'e-mail. Le procedure per la configurazione di un indirizzo e-mail non rientrano nell'ambito di questa guida.
- La convalida si applica solo ai certificati pubblicamente attendibili rilasciati da ACM. ACM non convalida la proprietà del dominio per i [certificati importati](#) o per i certificati firmati da una CA privata. ACM non è in grado di convalidare le risorse in una [Zona ospitata privata](#) di Amazon VPC o qualsiasi altro dominio privato. Per ulteriori informazioni, consulta [Risoluzione dei problemi di convalida dei certificati](#).
- Dopo aver creato un certificato con convalida e-mail, non è possibile passare alla convalida con DNS.

I certificati ACM sono validi per 13 mesi (395 giorni). Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACM inizia a inviare avvisi di rinnovo 45 giorni prima della scadenza, utilizzando gli indirizzi della casetta postale WHOIS del dominio e a cinque indirizzi amministratore comuni. Le notifiche contengono un link su cui il proprietario del dominio può cliccare per il rinnovo. Una volta convalidati tutti i domini elencati, ACM rilascia un certificato rinnovato con lo stesso ARN.

In caso di problemi con la convalida dell'email, consulta [Risoluzione dei problemi di convalida e-mail](#).

ACM invia e-mail ai tre indirizzi di contatto elencati nel database WHOIS e ai cinque indirizzi di amministrazione del sistema per ogni dominio specificato. Ciò significa che verranno inviati fino a otto messaggi e-mail per ogni nome di dominio e nome di oggetto alternativo inclusi nella richiesta. Ad esempio, se specifichi un solo nome di dominio, riceverai fino a otto messaggi e-mail. Per la convalida, è necessario agire su uno di questi otto messaggi entro 72 ore. Se specifichi tre nomi di dominio, riceverai fino a 24 messaggi. Per la convalida, è necessario agire almeno su tre di queste e-mail, una per ogni nome specificato, entro 72 ore.

I messaggi e-mail vengono inviati ai seguenti tre indirizzi di contatto registrati in WHOIS:

- Registrant del dominio
- Contatto tecnico

- Contatto amministrativo

**Note**

È fortemente consigliato configurare e monitorare i cinque indirizzi di sistema comuni per il certificato. Il recupero delle informazioni di contatto da WHOIS non è affidabile. La percentuale di successo delle ricerche WHOIS è bassa (inferiore al 5%), in parte a causa della conformità alle leggi globali sulla privacy.

**Important**

A partire da giugno 2024, ACM non supporterà la nuova convalida delle e-mail tramite gli indirizzi di contatto WHOIS. Per i certificati esistenti, a partire da ottobre 2024, ACM non invierà avvisi di rinnovo agli indirizzi di contatto WHOIS del dominio. ACM continuerà a inviare e-mail di convalida ai cinque indirizzi di sistema comuni per il dominio richiesto. Per maggiori dettagli, consulta [AWS Certificate Manager Interromperà la ricerca WHOIS per i certificati convalidati](#) tramite e-mail

Se utilizzi la console per richiedere un certificato, ACM esegue una ricerca MX per determinare quali server accettano l'e-mail per il tuo dominio e invia l'e-mail ai successivi 5 indirizzi di sistema comuni per il primo dominio trovato. Se si utilizza l'[RequestCertificate](#) API o il AWS CLI comando [request-certificate](#), ACM non esegue una ricerca MX. Al contrario, invia l'e-mail al nome di dominio specificato nel parametro `DomainName` o nel parametro `ValidationDomain` opzionale. Per ulteriori informazioni, consulta [Registro MX](#).

- `amministratore@nome-del-dominio`
- `hostmaster@nome-del-dominio`
- `postmaster@nome-del-dominio`
- `webmaster@nome-del-dominio`
- `admin@nome-del-dominio`

Per ulteriori informazioni su come ACM determina gli indirizzi e-mail per i domini, consultare [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#).

## Eccezione a questo processo

Se richiedi un certificato ACM per un nome di dominio che inizia con **www** o un carattere jolly asterisco (\*), ACM rimuove **www** o l'asterisco iniziale e invia l'e-mail agli indirizzi amministrativi. Questi indirizzi sono formati anteponendo **admin@**, **administrator@**, **hostmaster@**, **postmaster@** e **webmaster@** alla parte restante del nome di dominio. Ad esempio, se richiedi un certificato ACM per **www.example.com**, l'e-mail viene inviata ad **admin@example.com** anziché ad **admin@www.example.com**. Analogamente, se richiedi un certificato ACM per **\*.test.example.com**, l'e-mail viene inviata ad **admin@test.example.com**. Gli altri indirizzi amministrativi comuni vengono formati in modo analogo.

### Note

Verifica che l'e-mail venga inviata agli indirizzi amministrativi per un dominio apex, ad esempio **example.com**, piuttosto che agli indirizzi amministrativi per un sottodominio, ad esempio **test.example.com**. [Per farlo, specifica l'opzione nell'API o nel comando `request-certificate`. `ValidationDomainRequestCertificate`](#) AWS CLI Questa funzionalità non è attualmente supportata quando si utilizza la console per richiedere un certificato. Anche quando tutti i messaggi vengono inviati a un unico indirizzo di posta elettronica, è necessario rispondere a un messaggio per ogni dominio o sottodominio per convalidarlo e generare il certificato.

## Scadenza e rinnovo dei certificati

I certificati ACM sono validi per 13 mesi (395 giorni). Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACM inizia a inviare avvisi di rinnovo 45 giorni prima della scadenza, utilizzando gli indirizzi della casetta postale WHOIS del dominio e a cinque indirizzi amministratore comuni. Le notifiche contengono un link su cui il proprietario del dominio può cliccare per il rinnovo. Una volta convalidati tutti i domini elencati, ACM rilascia un certificato rinnovato con lo stesso ARN.

Consultare [Convalida e-mail](#), sopra, per ulteriori informazioni.

### (Facoltativo) Rinvio dell'e-mail di convalida

Ogni e-mail di convalida contiene un token che puoi utilizzare per approvare una richiesta di certificato. Tuttavia, poiché l'e-mail di convalida necessaria per il processo di approvazione può

essere bloccata da filtri antispam o smarrita durante il transito, il token scade automaticamente dopo 72 ore. Se non hai ricevuto l'e-mail originale o il token è scaduto, puoi richiedere un nuovo invio dell'e-mail.

Per problemi persistenti con la convalida tramite e-mail, consulta la sezione [Risoluzione dei problemi di convalida e-mail](#) in [Risoluzione dei problemi](#).

#### Note

Le informazioni seguenti si applicano solo ai certificati forniti da ACM e solo ai certificati che utilizzano la convalida tramite e-mail. L'e-mail di convalida non è necessaria per i certificati PKI privati o per [i certificati importati in ACM](#). Per informazioni sulla convalida del dominio DNS, consulta [Convalida DNS](#).

Per il rinvio dell'e-mail di convalida usando la console

1. [Accedi alla console di AWS gestione e apri la console ACM all'indirizzo https://console.aws.amazon.com/acm/home](https://console.aws.amazon.com/acm/home).
2. Nell'elenco dei certificati, scegli Certificate ID (ID del certificato) di certificato che intendi convalidare. Questa operazione apre una pagina dei dettagli.

#### Note

A seconda di come hai ordinato l'elenco, un certificato che stai cercando potrebbe non essere immediatamente visibile. È possibile fare clic sul triangolo nero a destra per modificare l'ordine. È inoltre possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra.

3. Nella sezione Domains (Domini), scegli Resend validation email (Invia di nuovo l'e-mail di convalida), seleziona ciascuno dei domini che richiedono la convalida, quindi scegli Resend (Rinvio). Il banner Successfully resent validation emails (Reinvio con successo delle e-mail di convalida) viene visualizzato.

Per inviare nuovamente l'e-mail di convalida con AWS CLI

È possibile utilizzare il [resend-validation-email](#) comando per inviare nuovamente l'e-mail.

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

### Note

Il [resend-validation-email](#) comando si applica solo ai certificati ACM per i quali si utilizza la convalida e-mail. La convalida non è necessaria per i certificati importati in ACM o per i certificati privati gestiti utilizzando ACM.

## Elenco dei certificati gestiti da ACM

È possibile utilizzare la console ACM o AWS CLI elencare i certificati gestiti da ACM. La console può elencare fino a 500 certificati in una pagina e la CLI fino a 1000.

Per elencare certificati tramite la console

1. Apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/>.
2. Esaminare le informazioni nell'elenco dei certificati. È possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra. Ogni certificato occupa una riga con le seguenti colonne visualizzate per impostazione predefinita per ogni certificato:
  - Nome dominio – Il nome di dominio completo (FQDN) per il certificato.
  - Type (Tipo): il tipo di certificato. I valori possibili sono: Amazon issued (Rilasciato da Amazon)|Private (Privato)|Imported (Importato)
  - Stato – Stato del certificato. I valori possibili sono: Pending validation (Convalida in attesa) | Issued (Emesso) | Inactive (Inattivo) | Expired (Scaduto) | Revoked (Revocato) | Failed (Non riuscito) | Validation timed out (Convalida scaduta)
  - In use? (In uso?) — Se il certificato ACM è associato attivamente a un AWS servizio come Elastic Load CloudFront Balancing o. Il valore può essere No o Sì.
  - Idoneità al rinnovo: se il certificato può essere rinnovato automaticamente da ACM quando si avvicina la scadenza. I valori possibili sono: Idoneo | Non idoneo. Per le regole di idoneità, consulta [Rinnovo gestito per i certificati ACM](#).

Scegliendo l'icona delle impostazioni nell'angolo superiore destro della console, puoi personalizzare il numero di certificati visualizzati su una pagina, specificare il comportamento di avvolgimento delle righe del contenuto delle celle e visualizzare campi di informazioni aggiuntivi. Sono disponibili i seguenti campi facoltativi:

- Nomi di dominio aggiuntivi: uno o più nomi di dominio (nomi alternativi dell'oggetto) inclusi nel certificato.
- Richiesto a: momento in cui ACM ha richiesto il certificato.
- Emesso alle: ora in cui è stato emesso il certificato. Queste informazioni sono disponibili solo per i certificati emessi da Amazon, non per quelli importati.
- Non prima: l'ora prima della quale il certificato non è valido.
- Non dopo: l'ora dopo la quale il certificato non è valido.
- Revocato il: per i certificati revocati, il momento della revoca.
- Nome tag: il valore di un tag su questo certificato chiamato Nome, se tale tag esiste.
- Stato di rinnovo: stato del rinnovo richiesto di un certificato. Questo campo viene visualizzato e ha un valore solo quando è stato richiesto il rinnovo. I valori possibili sono: Rinnovo automatico in sospeso | Convalida in sospeso | Successo | Errore.

#### Note

È possibile che le modifiche di stato per il certificato impieghino diverse ore per diventare disponibili. Se si verifica un problema, la richiesta di certificato scade dopo 72 ore e il processo di emissione o rinnovo deve essere ripetuto dall'inizio.

La preferenza Page size (Dimensione pagina) specifica il numero di certificati restituiti in ogni pagina della console.

Per ulteriori informazioni sui dettagli di certificato disponibili, consulta [Descrizione dei certificati ACM](#).

Per elencare i certificati utilizzando il AWS CLI

Usa il comando [list-certificates](#) per elencare i certificati gestiti da ACM come illustrato nell'esempio seguente:

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

Questo comando restituisce informazioni simili alle seguenti:

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

Per impostazione predefinita, vengono restituiti solo i certificati con keyTypes RSA\_1024 o RSA\_2048 e con almeno un dominio specificato. Per visualizzare altri certificati controllati, ad esempio certificati senza dominio o certificati che utilizzano un algoritmo o una dimensione bit diversa, specifica il parametro `--includes` come illustrato nell'esempio seguente. Il parametro consente di specificare un membro della struttura [Filtri](#).

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

# Descrizione dei certificati ACM


Puoi utilizzare la console ACM o AWS CLI per elencare metadati dettagliati sui tuoi certificati.

Per visualizzare i dettagli del certificato nella console

1. Per visualizzare i certificati apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/>. È possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra.
2. Per visualizzare i metadati dettagliati per un certificato elencato, scegli l'ID certificato. Si apre una pagina che visualizza le seguenti informazioni:
  - Stato del certificato
    - Identificatore: identificatore univoco esadecimale a 32 byte del certificato
    - ARN: un Amazon Resource Name (ARN) nel modulo `arn:aws:acm:Region:444455556666:certificate/certificate_ID`
    - Tipo: identifica la categoria di gestione di un certificato ACM. I valori possibili sono: Rilasciato da Amazon | Privato | Importato. Per ulteriori informazioni, consulta [Richiesta di un certificato pubblico](#), [Richiesta di un certificato PKI privato](#) o [Importazione di certificati in AWS Certificate Manager](#).
    - Stato: stato del certificato. I valori possibili sono: Pending validation (Convalida in attesa) | Issued (Emesso) | Inactive (Inattivo) | Expired (Scaduto) | Revoked (Revocato) | Failed (Non riuscito) | Validation timed out (Convalida scaduta)
    - Stato dettagliato: data e ora in cui il certificato è stato emesso o importato
  - Domini
    - Nome dominio: il nome di dominio completo (FQDN) per il certificato.
    - Stato: lo stato di convalida del dominio. I valori possibili sono: Pending validation (Convalida in attesa) | Revoked (Revocato) | Failed (Non riuscito) | Validation timed out (Convalida scaduta) | Success (Riuscito)
  - Dettagli
    - In use? (In uso?) — Indica se il certificato è associato a un [servizio integrato AWS](#) I valori possibili sono: Sì | No
    - Nome dominio: il primo nome di dominio pienamente qualificato (FQDN) per il certificato.
    - Numero di nomi aggiuntivi: numero di nomi di dominio per i quali il certificato è valido
    - Numero di serie: numero di serie esadecimale a 16 byte del certificato



- Informazioni sulla chiave pubblica: l'algoritmo di crittografia che ha generato la coppia di chiavi
- Algoritmo di firma: l'algoritmo crittografico usato per firmare il certificato.
- Può essere utilizzato con: un elenco di [servizi integrati](#) ACM che supportano un certificato con questi parametri
- Richiesto il: data e ora della richiesta di emissione
- Rilasciato il: se applicabile, la data e l'ora dell'emissione
- Importato il: se applicabile, la data e l'ora dell'importazione
- Non prima: inizio del periodo di validità del certificato
- Non dopo: la data e l'ora di scadenza del certificato
- Idoneità al rinnovo: i valori possibili sono: Idoneo | Non idoneo. Per le regole di idoneità, consulta [Rinnovo gestito per i certificati ACM](#).
- Stato di rinnovo: stato del rinnovo richiesto di un certificato. Questo campo viene visualizzato e ha un valore solo quando è stato richiesto il rinnovo. I valori possibili sono: Rinnovo automatico in sospeso | Convalida in sospeso | Successo | Errore.

 Note

È possibile che le modifiche di stato per il certificato impieghino diverse ore per diventare disponibili. Se si verifica un problema, la richiesta di certificato scade dopo 72 ore e il processo di emissione o rinnovo deve essere ripetuto dall'inizio.

- CA: l'ARN della CA firmataria
- Tag
  - Key (Chiave)
  - Value (Valore)
- Stato di convalida — Se applicabile, i valori possibili sono:
  - In attesa — La convalida è stata richiesta e non è stata completata.
  - Convalida scaduta— La convalida richiesta è scaduta, ma è possibile ripetere la richiesta.
  - Nessuno — Il certificato è per una PKI privata o è autofirmato e non necessita di convalida.

Per visualizzare i dettagli dei certificati, utilizzare il AWS CLI

Utilizzate il [comando `describe-certificate`](#) in AWS CLI per visualizzare i dettagli del certificato, come illustrato nel comando seguente:

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

Questo comando restituisce informazioni simili alle seguenti:

```
{
  "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"
}
```

## Eliminazione di certificati gestiti da ACM

È possibile utilizzare la console ACM o AWS CLI eliminare un certificato.

### Important

- Non puoi eliminare un certificato ACM utilizzato da un altro servizio AWS . Per eliminare un certificato in uso, è necessario prima rimuovere l'associazione del certificato. Questa operazione viene eseguita utilizzando la console o la CLI per il servizio associato.
- L'eliminazione di un certificato emesso da un'autorità di certificazione (CA) privata non ha alcun effetto sulla CA. I costi dell'autorità di certificazione continueranno a essere addebitati fino all'eliminazione. Per ulteriori informazioni consulta la pagina [Eliminazione della CA privata](#) nella Guida per l'utente dell'AWS Private Certificate Authority .

Per eliminare un certificato CA utilizzando la console

1. Apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/>.
2. Nell'elenco dei certificati, seleziona la casella di controllo per un certificato ACM, poi scegli Delete (Elimina).

### Note

A seconda di come hai ordinato l'elenco, un certificato che stai cercando potrebbe non essere immediatamente visibile. È possibile fare clic sul triangolo nero a destra per modificare l'ordine. È inoltre possibile navigare tra più pagine di certificati utilizzando i numeri di pagina in alto a destra.

Per eliminare un certificato utilizzando il AWS CLI

Usa il comando [delete-certificate](#) per eliminare un certificato, come illustrato nel comando seguente:

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

## Installazione dei certificati ACM

Non è possibile utilizzare ACM per installare un certificato pubblico direttamente sul sito Web o sull'applicazione AWS basata. Devi utilizzare uno dei servizi seguenti integrati con ACM. Per ulteriori informazioni, consulta [Servizi integrati con AWS Certificate Manager](#).

I certificati ACM firmati da una CA CA privata AWS e destinati alla tua PKI privata possono essere [esportati](#) e installati manualmente su qualsiasi sistema a cui disponi di accesso amministrativo. Questi certificati non sono attendibili su Internet pubblico.

# Rinnovo gestito per i certificati ACM

ACM fornisce il rinnovo gestito dei certificati SSL/TLS emessi da Amazon. Ciò significa che ACM rinnoverà automaticamente i certificati (se si utilizza la convalida DNS) oppure invierà avvisi e-mail quando si avvicina la scadenza. Questi servizi sono forniti sia per i certificati ACM pubblici che privati.

Un certificato è idoneo per il rinnovo automatico, fatte salve le seguenti considerazioni:

- IDONEO se associato a un altro AWS servizio, come Elastic Load Balancing o. CloudFront
- È idoneo se esportato dopo il rilascio o l'ultimo rinnovo.
- ELIGIBILE se si tratta di un certificato privato emesso chiamando l'[RequestCertificateAPI](#) ACM e quindi esportato o associato a un altro servizio. AWS
- È IDONEO se si tratta di un certificato privato rilasciato attraverso la [console di gestione](#) e quindi esportato o associato a un altro servizio AWS .
- NON IDONEO se si tratta di un certificato privato emesso chiamando l' CA privata AWS [IssueCertificateAPI](#).
- Non è idoneo se è [importato](#).
- NON È IDONEO se è già scaduto.

Inoltre, i seguenti requisiti [Punycode](#) relativi a [Nomi di dominio internazionalizzati](#) devono essere soddisfatti:

1. I nomi di dominio che iniziano con il modello "<character><character>--" devono corrispondere a "xn--".
2. Anche i nomi di dominio che iniziano con "xn--" devono essere nomi di dominio internazionalizzati validi.

## Esempi di punycode

Nome dominio	Soddisfa #1	Soddisfa #2	Consiglio	Nota
esempio.com	N/A	n/a	✓	Non inizia con "<character><character>--"

Nome dominio	Soddisfa #1	Soddisfa #2	Conse o	Nota
a--esempi o.com	N/A	n/a	✓	Non inizia con "<character><character>--"
abc—esemp io.com	N/A	n/a	✓	Non inizia con "<character><character>--"
xn—xyz.com	Sì	Sì	✓	Nome di dominio internazionalizzato valido (si risolve su 简.com)
xn--esemp io.com	Sì	No	✗	Nome di dominio internazionalizzato non valido
ab--esemp io.com	No	No	✗	Deve iniziare con "xn--"

Quando ACM rinnova un certificato, il certificato Amazon Resource Name (ARN) rimane invariato. Anche i certificati ACM sono [risorse regionali](#). Se disponi di certificati per lo stesso nome di dominio in più AWS regioni, ognuno di questi certificati deve essere rinnovato indipendentemente.

### Argomenti

- [Scopri come come richiedere un certificato pubblicamente attendibile da ACM.](#)
- [Rinnovo dei certificati in una PKI privata](#)
- [Verifica dello stato di rinnovo di un certificato](#)

## Scopri come come richiedere un certificato pubblicamente attendibile da ACM.

Quando si rilascia un certificato gestito e pubblicamente attendibile, è AWS Certificate Manager necessario dimostrare di essere il proprietario del dominio. Ciò avviene tramite la [Convalida DNS](#) o la [convalida tramite e-mail](#). Quando viene visualizzato un certificato che deve essere rinnovato, ACM utilizza lo stesso metodo scelto in precedenza per riconvalidare la proprietà. I seguenti argomenti descrivono come funziona il processo di rinnovo in ogni caso.

## Argomenti

- [Rinnovo per domini convalidati dal DNS](#)
- [Rinnovo per domini convalidati tramite e-mail](#)

## Rinnovo per domini convalidati dal DNS

Il rinnovo gestito è completamente automatizzato per i certificati ACM emessi in origine utilizzando la [convalida DNS](#).

A 60 giorni prima della scadenza, ACM verifica i seguenti criteri di rinnovo:

- Il certificato è attualmente utilizzato da un AWS servizio.
- Tutti i record DNS CNAME DNS richiesti forniti da ACM (uno per ogni nome alternativo soggetto univoco) sono presenti e accessibili tramite DNS pubblico.

Se questi criteri sono soddisfatti, ACM considera i nomi di dominio convalidati e rinnova il certificato.

ACM invia AWS Health eventi e EventBridge eventi Amazon quando non è in grado di convalidare automaticamente un dominio durante il rinnovo (ad esempio, a causa della presenza del record CAA). Questi eventi vengono inviati 45 giorni, 30 giorni, 15 giorni, sette giorni, tre giorni e un giorno prima della scadenza. Per ulteriori informazioni, consulta [EventBridge Supporto Amazon per ACM](#).

## Rinnovo per domini convalidati tramite e-mail

I certificati ACM sono validi per 13 mesi (395 giorni). Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACM inizia a inviare avvisi di rinnovo 45 giorni prima della scadenza, utilizzando gli indirizzi della casetta postale WHOIS del dominio e a cinque indirizzi amministratore comuni. Le notifiche contengono un link su cui il proprietario del dominio può cliccare per il rinnovo. Una volta convalidati tutti i domini elencati, ACM rilascia un certificato rinnovato con lo stesso ARN.

Per ulteriori informazioni sui messaggi di convalida e-mail, consultare [Convalida e-mail](#).

Per informazioni su come rispondere a livello di programmazione all'e-mail di convalida, consultare [Automatizzare la convalida via e-mail](#).



## Richiedere un messaggio e-mail di convalida del dominio

Dopo aver configurato gli indirizzi e-mail di contatto per il dominio (vedi [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#)), puoi utilizzare la console di AWS Certificate Manager o l'API ACM per richiedere ad ACM di inviarti un'e-mail di convalida del dominio per il rinnovo del certificato. Devi seguire questa procedura nei seguenti casi:

- Hai utilizzato la convalida dell'e-mail quando hai richiesto inizialmente il certificato ACM.
- Lo stato di rinnovo del certificato è pending validation (in attesa di convalida). Per informazioni su come stabilire lo stato di rinnovo di un certificato, consulta [Verifica dello stato di rinnovo di un certificato](#).
- Non hai ricevuto o non sei in grado di trovare l'e-mail originale di convalida del dominio che ACM ha inviato per il rinnovo del certificato.

Per richiedere che ACM invii di nuovo l'e-mail di convalida del dominio (console)

1. [Apri la AWS Certificate Manager console all'indirizzo https://console.aws.amazon.com/acm/home](https://console.aws.amazon.com/acm/home).
2. Scegli Certificate ID (ID del certificato) del certificato che richiede la convalida.
3. Scegli Resend validation email (Rinvio dell'e-mail di convalida).

Per richiedere che ACM invii di nuovo l'e-mail di convalida del dominio (API ACM)

Utilizza l'[ResendValidationEmail](#) operazione nell'API ACM. In questo modo, passare l'ARN del certificato, il dominio che richiede la convalida manuale e il dominio in cui si desidera ricevere le e-mail di convalida. L'esempio seguente mostra come eseguire questa operazione con l' AWS CLI. Questo esempio contiene le interruzioni di riga che facilitano la lettura.

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

## Rinnovo dei certificati in una PKI privata

I certificati ACM firmati da una CA privata di CA privata AWS sono ideali per il rinnovo gestito. A differenza dei certificati ACM di fiducia pubblica, un certificato per una PKI privata non richiede alcuna

convalida. L'attendibilità viene stabilita quando un amministratore installa il certificato CA radice appropriato negli archivi client attendibili.

#### Note

Solo i certificati ottenuti utilizzando la console ACM o l'[RequestCertificate](#)azione dell'API ACM sono idonei per il rinnovo gestito. I certificati emessi direttamente dall' CA privata AWS utilizzo dell'[IssueCertificate](#)azione dell' CA privata AWS API non sono gestiti da ACM.

Quando per un certificato gestito mancano 60 giorni alla scadenza, ACM tenta automaticamente di rinnovarlo. Sono inclusi i certificati esportati e installati manualmente (ad esempio, in un data center locale). I clienti possono anche forzare il rinnovo in qualsiasi momento utilizzando l'[RenewCertificate](#)azione dell'API ACM. Per un'implementazione Java di esempio del rinnovo forzato, vedi [Rinnovo di un certificato](#).

Dopo il rinnovo, la distribuzione di un certificato in servizio si verifica in uno dei modi seguenti:

- Se il certificato è associato a un [servizio integrato](#) ACM, il nuovo certificato sostituisce quello precedente senza ulteriori azioni da parte del cliente.
- Se il certificato non è associato a un [servizio integrato](#) ACM, è necessaria un'azione del cliente per esportare e installare il certificato rinnovato. Puoi eseguire queste azioni manualmente o con l'assistenza [AWS Health](#) di [Amazon EventBridge](#) e [AWS Lambda](#) come segue. Per ulteriori informazioni, consulta [Automatizzazione dell'esportazione dei certificati rinnovati](#)

## Automatizzazione dell'esportazione dei certificati rinnovati

La procedura seguente fornisce una soluzione di esempio per automatizzare l'esportazione dei certificati PKI privati quando ACM li rinnova. Questo esempio esporta solo un certificato e la sua chiave privata da ACM; dopo l'esportazione, il certificato deve ancora essere installato sul rispettivo dispositivo di destinazione.

Per automatizzare l'esportazione dei certificati utilizzando la console

1. Seguendo le procedure riportate nella AWS Lambda Developer Guide, crea e configura una funzione Lambda che richiama l'API di esportazione ACM.
  - a. [Creazione di una funzione Lambda](#).

- b. [Crea un ruolo di esecuzione Lambda](#) per la tua funzione e aggiungici la seguente policy di attendibilità. La policy concede l'autorizzazione al codice della funzione per recuperare il certificato e la chiave privata rinnovati richiamando l'[ExportCertificate](#)azione dell'API ACM.

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

2.

[Crea una regola in Amazon](#) per EventBridge ascoltare gli eventi sanitari ACM e richiama la funzione Lambda quando ne rileva uno. ACM scrive su un AWS Health evento ogni volta che tenta di rinnovare un certificato. Per ulteriori informazioni su questi valori, consulta [Controlla lo stato utilizzando Personal Health Dashboard \(PHD\)](#).

Configura la regola aggiungendo il seguente modello di eventi.

```
{
  "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. Completa il processo di rinnovo installando manualmente il certificato nel sistema di destinazione.

## Test del rinnovo gestito dei certificati PKI privati

Puoi utilizzare l'API ACM o testare manualmente la configurazione del AWS CLI flusso di lavoro di rinnovo gestito ACM. In questo modo, è possibile confermare che i certificati saranno rinnovati automaticamente da ACM prima della scadenza.

### Note

Puoi testare solo il rinnovo dei certificati emessi ed esportati da CA privata AWS

Quando si utilizzano le azioni API o i comandi CLI descritti di seguito, ACM tenta di rinnovare il certificato. Se il rinnovo ha esito positivo, ACM aggiorna i metadati del certificato visualizzati nella console di gestione o nell'output dell'API. Se il certificato è associato a un [servizio integrato](#) ACM, il nuovo certificato viene distribuito e viene generato un evento di rinnovo in Amazon CloudWatch Events. Se il rinnovo non riesce, ACM restituisce un errore e suggerisce un'azione correttiva. (È possibile visualizzare queste informazioni utilizzando il comando [describe-certificate](#).) Se il certificato non viene distribuito tramite un servizio integrato, è comunque necessario esportarlo e installarlo manualmente nella risorsa.

### Important

Per rinnovare i CA privata AWS certificati con ACM, devi prima concedere al servizio ACM le autorizzazioni principali per farlo. Per ulteriori informazioni consulta [Come assegnare le autorizzazioni ad ACM per il rinnovo dei certificati](#).

Per testare manualmente il rinnovo dei certificati (AWS CLI)

1. Utilizza il comando [renew-certificate](#) per rinnovare un certificato privato esportato.

```
aws acm renew-certificate \
```

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

2. Quindi utilizza il comando [describe-certificate](#) per confermare l'avvenuto aggiornamento dei dettagli di rinnovo del certificato.

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

Per testare manualmente il rinnovo dei certificati (API ACM)

- Invia una [RenewCertificate](#) richiesta, specificando l'ARN del certificato privato da rinnovare. Quindi utilizza l'[DescribeCertificate](#) operazione per confermare che i dettagli di rinnovo del certificato sono stati aggiornati.

## Verifica dello stato di rinnovo di un certificato

Quando si tenta di rinnovare un certificato, ACM fornisce un campo di informazioni sullo Stato del rinnovo nei dettagli del certificato. Puoi utilizzare la AWS Certificate Manager console, l'API ACM o il AWS CLI AWS Health Dashboard per verificare lo stato di rinnovo di un certificato ACM. Se utilizzi la console o l'API ACM AWS CLI, lo stato di rinnovo può avere uno dei quattro possibili valori di stato elencati di seguito. Valori simili vengono visualizzati se si utilizza AWS Health Dashboard.

### Rinnovo automatico in attesa

ACM sta cercando di convalidare automaticamente i nomi del dominio nel certificato. Per ulteriori informazioni, consulta [Rinnovo per domini convalidati dal DNS](#). Non è richiesta alcuna operazione aggiuntiva.

### Convalida in attesa

ACM non è riuscito a convalidare automaticamente uno o più nomi del dominio nel certificato. Devi agire per convalidare questi nomi del dominio o il certificato non sarà rinnovato. Se hai utilizzato la convalida dell'e-mail per il certificato, cerca un'e-mail da ACM e quindi segui il link nell'e-mail per eseguire la convalida. Se hai utilizzato la convalida DNS, verifica che il record DNS esista e che il tuo certificato rimanga in uso.

### Riuscito

Tutti i nomi del dominio nel certificato sono convalidati e ACM ha rinnovato il certificato. Non è richiesta alcuna operazione aggiuntiva.

## Non riuscito

Uno o più nomi del dominio non sono stati convalidati prima della scadenza del certificato e ACM non ha rinnovato il certificato. Puoi [richiedere un nuovo certificato](#).

Un certificato è idoneo al rinnovo se è associato a un altro AWS servizio, come Elastic Load Balancing o CloudFront se è stato esportato dopo l'emissione o l'ultimo rinnovo.

### Note

È possibile che le modifiche di stato del rinnovo impieghino diverse ore per diventare disponibili. Se si verifica un problema, la richiesta di rinnovo scade dopo 72 ore e il processo di emissione o rinnovo deve essere ripetuto dall'inizio. Per la risoluzione dei problemi, consultare [Risoluzione dei problemi relativi alle richieste di certificato](#).

## Argomenti

- [Controllo dello stato \(console\)](#)
- [Controllo dello stato \(API\)](#)
- [Controllo dello stato \(CLI\)](#)
- [Controlla lo stato utilizzando Personal Health Dashboard \(PHD\)](#)

## Controllo dello stato (console)

La procedura seguente illustra come utilizzare la console ACM per controllare il rinnovo dello stato di un certificato ACM.

1. [Apri la AWS Certificate Manager console all'indirizzo https://console.aws.amazon.com/acm/home](https://console.aws.amazon.com/acm/home).
2. Espandere un certificato per visualizzare i dettagli.
3. Trova lo Stato di rinnovo nella sezione Dettagli. Se non viene visualizzato lo stato, ACM non ha iniziato il processo di rinnovo gestito per il certificato.

## Controllo dello stato (API)

Per un esempio in Java che mostra come utilizzare l'[DescribeCertificate](#) azione per controllare lo stato, consulta [Descrizione di un certificato](#).

## Controllo dello stato (CLI)

L'esempio seguente mostra come controllare lo stato del rinnovo del tuo certificato ACM con [AWS Command Line Interface \(AWS CLI\)](#).

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

Nella risposta, annotare il valore nel campo `RenewalStatus`. Se non viene visualizzato il campo `RenewalStatus`, ACM non ha iniziato il processo di rinnovo gestito per il certificato.

## Controlla lo stato utilizzando Personal Health Dashboard (PHD)

ACM tenta di rinnovare automaticamente il certificato ACM sessanta giorni prima della scadenza. Se ACM non è in grado di rinnovare automaticamente il certificato, invia avvisi relativi agli eventi di rinnovo del certificato AWS Health Dashboard a intervalli di 45 giorni, 30 giorni, 15 giorni, 7 giorni, 3 giorni e 1 giorno dalla scadenza per informarti della necessità di agire. Fa AWS Health Dashboard parte del servizio. AWS Health Questo servizio non richiede l'installazione e può essere visualizzato da qualsiasi utente autenticato nell'account. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Health](#).

### Note

ACM scrive avvisi di eventi di rinnovo successivi a un singolo evento nella linea temporale del PHD. Ogni avviso sovrascrive quello precedente fino a quando il rinnovo non ha esito positivo.

Per utilizzare AWS Health Dashboard:

1. Accedere all' AWS Health Dashboard indirizzo <https://phd.aws.amazon.com/phd/home#/>.
2. Scegliere Event log (Log evento).
3. Per Filter by tags or attributes (Filtra per tag o attributi), scegliere Service (Servizio).

4. Scegliere Certificate Manager.
5. Scegli Applica.
6. Per Event category (Categoria eventi), scegliere Scheduled Change (Modifica pianificata).
7. Scegli Applica.



# Automatizzare la convalida via e-mail

I certificati ACM convalidati tramite posta elettronica in genere richiedono l'intervento manuale da parte del proprietario del dominio. Le organizzazioni che si occupano di un gran numero di certificati convalidati tramite e-mail possono preferire creare un parser in grado di automatizzare le risposte richieste. Per aiutare i clienti a utilizzare la convalida della posta elettronica, le informazioni in questa sezione descrivono i modelli utilizzati per i messaggi e-mail di convalida del dominio e il flusso di lavoro coinvolto nel completamento del processo di convalida.

## Modelli di e-mail di convalida

I messaggi e-mail di convalida hanno uno dei due formati seguenti a seconda che venga richiesto un nuovo certificato o che venga rinnovato un certificato esistente. Il contenuto delle stringhe evidenziate deve essere sostituito con valori specifici del dominio da convalidare.

### Convalida di un nuovo certificato

Testo del modello di e-mail:

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

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

Sincerely,  
Amazon Web Services

## Convalida di un certificato per il rinnovo

Testo del modello di e-mail:

Greetings from Amazon Web Services,

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

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

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

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

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

Sincerely,  
Amazon Web Services

--

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

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

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

Dopo aver ricevuto un nuovo messaggio di convalida da AWS, ti consigliamo di utilizzarlo come modello più aggiornato e autorevole per il tuo parser. I clienti con parser di messaggi progettati prima di novembre 2020 devono verificare le seguenti modifiche che potrebbero essere state apportate al modello:

- La riga dell'oggetto dell' e-mail è ora "Certificate request for *domain name*" anziché ""Certificate approval for *domain name*".
- L'AWS account ID è ora presentato senza linee e trattini.
- L'Certificate Identifier presenta ora l'intero ARN del certificato anziché un modulo abbreviato, ad esempio *arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369* anziché *3b4d78e1-0882-4f51-954a-298ee44ff369*.
- L'URL di approvazione del certificato contiene ora *acm-certificates.amazon.com* anziché *certificates.amazon.com*.
- Il modulo di approvazione aperto facendo clic sull'URL di approvazione del certificato contiene ora il pulsante di approvazione. Il nome del pulsante di approvazione div è ora *approve-button* anziché *approval\_button*.
- I messaggi di convalida sia per i certificati appena richiesti che per i certificati di rinnovo hanno lo stesso formato di posta elettronica.

## Flusso di lavoro di convalida

Questa sezione contiene informazioni relative al flusso di lavoro di rinnovo dei certificati convalidati tramite e-mail.

- Quando la console ACM elabora una richiesta di certificato multidominio, invia messaggi e-mail di convalida al primo dominio individuato che include un registro MX. Il proprietario del dominio deve

convalidare un messaggio e-mail per ogni dominio prima che ACM possa emettere il certificato. Per ulteriori informazioni, consulta [Utilizzo delle e-mail per convalidare la proprietà del dominio](#).

- La convalida via e-mail per le richieste di certificati multidominio che usano l'API ACM o CLI comporta l'invio di un messaggio di posta elettronica per impostazione predefinita al dominio apex e a ciascun sottodominio. Il proprietario del dominio deve convalidare un messaggio di posta elettronica per ciascuno di questi domini prima che ACM possa emettere il certificato.

#### Note

Prima del novembre 2020, i clienti dovevano convalidare solo il dominio apex e ACM emetterebbe un certificato che coprisse anche eventuali sottodomini. I clienti con parser di messaggi progettati prima di tale ora devono verificare la modifica del flusso di lavoro di convalida via e-mail.

- Con l'API ACM o l'interfaccia CLI, è possibile forzare tutti i messaggi e-mail di convalida per una richiesta di certificato multidominio da inviare al dominio apex. Nell'API, usa il parametro `DomainValidationOptions` dell'azione [RequestCertificate](#) per specificare un valore per `ValidationDomain`, che è un membro del tipo [DomainValidationOption](#). In CLI, `--domain-validation-options` usa il parametro del comando [request-certificate](#) per specificare un valore per `ValidationDomain`.

# Importazione di certificati in AWS Certificate Manager

Oltre a richiedere i certificati SSL/TLS forniti da AWS Certificate Manager (ACM), puoi importare certificati ottenuti al di fuori di AWS. L'utente potrebbe eseguire questa operazione perché ha già un certificato di un'autorità di certificazione (CA) terza parte o perché ha requisiti specifici dell'applicazione che non sono soddisfatti dai certificati rilasciati da ACM.

È possibile utilizzare un certificato importato con qualsiasi [servizio AWS integrato con ACM](#). I certificati importati funzionano esattamente come quelli forniti da ACM, con una sola eccezione importante: ACM non offre il [rinnovo gestito](#) per i certificati importati.

Per rinnovare un certificato importato, è possibile ottenere un nuovo certificato dall'emittente del certificato e poi [reimportarlo](#) manualmente in ACM. Questa operazione conserva l'associazione del certificato e il relativo Amazon Resource Name (ARN). In alternativa, è possibile importare un certificato completamente nuovo. Possono essere importati più certificati con lo stesso nome di dominio, ma devono essere importati uno alla volta.

## Important

L'utente è responsabile del monitoraggio della data di scadenza dei certificati importati e del rinnovo prima della loro scadenza. Puoi semplificare questa attività utilizzando Amazon CloudWatch Events per inviare avvisi quando i certificati importati si avvicinano alla scadenza. Per ulteriori informazioni, consulta [Usare Amazon EventBridge](#).

Tutti i certificati in ACM sono risorse regionali, inclusi i certificati importati. Per utilizzare lo stesso certificato con sistemi di bilanciamento del carico Elastic Load Balancing in AWS regioni diverse, devi importare il certificato in ogni regione in cui desideri utilizzarlo. Per utilizzare un certificato con Amazon CloudFront, devi importarlo nella regione Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni, consulta [Regioni supportate](#).

Per ulteriori informazioni su come importare i certificati in ACM, consulta i seguenti argomenti. Se si verificano problemi durante l'importazione di un certificato, vedere [Problemi di importazione della certificazione](#).

## Argomenti

- [Prerequisiti per l'importazione di certificazione](#)

- [Formato del certificato e della chiave per l'importazione](#)
- [Importazione di un certificato](#)
- [Reimportazione di un certificato](#)

## Prerequisiti per l'importazione di certificazione

Per importare un certificato SSL/TLS autofirmato su ACM, è necessario fornire sia il certificato che la sua chiave privata. Per importare un certificato firmato da un'autorità di certificazione (CA) diversa da AWS, devi includere anche la chiave pubblica e privata del certificato. Il certificato deve soddisfare tutti i criteri descritti in questo argomento.

Per tutti i certificati importati, devi specificare un algoritmo di crittografia e una dimensione della chiave. ACM supporta i seguenti algoritmi (nome API tra parentesi):

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

Si noti anche i seguenti requisiti aggiuntivi:

- I [servizi integrati](#) ACM permettono solo agli algoritmi e alle dimensioni della chiave di accesso supportati di essere associati alle loro risorse. Ad esempio, supporta CloudFront solo chiavi RSA a 1024 bit, RSA a 2048 bit, RSA a 3072 bit ed Elliptic Prime Curve a 256 bit, mentre Application Load Balancer supporta tutti gli algoritmi disponibili da ACM. Per ulteriori informazioni, consulta la documentazione relativa al servizio che usi.
- Un certificato deve essere la terza versione del certificato SSL/TLS X.509. Deve contenere una chiave di accesso pubblica, il nome di dominio completo (FQDN) per il sito Web e le informazioni sull'emittente.
- Un certificato può essere autofirmato tramite una chiave privata che si possiede o firmato tramite la chiave privata di una CA emittente. È necessario fornire la chiave privata, che non deve superare i 5 KB (5.120 byte) e deve essere non crittografata.

- Se il certificato è firmato da una CA e si sceglie di fornire la catena di certificati, la catena deve essere codificata con PEM.
- Un certificato deve essere valido al momento dell'importazione. Non è possibile importare un certificato prima dell'inizio del suo periodo di validità o dopo la sua scadenza. Il campo del certificato `NotBefore` contiene la data di inizio validità e il campo `NotAfter` contiene la data di fine.
- Tutti i materiali del certificato richiesti (certificato, la chiave privata e la catena di certificati) devono essere codificati con PEM. Il caricamento di materiali con codifica DER genera un errore. Per maggiori informazioni ed esempi, consulta [Formato del certificato e della chiave per l'importazione](#).
- Quando si rinnova (reimporta) un certificato, non è possibile aggiungere un'estensione `KeyUsage` o `ExtendedKeyUsage` se l'estensione non era presente nel certificato precedentemente importato.
- AWS CloudFormation non supporta l'importazione di certificati in ACM.

## Formato del certificato e della chiave per l'importazione

ACM richiede che tu importi separatamente il certificato, la catena di certificati e la chiave privata e di decodificare ciascun componente in formato PEM. PEM sta per Privacy Enhanced Mail. Il formato PEM è spesso utilizzato per rappresentare i certificati, le richieste di certificati, le catene di certificati e le chiavi. L'estensione tipica per un file in formato PEM è `.pem`, ma non è necessario che sia così.

### Note

AWS non fornisce utilità per la manipolazione di file PEM o altri formati di certificati. Gli esempi seguenti si basano su un editor di testo generico per operazioni semplici. Se è necessario eseguire attività più complesse (come la conversione di formati di file o l'estrazione di chiavi), strumenti gratuiti e open source come [OpenSSL](#) sono facilmente disponibili.

Gli esempi seguenti illustrano il formato dei file da importare. Se i componenti vengono a te in un singolo file, usa un editor di testo (con attenzione) per separarli in tre file. Se modifichi uno qualsiasi dei caratteri in un file PEM non correttamente o se aggiungi uno o più spazi al termine di qualsiasi riga, il certificato, la catena di certificati o la chiave privata non saranno validi.

## Example 1. Certificato con codifica PEM

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

## Example 2. Catena di certificati con codifica PEM

Una catena di certificati contiene uno o più certificati. Puoi utilizzare un editor di testo, il comando copy in Windows, oppure il comando Linux `cat` per concatenare i tuoi file del certificato in una catena. I certificati devono essere concatenati in modo che ognuno certifichi direttamente quello precedente. Se si importa un certificato privato, copiare il certificato root per ultimo. L'esempio seguente contiene tre certificati, ma la catena di certificati può contenerne di più o di meno.

### Important

Non copiare il certificato nella catena di certificati.

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

## Example 3. Chiavi private con codifica PEM

I certificati X.509 versione 3 usano gli algoritmi della chiave pubblica. Quando crei un certificato X.509 o una richiesta di certificato, devi specificare le dimensioni di bit dell'algoritmo e della chiave che devono essere utilizzate per creare la coppia chiave pubblica-chiave privata. La chiave pubblica viene posizionata nel certificato o nella richiesta. Devi mantenere la chiave privata associata segreta. Specifica la chiave privata quando importi il certificato. La chiave deve essere non crittografata. Di seguito è illustrato un esempio di chiave privata RSA.

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



```
-----END RSA PRIVATE KEY-----
```

L'esempio seguente mostra una chiave privata basata su curva ellittica con codifica PEM. A seconda di come viene creata la chiave, il blocco dei parametri potrebbe non essere incluso. Se il blocco dei parametri è incluso, ACM lo rimuove prima di utilizzare la chiave durante il processo di importazione.

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

## Importazione di un certificato

È possibile importare un certificato ottenuto esternamente (ovvero uno fornito da un fornitore di servizi fiduciari di terze parti) in ACM utilizzando l' AWS Management Console API AWS CLI ACM. Negli argomenti seguenti viene illustrato come utilizzare e il. AWS Management Console AWS CLILe procedure per ottenere un certificato da un ente nonAWS emittente non rientrano nell'ambito di questa guida.

### Important

L'algoritmo di firma selezionato deve soddisfare i [Prerequisiti per l'importazione di certificazione](#).

### Argomenti

- [Importazione \(console\)](#)
- [Importa \(AWS CLI\)](#)

## Importazione (console)

L'esempio seguente mostra come importare un certificato utilizzando AWS Management Console.

1. Apri la console ACM all'indirizzo <https://console.aws.amazon.com/acm/home>. Se questa è la prima volta che utilizzi ACM, cerca l'intestazione AWS Certificate Manager e scegli il pulsante Avvia sotto di essa.

2. Seleziona **Import a certificate** (Importa un certificato).
3. Esegui questa operazione:
  - a. Per **Certificate body** (Corpo del certificato), incolla il certificato con codifica PEM da importare. Dovrebbe iniziare con `-----BEGIN CERTIFICATE-----` e terminare con `-----END CERTIFICATE-----`.
  - b. Per **Certificate private key** (Chiave privata certificato), incolla la chiave privata non crittografata con codifica PEM del certificato. Dovrebbe iniziare con `-----BEGIN PRIVATE KEY-----` e terminare con `-----END PRIVATE KEY-----`.
  - c. (Opzionale) Per **Certificate chain** (Catena certificato), incollare la catena di certificati con codifica PEM.
4. Seleziona **Review and import** (Riconsulta e importa).
5. Sulla pagina **Revisione e importazione**, controlla i metadati visualizzati relativi al certificato per assicurarsi che sia ciò che si desidera. Questi campi includono:
  - **Domini**— Un elenco di nomi di dominio completi (FQDN) autenticati dal certificato
  - **Scade tra**— Il numero di giorni prima della scadenza del certificato
  - **Informazioni chiave pubblica**— L'algoritmo crittografico utilizzato per generare la coppia di chiavi
  - **Algoritmo di firma**— L'algoritmo crittografico usato per creare la firma del certificato
  - **Può essere utilizzato con**— Un elenco di [servizi integrati](#) ACM che supportano il tipo di certificato che si sta importando

Se tutto è corretto, seleziona **Importa**.

## Importa (AWS CLI)

L'esempio seguente mostra come importare un certificato utilizzando [AWS Command Line Interface \(AWS CLI\)](#). L'esempio presuppone quanto segue:

- Il certificato con codifica PEM è archiviato in un file denominato `Certificate.pem`.
- La catena di certificati con codifica PEM è archiviata in un file denominato `CertificateChain.pem`.
- La chiave privata non crittografata con codifica PEM è archiviata in un file denominato `PrivateKey.pem`.

Per utilizzare l'esempio seguente, sostituisci i nomi dei file con i tuoi e digita il comando su una riga continua. L'esempio seguente include interruzioni di linea e spazi aggiuntivi per agevolare la lettura.

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

Se il comando `import-certificate` viene eseguito correttamente, restituisce l'[Amazon Resource Name \(ARN\)](#) del certificato importato.

## Reimportazione di un certificato

Se hai importato un certificato e lo hai associato ad altri AWS servizi, puoi reimportarlo prima che scada, preservando le associazioni di AWS servizio del certificato originale. Per ulteriori informazioni sui AWS servizi integrati con ACM, consulta [Servizi integrati con AWS Certificate Manager](#)

Le condizioni seguenti si applicano quando si reimporta un certificato:

- È possibile aggiungere o rimuovere i nomi di dominio.
- Non è possibile rimuovere tutti i nomi di dominio da un certificato.
- Se le estensioni Key usage (Utilizzo chiave) sono presenti nel certificato originariamente importato, è possibile aggiungere nuovi valori di estensione, ma non è possibile rimuovere i valori esistenti.
- Se le estensioni Extended Key Usage (Utilizzo chiave esteso) sono presenti nel certificato originariamente importato, è possibile aggiungere nuovi valori di estensione, ma non è possibile rimuovere i valori esistenti.
- Il tipo e la dimensione della chiave non possono essere modificati.
- Non è possibile applicare i tag delle risorse durante la reimportazione di un certificato.

### Argomenti

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

## Reimportazione (console)

L'esempio seguente mostra come importare nuovamente un certificato utilizzando AWS Management Console.


1. Aprire la console ACM all'indirizzo <https://console.aws.amazon.com/acm/home>.
2. Selezionare o espandere il certificato da reimportare.
3. Aprire il riquadro dei dettagli del certificato e scegliere il pulsante Reimport certificate (Reimporta certificato). Se si è selezionato il certificato spuntando la casella accanto al nome, scegliere Reimport certificate (Reimporta certificato) nel menu Actions (Operazioni).
4. Per Certificate body (Corpo del certificato), incollare il certificato di entità finale con codifica PEM.
5. Per Certificate private key (Chiave privata certificato), incollare la chiave privata non crittografata, con codifica PEM, associata alla chiave pubblica del certificato.
6. (Opzionale) Per Certificate chain (Catena certificato), incollare la catena di certificati con codifica PEM. La catena di certificati include uno o più certificati per tutte le autorità di certificazione emittenti intermedie e il certificato root. Se il certificato da importare è stato assegnato automaticamente, non è necessaria alcuna catena di certificati.
7. Seleziona Review and import (Riconsulta e importa).
8. Verificare che le informazioni sul certificato siano corrette. Se non ci sono errori, scegliere Reimport (Reimporta).

## Reimportazione (AWS CLI)

L'esempio seguente mostra come importare nuovamente un certificato utilizzando [AWS Command Line Interface \(AWS CLI\)](#). L'esempio presuppone quanto segue:

- Il certificato con codifica PEM è archiviato in un file denominato `Certificate.pem`.
- La catena di certificati con codifica PEM è archiviata in un file denominato `CertificateChain.pem`.
- (Solo certificati privati) La chiave privata non crittografata con codifica PEM viene archiviata in un file denominato `PrivateKey.pem`.
- Hai l'ARN del certificato che desideri reimportare.

Per utilizzare l'esempio seguente, sostituisci i nomi dei file e l'ARN con i tuoi e digita il comando su una riga continua. L'esempio seguente include interruzioni di linea e spazi aggiuntivi per agevolare la lettura.

 Note

Per reimportare un certificato, è necessario specificare l'ARN del certificato.

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

Se il comando `import-certificate` viene eseguito correttamente, restituisce l'[Amazon Resource Name \(ARN\)](#) del certificato.

# Esportazione di un certificato privato

È possibile esportare un certificato emesso da CA privata AWS per utilizzarlo ovunque nel proprio ambiente PKI privato. Il file esportato contiene il certificato, la catena di certificati e la chiave privata crittografata. Questo file deve essere archiviato in modo sicuro. Per ulteriori informazioni in merito CA privata AWS, consulta la [Guida AWS Private Certificate Authority per l'utente](#).

## Note

Non è possibile esportare un certificato pubblicamente attendibile o la relativa chiave privata, indipendentemente dal fatto che sia emesso da ACM o importato.

## Argomenti

- [Esportazione di un certificato privato \(console\)](#)
- [Esportazione di un certificato privato \(CLI\)](#)

## Esportazione di un certificato privato (console)

1. [Accedi alla console di AWS gestione e apri la console ACM all'indirizzo `https://console.aws.amazon.com/acm/home`.](https://console.aws.amazon.com/acm/home)
2. Scegliere Certificate Manager.
3. Scegli il link del certificato da esportare.
4. Scegli Export (Esporta).
5. Immettere e confermare una passphrase per la chiave privata.

## Note

Quando si crea la passphrase, si può usare qualsiasi carattere ASCII tranne #, \$ o %.

6. Scegliere Generate PEM Encoding (Genera codifica PEM).
7. È possibile copiare il certificato, la catena di certificati e la chiave crittografata nella memoria o scegliere Export to a file (Esporta in un file) per ciascuno di questi.
8. Seleziona Fatto.

## Esportazione di un certificato privato (CLI).

Utilizzare il comando [export-certificate](#) per esportare un certificato privato e una chiave privata. È necessario assegnare una passphrase quando si esegue il comando. Per una maggiore sicurezza, utilizza un editor di file per memorizzare la passphrase in un file e quindi fornire la passphrase fornendo il file. In questo modo si impedisce l'archiviazione della passphrase nella cronologia dei comandi e si impedisce ad altri utenti di visualizzare la passphrase digitata.

### Note

Il file contenente la passphrase non deve terminare con un terminatore di riga. È possibile controllare il file della password in questo modo:

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

L'esempi seguenti reindirizza l'output del comando su jq per applicare la formattazione PEM.

[Linux]

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

[Windows]

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

Questa operazione restituisce un certificato in formato PEM con codifica Base64 contenente anche la catena di certificati e la chiave privata crittografata, come nel seguente esempio abbreviato.

```
-----BEGIN CERTIFICATE-----
MIIDTCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMtkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwW0dL0kxpwkkKWtcEkQuHE1v5Vn6HpbFmXkdPEasoDhthH
```

```

FFWIf4/+V01bDLgju4HgtmV4IJDtqM9rG0Z42eFYmmc3eQ00GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h71HUmannS8j6YxmtPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMtkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQQKDAh0cm9sb2xvbDCCASIwDQYJKoZIhvcNAQEBBQADggEP
...
j2PA0viqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPd1+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCaggAMB0GCWCGSAF1AwQBKqQQDViroIHStQgN0jR6nTUuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTPskNCdCAHqdh0SqBwt65qUTZe3gBT
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrXuHTWjF1
wEuqyd8X/ApkQsYFX/nhep0EIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxf0C1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs90V/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----

```

Per inviare tutto l'output in un file, accodare il redirector > all'esempio precedente, ottenendo quanto segue.

```

$ 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

```



# Tagging di certificati AWS Certificate Manager

Un tag è un'etichetta che puoi assegnare a un certificato ACM. Ciascun tag è formato da una chiave e da un valore. Puoi utilizzare la console di AWS Certificate Manager, l'AWS Command Line Interface (AWS CLI) o l'API ACM per aggiungere, visualizzare o eliminare tag per i certificati ACM. Puoi scegliere i tag da mostrare nella console ACM.

Puoi creare tag personalizzati per le tue esigenze. Ad esempio, puoi taggare più certificati ACM con un tag `Environment = Prod` o `Environment = Beta` per identificare a quale ambiente è destinato ciascun certificato ACM. L'elenco seguente include alcuni esempi aggiuntivi di altri tag personalizzati:

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

Il tagging è supportato anche da altre risorse AWS. Puoi pertanto assegnare lo stesso tag a risorse diverse per indicare se tali risorse sono correlate. Ad esempio, puoi assegnare un tag come `Website = example.com` al certificato ACM, al load balancer e ad altre risorse utilizzate per il sito `Web example.com`.

## Argomenti

- [Limitazioni applicate ai tag](#)
- [Gestione dei tag](#)

## Limitazioni applicate ai tag

Ai tag del certificato ACM; si applicano le seguenti limitazioni di base:

- Il numero massimo di tag per il certificato ACM è 50.
- La lunghezza massima di una chiave di un tag è 127 caratteri.
- La lunghezza massima di un valore di tag è 255 caratteri.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;

- Il prefisso `aws:` è riservato all'uso da parte di AWS: non è possibile aggiungere, modificare o eliminare tag la cui chiave inizia con `aws:`. I tag che iniziano con `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.
- Se si prevede di utilizzare lo schema di tagging in più servizi e risorse, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. Consultare la documentazione per quel servizio.
- I tag del certificato ACM non sono disponibili per l'uso nell'[editor dei tag e in Resource Groups](#) di AWS Management Console.

Per informazioni generali sulle convenzioni per AWS l'assegnazione di tag, consultare [Risorse per i AWS tag](#).

## Gestione dei tag

Puoi aggiungere, modificare ed eliminare i tag utilizzando la console di gestione AWS, AWS Command Line Interface oppure l'API AWS Certificate Manager.

### Gestione dei tag (Console)

Puoi utilizzare la AWS Management Console per aggiungere, eliminare o modificare i tag. Puoi anche visualizzare i tag nelle colonne.

#### Aggiunta di tag

Segui questa procedura per aggiungere tag utilizzando la console ACM.

#### Aggiunta di tag a un certificato (Console)

1. Accedi alla AWS Management Console e apri la console di AWS Certificate Manager all'indirizzo <https://console.aws.amazon.com/acm/home>.
2. Scegli la freccia accanto al certificato che desideri taggare.
3. Nel riquadro dei dettagli, scorrere verso il basso fino a Tags (Tag).
4. Scegliere Edit (Modifica) e Add Tag (Aggiungi tag).
5. Digitare una chiave e un valore per il tag.
6. Seleziona Salva.

## Eliminazione di tag

Segui questa procedura per eliminare tag utilizzando la console ACM.

Per eliminare un tag (console)

1. Accedi alla AWS Management Console e apri la console di AWS Certificate Manager all'indirizzo <https://console.aws.amazon.com/acm/home>.
2. Scegliere la freccia posizionata accanto al certificato con un tag che si desidera eliminare.
3. Nel riquadro dei dettagli, scorrere verso il basso fino a Tags (Tag).
4. Scegliere Edit (Modifica).
5. Scegliere X accanto al tag da eliminare.
6. Seleziona Salva.

## Modifica dei tag

Segui questa procedura per modificare i tag utilizzando la console ACM.

Per modificare un tag (console)

1. Accedi alla AWS Management Console e apri la console di AWS Certificate Manager all'indirizzo <https://console.aws.amazon.com/acm/home>.
2. Scegliere la freccia posizionata accanto al certificato che si desidera modificare.
3. Nel riquadro dei dettagli, scorrere verso il basso fino a Tags (Tag).
4. Scegliere Edit (Modifica).
5. Modificare la chiave o il valore del tag che si desidera modificare.
6. Seleziona Salva.

## Visualizzazione dei tag nelle colonne

Segui questa procedura per visualizzare i tag in colonne utilizzando la console ACM.

Per visualizzare i tag in colonne (console)

1. Accedi alla AWS Management Console e apri la console di AWS Certificate Manager all'indirizzo <https://console.aws.amazon.com/acm/home>.

2. Scegli i tag che desideri visualizzare come colonne scegliendo l'icona a forma di ingranaggio



nell'angolo superiore destro della console.

3. Selezionare la casella di controllo accanto al tag che si desidera visualizzare in una colonna.

## Gestione dei tag (CLI)

Consulta i seguenti argomenti su come aggiungere, elencare ed eliminare i tag utilizzando la AWS CLI.

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

## Gestione dei tag (API ACM)

Consulta i seguenti argomenti su come aggiungere, elencare ed eliminare i tag utilizzando l'API.

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

# Monitoraggio e registrazione AWS Certificate Manager

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Certificate Manager AWS soluzioni esistenti. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica.

I seguenti argomenti descrivono gli strumenti di AWS monitoraggio del cloud disponibili per l'uso con ACM.

## Argomenti

- [Usare Amazon EventBridge](#)
- [Utilizzo con CloudTrail AWS Certificate Manager](#)
- [CloudWatch Metriche supportate](#)

## Usare Amazon EventBridge

Puoi usare [Amazon EventBridge](#) (precedentemente CloudWatch Events) per automatizzare AWS i tuoi servizi e rispondere automaticamente a eventi di sistema come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi dei AWS servizi, incluso ACM, vengono consegnati ad Amazon quasi EventBridge in tempo reale. Puoi utilizzare gli eventi per attivare obiettivi tra cui AWS Lambda funzioni, AWS Batch job, argomenti di Amazon SNS e molti altri. Per ulteriori informazioni, consulta [What Is Amazon EventBridge?](#)

## Argomenti

- [EventBridge Supporto Amazon per ACM](#)
- [Attivazione di azioni con Amazon EventBridge in ACM](#)

## EventBridge Supporto Amazon per ACM

Questo argomento elenca e descrive gli eventi correlati ad ACM supportati da Amazon EventBridge.

## Evento ACM Certificate Approaching Expiration

ACM invia eventi di scadenza giornaliera per tutti i certificati attivi (pubblici, privati e importati) a partire da 45 giorni prima della scadenza. Questa tempistica può essere modificata utilizzando l'[PutAccountConfiguration](#) dell'API ACM.

ACM avvia automaticamente il rinnovo dei certificati idonei emessi, ma i certificati importati devono essere riemessi e reimportati prima della scadenza per evitare interruzioni. Per ulteriori informazioni, vedere [Reimportazione di un certificato](#). È possibile utilizzare gli eventi di scadenza per configurare l'automazione allo scopo di reimportare i certificati in ACM. Per un esempio di utilizzo dell'automazione, consulta [AWS Lambda Attivazione di azioni con Amazon EventBridge in ACM](#).

Gli eventi ACM Certificate Approaching Expiration hanno la seguente struttura.

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

## Evento ACM Certificate Expired

### Note

Gli eventi di scadenza dei certificati non sono disponibili per i [certificati importati](#).

I clienti possono ascoltare questo evento per essere avvisati quando un certificato pubblico o privato emesso da ACM nel proprio account scade.

Gli eventi ACM Certificate Expired hanno la seguente struttura.

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

## Evento ACM Certificate Available

I clienti possono ascoltare questo evento per essere avvisati quando un certificato pubblico o privato gestito è pronto per l'utilizzo. L'evento viene pubblicato su emissione, rinnovo e importazione. Nel caso di un certificato privato, una volta disponibile, è comunque necessario l'intervento del cliente per distribuirlo sugli host.

Gli eventi ACM Certificate Available hanno la seguente struttura.

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

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

## Evento ACM Certificate Renewal Action Required

### Note

Gli eventi Certificate Renewal Action Required non sono disponibili per i [certificati importati](#).

I clienti possono ascoltare questo evento per essere avvisati quando è necessaria un'operazione da parte del cliente prima che un certificato possa essere rinnovato. Ad esempio, se un cliente aggiunge record CAA che impediscono ad ACM di rinnovare un certificato, ACM pubblica questo evento in caso di esito negativo del rinnovo automatico 45 giorni prima della scadenza. Se non viene eseguita alcuna operazione da parte del cliente, ACM effettua ulteriori tentativi di rinnovo a 30 giorni, 15 giorni, 3 giorni e 1 giorno o fino a quando il cliente non esegue un'operazione, il certificato scade o il certificato non è più idoneo al rinnovo. Viene pubblicato un evento per ciascuno di questi tentativi di rinnovo.

Gli eventi ACM Certificate Renewal Action Required hanno la seguente struttura.

```
{
  "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 eventi sanitari

AWS gli eventi sanitari vengono generati per i certificati ACM idonei al rinnovo. Per informazioni sull'idoneità al rinnovo, consulta [Rinnovo gestito per i certificati ACM](#).

Gli eventi sull'integrità vengono generati in due scenari:

- Al rinnovo positivo di un certificato pubblico o privato.
- Quando un cliente deve intervenire affinché si verifichi un rinnovo. Ciò potrebbe significare fare clic su un collegamento in un messaggio e-mail (per i certificati convalidati tramite e-mail) o risolvere un errore. Uno dei seguenti codici evento è incluso in ogni evento. I codici sono esposti come variabili che è possibile utilizzare per il filtro.
  - AWS\_ACM\_RENEWAL\_STATE\_CHANGE (il certificato è stato rinnovato, è scaduto o è in scadenza)
  - CAA\_CHECK\_FAILURE (Controllo CAA non riuscito)
  - AWS\_ACM\_RENEWAL\_FAILURE (per certificati firmati da una CA privata)

Gli eventi sull'integrità hanno la seguente struttura. In questo esempio, è stato generato un evento di AWS\_ACM\_RENEWAL\_STATE\_CHANGE.

```
{
```

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

## Attivazione di azioni con Amazon EventBridge in ACM

Puoi creare EventBridge regole Amazon basate su questi eventi e utilizzare la EventBridge console Amazon per configurare le azioni da eseguire quando vengono rilevati gli eventi. Questa sezione fornisce procedure di esempio per configurare le EventBridge regole di Amazon e le azioni risultanti.

### Argomenti

- [Risposta a un evento con Amazon SNS](#)
- [Rispondere a un evento con una funzione Lambda](#)

## Risposta a un evento con Amazon SNS

In questa sezione viene illustrato come configurare Amazon SNS per inviare una notifica di testo ogni volta che ACM genera un evento sull'integrità.

Completa la procedura seguente per configurare una risposta.

Per creare una EventBridge regola Amazon e attivare un'azione

1. Crea una EventBridge regola Amazon. Per ulteriori informazioni, consulta [Creazione di EventBridge regole Amazon che reagiscono agli eventi](#).

- a. Nella EventBridge console Amazon all'[indirizzo https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/), vai alla pagina Eventi > Regole e scegli Crea regola.
- b. Dalla pagina Crea una regola seleziona Pattern di eventi.
- c. Per Nome servizio, scegli Integrità dal menu.
- d. Per Tipo di evento, scegli Eventi specifici sull'integrità.
- e. Seleziona Servizi specifici e scegli ACM dal menu.
- f. Seleziona Categorie specifiche del tipo di evento e scegli accountNotification.
- g. Scegli Qualsiasi codice del tipo di evento.
- h. Seleziona Qualsiasi risorsa.
- i. Nell'editor Anteprima dei pattern degli eventi, incolla il pattern JSON emesso dall'evento. In questo esempio viene utilizzato il pattern della sezione [AWS eventi sanitari](#).

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

## 2. Configurare un'operazione.

Nella sezione Target, puoi scegliere tra molti servizi che possono attivare immediatamente il tuo evento, ad esempio Amazon Simple Notification Service (SNS), oppure puoi scegliere la

funzione Lambda per passare l'evento al codice eseguibile personalizzato. Per un esempio di implementazione AWS Lambda , consulta [Rispondere a un evento con una funzione Lambda](#).

## Rispondere a un evento con una funzione Lambda

Questa procedura illustra come utilizzare per AWS Lambda ascoltare su Amazon EventBridge, creare notifiche con Amazon Simple Notification Service (SNS) e pubblicare i risultati AWS Security Hub, fornendo visibilità agli amministratori e ai team di sicurezza.

Per impostare una funzione Lambda e un ruolo IAM

1. Per prima cosa configura un ruolo AWS Identity and Access Management (IAM) e definisci le autorizzazioni necessarie alla funzione Lambda. Questa procedura consigliata per la protezione offre flessibilità nella designazione dell'utente che dispone dell'autorizzazione a chiamare la funzione e nella limitazione delle autorizzazioni concesse a tale persona. Non è consigliabile eseguire la maggior parte delle AWS operazioni direttamente con un account utente e soprattutto non con un account amministratore.

Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

2. Usa l'editor delle policy JSON per creare la policy definita nel modello seguente. Fornisci i dettagli della tua regione e AWS del tuo account. Per ulteriori informazioni, consulta [Creazione di policy nella scheda JSON](#).

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

```

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

```

3. Creare un ruolo IAM e collegare la policy. Per informazioni sulla creazione di un ruolo IAM e sull'associazione di una policy, consulta [Creating a role for an AWS service \(console\)](#).
4. Apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.

5. Creazione della funzione Lambda Per ulteriori informazioni sull'utilizzo di Lambda, consulta [Creare una funzione Lambda con la console](#). Completa questa procedura:
  - a. Nella pagina Crea funzione, scegli l'opzione Crea da zero per creare la funzione.
  - b. Specificate un nome come handle-expiring-certificates "" nel campo Nome funzione.
  - c. Scegli Python 3.8 dall'elenco Tempo di esecuzione.
  - d. Espandi Modifica ruolo di esecuzione predefinito e scegli Usa un ruolo esistente.
  - e. Scegli il ruolo creato in precedenza dall'elenco Ruolo esistente.
  - f. Scegli Crea funzione.
  - g. In Codice della funzione, inserisci il seguente codice:

```
# 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. Sotto Variabili ambiente, scegli Modifica e facoltativamente aggiungi le seguenti variabili.

- (Facoltativo) EXPIRY\_DAYS

Specifica il lead time, espressa in giorni, prima dell'invio della notifica di scadenza del certificato. Il valore predefinito della funzione è 45 giorni, ma è possibile specificare valori personalizzati.

- (Facoltativo) SNS\_TOPIC\_ARN

Specifica un ARN per un Amazon SNS. Fornisci l'ARN completo nel formato `arn:aws:sns:<region>:<account-number>:<topic-name>`.

- (Opzionale) SECURITY\_HUB\_REGION

Specificate un valore AWS Security Hub in una regione diversa. Se questo non viene specificato, viene utilizzata la regione della funzione Lambda in esecuzione. Se la funzione viene eseguita in più regioni, potrebbe essere consigliabile che tutti i messaggi dei certificati vengano inviati a Security Hub in un'unica Regione.

- i. In Impostazioni di base, imposta il valore Timeout su 30 secondi.
- j. Nella parte superiore della pagina, scegli Implementa.

Completare le attività descritte nella procedura seguente per iniziare a utilizzare questa soluzione.

Per automatizzare una notifica e-mail di scadenza

In questo esempio, forniamo un'unica e-mail per ogni certificato in scadenza nel momento in cui l'evento viene segnalato tramite Amazon EventBridge. Per impostazione predefinita, ACM genera un evento ogni giorno per un certificato pari o inferiore a 45 giorni dalla scadenza. (Questo periodo può essere personalizzato utilizzando il [PutAccountConfiguration](#) funzionamento dell'API ACM.) Ciascuno di questi eventi attiva la seguente cascata di azioni automatiche:

```
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. Crea la funzione Lambda e configura le autorizzazioni. (Già completato — vedi [Per impostare una funzione Lambda e un ruolo IAM](#)).

2. Crea un argomento SNS standard per la funzione Lambda da utilizzare per inviare notifiche. Per ulteriori informazioni, consulta [Creazione di un argomento Amazon SNS](#).
3. Iscriviti tutte le parti interessate al nuovo argomento SNS. Per ulteriori informazioni, consulta [Iscrizione a un argomento Amazon SNS](#).
4. Crea una EventBridge regola Amazon per attivare la funzione Lambda. Per ulteriori informazioni, consulta [Creazione di EventBridge regole Amazon che reagiscono agli eventi](#).

Nella EventBridge console Amazon all'[indirizzo https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/), vai alla pagina Eventi > Regole e scegli Crea regola. Specifica Nome servizio, Tipo di evento e Funzione Lambda. Nell'editor Anteprima dei pattern degli eventi, incolla il seguente codice:

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

Un evento come quello ricevuto da Lambda viene visualizzato in Mostra eventi campione:

```
{
  "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"
  }
}
```

## Per eliminare

Una volta che non è più necessaria la configurazione di esempio o qualsiasi configurazione, è consigliabile rimuoverne tutte le tracce per evitare problemi di sicurezza e costi futuri imprevisti:

- Policy IAM e ruolo
- Funzione Lambda
- CloudWatch Regola degli eventi
- CloudWatch Log associati a Lambda
- Argomento SNS

## Utilizzo con CloudTrail AWS Certificate Manager

AWS Certificate Manager è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in ACM. CloudTrail è abilitato per impostazione predefinita sul tuo AWS account. CloudTrail acquisisce le chiamate API per ACM come eventi, incluse le chiamate dalla console ACM e le chiamate di codice alle operazioni dell'API ACM. Se configuri un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per ACM. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta ad ACM, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#). Quando si verifica un'attività di evento supportata in ACM, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS .

Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log.

Per ulteriori informazioni in merito CloudTrail, consulta la seguente documentazione:

- [AWS CloudTrail Guida per l'utente](#).
- [Panoramica della creazione di un trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)

- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

## Argomenti

- [Azioni API ACM supportate nella registrazione CloudTrail](#)
- [Registrazione di chiamate API per servizi integrati](#)

## Azioni API ACM supportate nella registrazione CloudTrail

ACM supporta la registrazione delle seguenti azioni come eventi nei file di registro: CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con Utente root dell'account AWS o AWS Identity and Access Management (IAM) credenziali utente.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, vedete l'elemento [CloudTrailuserIdentity](#).

Nelle sezioni seguenti vengono forniti log di esempio per le operazioni API supportate.

- [Aggiunta di tag a un certificato \(AddTagsToCertificate\)](#)
- [Eliminazione di un certificato \(DeleteCertificate\)](#)
- [Descrizione di un certificato \(DescribeCertificate\)](#)
- [Esportazione di un certificato \(ExportCertificate\)](#)
- [Importazione di un certificato \(ImportCertificate\)](#)
- [Elenco dei certificati \(ListCertificates\)](#)
- [Elenco di tag per un certificato \(ListTagsForCertificate\)](#)
- [Rimozione di tag da un certificato \(RemoveTagsFromCertificate\)](#)

- [Richiesta di un certificato \(RequestCertificate\)](#)
- [Rinvio dell'e-mail di convalida \(ResendValidationEmail\)](#)
- [Recupero di un certificato \(GetCertificate\)](#)

## Aggiunta di tag a un certificato ([AddTagsToCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
    }
  ]
}
```

```
}
]
}
```

## Eliminazione di un certificato ([DeleteCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
    }
  ]
}
```

## Descrizione di un certificato ([DescribeCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[DescribeCertificate](#)API.

**Note**

Il CloudTrail registro dell'`DescribeCertificate` operazione non mostra informazioni sul certificato ACM specificato. È possibile visualizzare le informazioni sul certificato utilizzando la console AWS Command Line Interface, l'o l'[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"
    }
  ]
}
```

**Esportazione di un certificato ([ExportCertificate](#))**

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[ExportCertificate API](#).



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

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

```

## Importazione di un certificato ([ImportCertificate](#))

L'esempio seguente mostra la voce di CloudTrail registro che registra una chiamata all'operazione [ImportCertificate](#) API ACM.

```

{
  "eventVersion":"1.04",
  "userIdentity":{

```

```
"type":"IAMUser",
"principalId":"AIDACKCEVSQ6C2EXAMPLE",
"arn":"arn:aws:iam::111122223333:user/Alice",
"accountId":"111122223333",
"accessKeyId":"AKIAIOSFODNN7EXAMPLE",
"userName":"Alice"
},
"eventTime":"2016-10-04T16:01:30Z",
"eventSource":"acm.amazonaws.com",
"eventName":"ImportCertificate",
"awsRegion":"ap-southeast-2",
"sourceIPAddress":"54.240.193.129",
"userAgent":"Coral/Netty",
"requestParameters":{
  "privateKey":{
    "hb":[
      "byte",
      "byte",
      "byte",
      "...",
    ],
    "offset":0,
    "isReadOnly":false,
    "bigEndian":true,
    "nativeByteOrder":false,
    "mark":-1,
    "position":0,
    "limit":1674,
    "capacity":1674,
    "address":0
  },
  "certificateChain":{
    "hb":[
      "byte",
      "byte",
      "byte",
      "...",
    ],
    "offset":0,
    "isReadOnly":false,
    "bigEndian":true,
    "nativeByteOrder":false,
    "mark":-1,
    "position":0,
```

```

        "limit":2105,
        "capacity":2105,
        "address":0
    },
    "certificate":{
        "hb":[
            "byte",
            "byte",
            "byte",
            "...",
        ],
        "offset":0,
        "isReadOnly":false,
        "bigEndian":true,
        "nativeByteOrder":false,
        "mark":-1,
        "position":0,
        "limit":2503,
        "capacity":2503,
        "address":0
    }
},
"responseElements":{
    "certificateArn":"arn:aws:acm:ap-
southeast-2:111122223333:certificate/01234567-89ab-cdef-0123-456789abcdef"
},
"requestID":"01234567-89ab-cdef-0123-456789abcdef",
"eventID":"01234567-89ab-cdef-0123-456789abcdef",
"eventType":"AwsApiCall",
"recipientAccountId":"111122223333"
}

```

## Elenco dei certificati ([ListCertificates](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[ListCertificates](#)API.

### Note

Il CloudTrail registro dell'[ListCertificates](#)operazione non mostra i certificati ACM. È possibile visualizzare l'elenco dei certificati utilizzando la console AWS Command Line Interface, l'o l'[ListCertificates](#)API.

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

## Elenco di tag per un certificato ([ListTagsForCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[ListTagsForCertificate](#) API.

**Note**

Il CloudTrail registro dell'`ListTagsForCertificate` operazione non mostra i tag. È possibile visualizzare l'elenco dei tag utilizzando la console AWS Command Line Interface, l' [l'`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"
    }
  ]
}
```

## Rimozione di tag da un certificato ([RemoveTagsFromCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
    }
  ]
}
```

## Richiesta di un certificato ([RequestCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
}
```



```
}
```

## Rinvio dell'e-mail di convalida ([ResendValidationEmail](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
    }
  ]
}
```

## Recupero di un certificato ([GetCertificate](#))

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'[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"
    }
  ]
}

```

## Registrazione di chiamate API per servizi integrati

È possibile CloudTrail utilizzarlo per controllare le chiamate API effettuate da servizi integrati con ACM. Per ulteriori informazioni sull'utilizzo CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#). I seguenti esempi mostrano i tipi di registri che possono essere generati in funzione delle risorse AWS a cui hai assegnato il certificato ACM.

### Argomenti

- [Creazione di un load balancer](#)

### Creazione di un load balancer

Puoi utilizzarlo CloudTrail per controllare le chiamate API effettuate dai servizi integrati con ACM. Per ulteriori informazioni sull'utilizzo CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#). Gli esempi seguenti mostrano i tipi di log che possono essere generati a seconda AWS delle risorse su cui si effettua il provisioning del certificato ACM.

### Argomenti

- [Creazione di un load balancer](#)
- [Registrazione di un'istanza Amazon EC2; con un load balancer](#)
- [Crittografia di una chiave di accesso privata](#)
- [Decrittografia di una chiave di accesso privata](#)

### Creazione di un load balancer

L'esempio seguente mostra una chiamata alla funzione `CreateLoadBalancer` effettuata da Alice, un utente IAM. Il nome del load balancer è `TestLinuxDefault` e l'ascoltatore viene creato tramite un certificato ACM.

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```

    "userName": "Alice"
  },
  "eventTime": "2016-01-01T21:10:36Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0/24",
  "userAgent": "aws-cli/1.9.15",
  "requestParameters": {
    "availabilityZones": [
      "us-east-1b"
    ],
    "loadBalancerName": "LinuxTest",
    "listeners": [
      {
        "sSLCertificateId": "arn:aws:acm:us-east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
        "protocol": "HTTPS",
        "loadBalancerPort": 443,
        "instanceProtocol": "HTTP",
        "instancePort": 80
      }
    ]
  },
  "responseElements": {
    "dNSName": "LinuxTest-1234567890.us-east-1.elb.amazonaws.com"
  },
  "requestID": "19669c3b-b0cc-11e5-85b2-57397210a2e5",
  "eventID": "5d6c00c9-a9b8-46ef-9f3b-4589f5be63f7",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

## Registrazione di un'istanza Amazon EC2; con un load balancer

Quando viene effettuato il provisioning di un sito Web o di un'applicazione su un'istanza Amazon Elastic Compute Cloud (Amazon EC2), il load balancer deve essere messo a conoscenza di tale istanza. Questo può essere fatto attraverso la console Elastic Load Balancing o AWS Command Line Interface. L'esempio seguente mostra una chiamata a `RegisterInstancesWithLoadBalancer` per un load balancer denominato `LinuxTest` sull'AWS account `123456789012`.

```

{
  "eventVersion": "1.03",

```

```
"userIdentity":{
  "type":"IAMUser",
  "principalId":"AIDACKCEVSQ6C2EXAMPLE",
  "arn":"arn:aws:iam::123456789012:user/Alice",
  "accountId":"123456789012",
  "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
  "userName":"Alice",
  "sessionContext":{
    "attributes":{
      "mfaAuthenticated":"false",
      "creationDate":"2016-01-01T19:35:52Z"
    }
  },
  "invokedBy":"signin.amazonaws.com"
},
"eventTime":"2016-01-01T21:11:45Z",
"eventSource":"elasticloadbalancing.amazonaws.com",
"eventName":"RegisterInstancesWithLoadBalancer",
"awsRegion":"us-east-1",
"sourceIPAddress":"192.0.2.0/24",
"userAgent":"signin.amazonaws.com",
"requestParameters":{
  "loadBalancerName":"LinuxTest",
  "instances":[
    {
      "instanceId":"i-c67f4e78"
    }
  ]
},
"responseElements":{
  "instances":[
    {
      "instanceId":"i-c67f4e78"
    }
  ]
},
"requestID":"438b07dc-b0cc-11e5-8afb-cda7ba020551",
"eventID":"9f284ca6-cbe5-42a1-8251-4f0e6b5739d6",
"eventType":"AwsApiCall",
"recipientAccountId":"123456789012"
}
```

## Crittografia di una chiave di accesso privata

L'esempio seguente mostra una chiamata `Encrypt` che esegue la crittografia della chiave di accesso privata associata a un certificato ACM. La crittografia viene eseguita all'interno di 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"
    }
  ]
}
```

```
]
}
```

## Decrittografia di una chiave di accesso privata

L'esempio seguente mostra una chiamata Decrypt che esegue la decrittografia della chiave di accesso privata associata a un certificato ACM. La decrittografia viene eseguita all'interno e la chiave decrittografata non esce AWS mai. AWS

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:1aba0dc8b3a728d6998c234a99178eff",
    "arn": "arn:aws:sts::111122223333:assumed-role/DecryptACMCertificate/1aba0dc8b3a728d6998c234a99178eff",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2016-01-01T21:13:28Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "APKAEIBAERJR2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/DecryptACMCertificate",
        "accountId": "111122223333",
        "userName": "DecryptACMCertificate"
      }
    }
  },
  "eventTime": "2016-01-01T21:13:28Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "encryptionContext": {
      "aws:elasticloadbalancing:arn": "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/LinuxTest",

```

```

    "aws:acm:arn": "arn:aws:acm:us-
east-1:123456789012:certificate/87654321-4321-4321-4321-210987654321"
  }
},
"responseElements": null,
"requestID": "809a70ff-b0cc-11e5-8f42-c7fdf1cb6e6a",
"eventID": "7f89f7a7-baff-4802-8a88-851488607fb9",
"readOnly": true,
"resources": [
  {
    "ARN": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012",
    "accountId": "123456789012"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012"
}

```

## CloudWatch Metriche supportate

Amazon CloudWatch è un servizio di monitoraggio delle AWS risorse. Puoi utilizzarlo CloudWatch per raccogliere e tenere traccia delle metriche, impostare allarmi e reagire automaticamente ai cambiamenti nelle tue AWS risorse. ACM pubblica le metriche una volta al giorno per ogni certificato in un account fino alla scadenza.

Il namespace `AWS/CertificateManager` include i parametri descritti di seguito.

Parametro	Descrizione	Unità	Dimensioni
DaysToExpiry	Numero di giorni alla scadenza di un certificato. ACM interrompe la pubblicazione di questo parametro dopo la scadenza di un certificato.	Numero intero	CertificateArn <ul style="list-style-type: none"> <li>Valore: ARN del certificato.</li> </ul>



Per ulteriori informazioni sulle CloudWatch metriche, consulta i seguenti argomenti:

- [Utilizzo di Amazon CloudWatch Metrics](#)
- [Creazione di CloudWatch allarmi Amazon](#)

## Utilizzo dell'API (esempi Java)

È possibile utilizzare l'API AWS Certificate Manager per interagire programmaticamente con il servizio inviando richieste HTTP. Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API di AWS Certificate Manager](#).

Oltre alle API Web (o API HTTP), è possibile utilizzare gli SDK AWS e gli strumenti a riga di comando per interagire con ACM e con altri servizi. Per ulteriori informazioni, consulta [Strumenti per Amazon Web Services](#).

I seguenti argomenti illustrano come usare uno degli SDK AWS, [AWS SDK for Java](#), per eseguire alcune delle operazioni disponibili nell'API AWS Certificate Manager.

### Argomenti

- [Aggiunta di tag a un certificato](#)
- [Eliminazione di un certificato](#)
- [Descrizione di un certificato](#)
- [Esportazione di un certificato](#)
- [Recupero di un certificato e di una catena di certificati](#)
- [Importazione di un certificato](#)
- [Elenco dei certificati](#)
- [Rinnovo di un certificato](#)
- [Elenco dei tag del certificato](#)
- [Rimozione di tag da un certificato](#)
- [Richiesta di un certificato](#)
- [Rinvio dell'e-mail di convalida](#)

## Aggiunta di tag a un certificato

Il seguente esempio illustra come utilizzare la funzione [AddTagsToCertificate](#).

```
package com.amazonaws.samples;

import java.io.IOException;
import java.nio.ByteBuffer;
```

```
import java.nio.charset.StandardCharsets;
import java.nio.file.Files;
import java.nio.file.Paths;

import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 * Certificate Manager
 * service.
 *
 * Input parameters:
 *   Accesskey - AWS access key
 *   SecretKey - AWS secret key
 *   CertificateArn - Use to reimport a certificate (not included in this example).
 *   region - AWS region
 *   Certificate - PEM file that contains the certificate to import. Ex: /data/certs/
servercert.pem
 *   CertificateChain - The certificate chain, not including the end-entity
certificate.
 *   PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 *   CertificcateArn - The ARN of the imported certificate.
 *
 */
public class AWSCertificateManagerSample {

    public static void main(String[] args) throws IOException {
        String accessKey = "";
        String secretKey = "";
        String certificateArn = null;
        Regions region = Regions.DEFAULT_REGION;
        String serverCertFilePath = "";
        String privateKeyFilePath = "";
        String caCertFilePath = "";

        ImportCertificateRequest req = new ImportCertificateRequest()
            .withCertificate(getCertContent(serverCertFilePath))
    }
```

```
        .withPrivateKey(getCertContent(privateKeyFilePath))

    .withCertificateChain(getCertContent(caCertFilePath)).withCertificateArn(certificateArn);

    AWSCertificateManager client =
    AWSCertificateManagerClientBuilder.standard().withRegion(region)
        .withCredentials(new AWSStaticCredentialsProvider(new
    BasicAWSCredentials(accessKey, secretKey)))
        .build();
    ImportCertificateResult result = client.importCertificate(req);

    System.out.println(result.getCertificateArn());

    List<Tag> expectedTags =
    ImmutableList.of(Tag.builder().withKey("key").withValue("value").build());

    AddTagsToCertificateRequest addTagsToCertificateRequest =
    AddTagsToCertificateRequest.builder()
        .withCertificateArn(result.getCertificateArn())
        .withTags(tags)
        .build();

    client.addTagsToCertificate(addTagsToCertificateRequest);
}

private static ByteBuffer getCertContent(String filePath) throws IOException {
    String fileContent = new String(Files.readAllBytes(Paths.get(filePath)));
    return StandardCharsets.UTF_8.encode(fileContent);
}
}
```

## Eliminazione di un certificato

Il seguente esempio illustra come utilizzare la funzione [DeleteCertificate](#). In caso di esito positivo, la funzione restituisce un set {} vuoto.

```
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);

}
}
```

## Descrizione di un certificato

Il seguente esempio illustra come utilizzare la funzione [DescribeCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.DescribeCertificateRequest;
import com.amazonaws.services.certificatemanager.model.DescribeCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
```

```
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the DescribeCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameter:
 * CertificateArn - The ARN of the certificate to be described.
 *
 * Output parameter:
 * Certificate information
 *
 */

public class AWSCertificateManagerExample {

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

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load the credentials from file.",
ex);
        }

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

        // Create a request object and set the ARN of the certificate to be described.
        DescribeCertificateRequest req = new DescribeCertificateRequest();
```

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

DescribeCertificateResult result = null;
try{
    result = client.describeCertificate(req);
}
catch (InvalidArnException ex)
{
    throw ex;
}
catch (ResourceNotFoundException ex)
{
    throw ex;
}

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

}
}
```

Se viene eseguito correttamente, l'esempio precedente visualizza informazioni simili alle seguenti.

```
{
  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,  
  }  
}
```

## Esportazione di un certificato

Il seguente esempio illustra come utilizzare la funzione [ExportCertificate](#). La funzione esporta un certificato privato emesso da un'autorità di certificazione privata (CA) nel formato PKCS #8. (Non è possibile esportare certificati pubblici che siano emessi o importati da ACM). Inoltre, esporta la catena di certificati e la chiave privata. In questo esempio, la passphrase per la chiave viene memorizzata in un file locale.

```
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();
}
}
```

## Recupero di un certificato e di una catena di certificati

Il seguente esempio illustra come utilizzare la funzione [GetCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.GetCertificateRequest;
import com.amazonaws.services.certificatemanager.model.GetCertificateResult;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.RequestInProgressException;
import com.amazonaws.AmazonClientException;

/**
 * This sample demonstrates how to use the GetCertificate function in the AWS
 * Certificate
 * Manager service.
 */
```

```
* Input parameter:  
* CertificateArn - The ARN of the certificate to retrieve.  
*  
* Output parameters:  
* Certificate - A base64-encoded certificate in PEM format.  
* CertificateChain - The base64-encoded certificate chain in PEM format.  
*  
*/
```

```
public class AWSCertificateManagerExample {  
  
    public static void main(String[] args) throws Exception{  
  
        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in  
Windows  
        // or the ~/.aws/credentials file in Linux.  
        AWSCredentials credentials = null;  
        try {  
            credentials = new ProfileCredentialsProvider().getCredentials();  
        }  
        catch (Exception ex) {  
            throw new AmazonClientException("Cannot load the credentials from the  
credential profiles file.", ex);  
        }  
  
        // Create a client.  
        AWSCertificateManager client = AWSCertificateManagerClientBuilder.standard()  
            .withRegion(Regions.US_EAST_1)  
            .withCredentials(new AWSStaticCredentialsProvider(credentials))  
            .build();  
  
        // Create a request object and set the ARN of the certificate to be described.  
        GetCertificateRequest req = new GetCertificateRequest();  
  
        req.setCertificateArn("arn:aws:acm:region:account:certificate/  
12345678-1234-1234-1234-123456789012");  
  
        // Retrieve the certificate and certificate chain.  
        // If you recently requested the certificate, loop until it has been created.  
        GetCertificateResult result = null;  
        long totalTimeout = 1200001;  
        long timeSlept = 01;  
        long sleepInterval = 100001;  
        while (result == null && timeSlept < totalTimeout) {
```

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

    timeSlept += sleepInterval;
}

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

L'esempio precedente crea un output simile al seguente.

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

## Importazione di un certificato

Il seguente esempio illustra come utilizzare la funzione [ImportCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.model.ImportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ImportCertificateResult;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

/**
 * This sample demonstrates how to use the ImportCertificate function in the AWS
 * Certificate Manager
 * service.
 *
 * Input parameters:
 * Certificate - PEM file that contains the certificate to import.
 * CertificateArn - Use to reimport a certificate (not included in this example).
 * CertificateChain - The certificate chain, not including the end-entity
 * certificate.
 * PrivateKey - The private key that matches the public key in the certificate.
 *
 * Output parameter:
 * CertificateArn - The ARN of the imported certificate.
 */
public class AWSCertificateManagerSample {

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

## Elenco dei certificati

L'esempio seguente mostra come utilizzare la funzione [ListCertificates](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListCertificatesRequest;
import com.amazonaws.services.certificatemanager.model.ListCertificatesResult;

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

import com.amazonaws.AmazonClientException;

import java.util.Arrays;
import java.util.List;

/**
 * This sample demonstrates how to use the ListCertificates function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameters:
 * CertificateStatuses - An array of strings that contains the statuses to use for
 * filtering.
 * MaxItems - The maximum number of certificates to return in the response.
 * NextToken - Use when paginating results.
 *
 * Output parameters:
 * CertificateSummaryList - A list of certificates.
 * NextToken - Use to show additional results when paginating a truncated list.
 *
 */
```

```
*/

public class AWSCertificateManagerExample {

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

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load the credentials from file.",
ex);
        }

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

        // Create a request object and set the parameters.
        ListCertificatesRequest req = new ListCertificatesRequest();
        List<String> Statuses = Arrays.asList("ISSUED", "EXPIRED", "PENDING_VALIDATION",
"FAILED");
        req.setCertificateStatuses(Statuses);
        req.setMaxItems(10);

        // Retrieve the list of certificates.
        ListCertificatesResult result = null;
        try {
            result = client.listCertificates(req);
        }
        catch (Exception ex)
        {
            throw ex;
        }

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

```
}
```

L'esempio precedente crea un output simile al seguente.

```
{
  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
  }]
}
```

## Rinnovo di un certificato

Il seguente esempio illustra come utilizzare la funzione [RenewCertificate](#). La funzione rinnova un certificato privato emesso da un'autorità di certificazione privata (CA) ed esportata con la funzione [ExportCertificate](#). Al momento, con questa funzione possono essere rinnovati solo i certificati privati esportati. Per rinnovare i certificati di CA privata AWS con ACM, è necessario prima concedere al principale del servizio ACM le autorizzazioni per poter procedere. Per ulteriori informazioni consulta [Come assegnare le autorizzazioni ad ACM](#) per il rinnovo dei certificati.

```
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);
}
}
```

## Elenco dei tag del certificato

L'esempio seguente mostra come utilizzare la funzione [ListTagsForCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ListTagsForCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.regions.Regions;
```

```
/**
 * This sample demonstrates how to use the ListTagsForCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameter:
 * CertificateArn - The ARN of the certificate whose tags you want to list.
 */

public class AWSCertificateManagerExample {

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

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        // Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

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

        // Create a request object and specify the ARN of the certificate.
        ListTagsForCertificateRequest req = new ListTagsForCertificateRequest();

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

        // Create a result object.
        ListTagsForCertificateResult result = null;
        try {
            result = client.listTagsForCertificate(req);
        }
    }
}
```

```
    }
    catch(InvalidArnException ex) {
        throw ex;
    }
    catch(ResourceNotFoundException ex) {
        throw ex;
    }

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

}
}
```

L'esempio precedente crea un output simile al seguente.

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

## Rimozione di tag da un certificato

L'esempio seguente mostra come utilizzare la funzione [RemoveTagsFromCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
import
    com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RemoveTagsFromCertificateResult;
import com.amazonaws.services.certificatemanager.model.Tag;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.InvalidTagException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.AmazonClientException;

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

import java.util.ArrayList;
```



```
/**
 * This sample demonstrates how to use the RemoveTagsFromCertificate function in the
 * AWS Certificate
 * Manager service.
 *
 * Input parameters:
 * CertificateArn - The ARN of the certificate from which you want to remove one or
 * more tags.
 * Tags - A collection of key-value pairs that specify which tags to remove.
 */

public class AWSCertificateManagerExample {

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

        // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
        Windows
        // or the ~/.aws/credentials file in Linux.
        AWSCredentials credentials = null;
        try {
            credentials = new ProfileCredentialsProvider().getCredentials();
        }
        catch (Exception ex) {
            throw new AmazonClientException("Cannot load your credentials from file.",
ex);
        }

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

        // Specify the tags to remove.
        Tag tag1 = new Tag();
        tag1.setKey("Short_Name");
        tag1.setValue("My_Cert");

        Tag tag2 = new Tag()
            .withKey("Purpose")
            .withValue("Test");
    }
}
```

```
// Add the tags to a collection.
ArrayList<Tag> tags = new ArrayList<Tag>();
tags.add(tag1);
tags.add(tag2);

// Create a request object.
RemoveTagsFromCertificateRequest req = new RemoveTagsFromCertificateRequest();

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

// Create a result object.
RemoveTagsFromCertificateResult result = null;
try {
    result = client.removeTagsFromCertificate(req);
}
catch(InvalidArnException ex)
{
    throw ex;
}
catch(InvalidTagException ex)
{
    throw ex;
}
catch(ResourceNotFoundException ex)
{
    throw ex;
}

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

## Richiesta di un certificato

Il seguente esempio illustra come utilizzare la funzione [RequestCertificate](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;
```

```
import com.amazonaws.services.certificatemanager.model.RequestCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RequestCertificateResult;

import
    com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;
import com.amazonaws.services.certificatemanager.model.LimitExceededException;
import com.amazonaws.AmazonClientException;

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

import java.util.ArrayList;

/**
 * This sample demonstrates how to use the RequestCertificate function in the AWS
 * Certificate
 * Manager service.
 *
 * Input parameters:
 * DomainName - FQDN of your site.
 * DomainValidationOptions - Domain name for email validation.
 * IdempotencyToken - Distinguishes between calls to RequestCertificate.
 * SubjectAlternativeNames - Additional FQDNs for the subject alternative names
 * extension.
 *
 * Output parameter:
 * Certificate ARN - The Amazon Resource Name (ARN) of the certificate you requested.
 */

public class AWSCertificateManagerExample {

    public static void main(String[] args) {

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

```
        throw new AmazonClientException("Cannot load your credentials from file.",
ex);
    }

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

    // Specify a SAN.
    ArrayList<String> san = new ArrayList<String>();
    san.add("www.example.com");

    // Create a request object and set the input parameters.
    RequestCertificateRequest req = new RequestCertificateRequest();
    req.setDomainName("example.com");
    req.setIdempotencyToken("1Aq25pTy");
    req.setSubjectAlternativeNames(san);

    // Create a result object and display the certificate ARN.
    RequestCertificateResult result = null;
    try {
        result = client.requestCertificate(req);
    }
    catch(InvalidDomainValidationOptionsException ex)
    {
        throw ex;
    }
    catch(LimitExceededException ex)
    {
        throw ex;
    }

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

L'esempio precedente crea un output simile al seguente.

```
{CertificateArn:  
  arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

## Rinvio dell'e-mail di convalida

L'esempio seguente mostra come utilizzare la funzione [ResendValidationEmail](#).

```
package com.amazonaws.samples;  
  
import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;  
import com.amazonaws.services.certificatemanager.AWSCertificateManager;  
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailRequest;  
import com.amazonaws.services.certificatemanager.model.ResendValidationEmailResult;  
  
import  
  com.amazonaws.services.certificatemanager.model.InvalidDomainValidationOptionsException;  
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;  
import com.amazonaws.services.certificatemanager.model.InvalidStateException;  
import com.amazonaws.services.certificatemanager.model.InvalidArnException;  
import com.amazonaws.AmazonClientException;  
  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.auth.AWSStaticCredentialsProvider;  
import com.amazonaws.auth.AWSCredentials;  
import com.amazonaws.regions.Regions;  
  
/**  
 * This sample demonstrates how to use the ResendValidationEmail function in the AWS  
 Certificate  
 Manager service.  
 *  
 * Input parameters:  
 * CertificateArn - Amazon Resource Name (ARN) of the certificate request.  
 * Domain - FQDN in the certificate request.  
 * ValidationDomain - The base validation domain that is used to send email.  
 *  
 */  
  
public class AWSCertificateManagerExample {  
  
    public static void main(String[] args) {
```

```
// Retrieve your credentials from the C:\Users\name\.aws\credentials file in
Windows
// or the ~/.aws/credentials file in Linux.
AWSCredentials credentials = null;
try {
    credentials = new ProfileCredentialsProvider().getCredentials();
}
catch (Exception ex) {
    throw new AmazonClientException("Cannot load your credentials from file.",
ex);
}

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

// Create a request object and set the input parameters.
ResendValidationEmailRequest req = new ResendValidationEmailRequest();

req.setCertificateArn("arn:aws:acm:region:account:certificate/
12345678-1234-1234-1234-123456789012");
req.setDomain("gregpe.io");
req.setValidationDomain("gregpe.io");

// Create a result object.
ResendValidationEmailResult result = null;
try {
    result = client.resendValidationEmail(req);
}
catch(ResourceNotFoundException ex)
{
    throw ex;
}
catch (InvalidStateException ex)
{
    throw ex;
}
catch (InvalidArnException ex)
{
    throw ex;
}
catch (InvalidDomainValidationOptionsException ex)
```

```
    {  
        throw ex;  
    }  
  
    // Display the result.  
    System.out.println(result.toString());  
  
    }  
}
```

L'esempio precedente rinvia l'e-mail di convalida e mostra un set vuoto.

# Risoluzione dei problemi

Consulta i seguenti argomenti in caso di problemi relativi all'utilizzo di AWS Certificate Manager.

## Note

Se il problema non è illustrato in questa sezione, si consiglia di visitare [Portale del sapere di AWS](#).

## Argomenti

- [Risoluzione dei problemi relativi alle richieste di certificato](#)
- [Risoluzione dei problemi di convalida dei certificati](#)
- [Risoluzione dei problemi relativi al rinnovo dei certificati gestiti](#)
- [Risoluzione di altri problemi](#)
- [Gestione delle eccezioni](#)

## Risoluzione dei problemi relativi alle richieste di certificato

Consulta i seguenti argomenti in caso di problemi durante la richiesta di un certificato ACM.

## Argomenti

- [Timeout della richiesta di certificato](#)
- [Errore nella richiesta di certificato](#)

## Timeout della richiesta di certificato

Le richieste per i certificati ACM scadono se non vengono convalidate entro 72 ore. Per correggere questa condizione, apri la console, trova il registro per il certificato, fai clic sulla casella di controllo relativa, scegli Operazioni e seleziona Elimina. Quindi scegli Operazioni e Richiedi un certificato per ricominciare. Per ulteriori informazioni, consulta [Convalida DNS](#) o [Convalida e-mail](#). È consigliabile utilizzare la convalida del DNS se possibile.



## Errore nella richiesta di certificato

Se la richiesta di ACM non riesce e viene visualizzato uno dei seguenti messaggi di errore, attieniti alla procedura suggerita per risolvere il problema. Non è possibile inviare nuovamente una richiesta di certificato non riuscita: dopo aver risolto il problema, inviare una nuova richiesta.

### Argomenti

- [Messaggio di errore: Nessun contatto disponibile](#)
- [Messaggio di errore: Verifica aggiuntiva richiesta](#)
- [Messaggio di errore: Dominio pubblico non valido](#)
- [Messaggio di errore: Altro](#)

### Messaggio di errore: Nessun contatto disponibile

Hai scelto la convalida dell'e-mail quando hai richiesto il certificato, ma ACM non ha trovato alcun indirizzo e-mail da utilizzare per la convalida di uno o più nomi di dominio nella richiesta. Per risolvere questo problema, puoi procedere in uno dei seguenti modi:

- Verifica di disporre di un indirizzo e-mail funzionante registrato in WHOIS e che tale indirizzo sia visibile quando esegui una ricerca WHOIS standard per i nomi di dominio nella richiesta di certificato. In genere, è possibile eseguire questa operazione tramite il registrar di dominio.
- Assicurati che il dominio sia configurato per ricevere e-mail. Il server dei nomi di dominio deve avere un registro mail exchanger (registro MX), in modo che i server di posta elettronica ACM sappiano dove inviare [l'e-mail di convalida del dominio](#).

L'esecuzione di una delle attività precedenti è sufficiente per risolvere il problema; non è necessario eseguire entrambe le attività. Dopo aver risolto il problema, richiedi un nuovo certificato.

Per ulteriori informazioni su come essere certi di ricevere le e-mail di convalida del dominio da ACM, consulta [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#) o [Mancata ricezione dell'e-mail di convalida](#). Se segui queste fasi e continui a ricevere il messaggio No Available Contacts (Nessun contatto disponibile), [segnala il problema ad AWS](#) per consentirci di eseguire ulteriori indagini.

### Messaggio di errore: Verifica aggiuntiva richiesta

ACM richiede ulteriori informazioni per elaborare la richiesta di certificato. Ciò avviene come misura di protezione contro le frodi se il tuo dominio si colloca all'interno dei [migliori 1000 siti web di Alexa](#). Per

fornire queste informazioni, usa il [Centro di supporto](#) per contattare AWS Support. Se non disponi di un piano di supporto, pubblica un nuovo thread nel [forum di discussione di ACM](#).

#### Note

Non puoi richiedere un certificato per i nomi di dominio di proprietà di Amazon, ad esempio quelli che finiscono con amazonaws.com, cloudfront.net o elasticbeanstalk.com.

## Messaggio di errore: Dominio pubblico non valido

Uno o più nomi di dominio nella richiesta di certificato non è valido. In genere questa situazione si verifica perché un nome di dominio nella richiesta non è un dominio di primo livello valido. Prova a richiedere di nuovo un certificato, correggendo gli eventuali errori ortografici o refusi presenti nella richiesta non riuscita e accertandoti che tutti i nomi di dominio nella richiesta facciano riferimento a domini di primo livello validi. Ad esempio, non puoi richiedere un certificato ACM per example.invalidpublicdomain perché "invalidpublicdomain" non è un dominio di primo livello valido. Se continui a ricevere questo motivo dell'errore, contatta il [Centro di supporto](#). Se non disponi di un piano di supporto, pubblica un nuovo thread nel [forum di discussione di ACM](#).

## Messaggio di errore: Altro

In genere questo problema si verifica in presenza di un errore tipografico in uno o più nomi di dominio nella richiesta di certificato. Prova a richiedere di nuovo un certificato, correggendo gli eventuali errori ortografici o refusi presenti nella richiesta non riuscita. Se continui a ricevere questo motivo dell'errore, usa il [Centro di supporto](#) per contattare AWS Support. Se non disponi di un piano di supporto, pubblica un nuovo thread nel [forum di discussione di ACM](#).

## Risoluzione dei problemi di convalida dei certificati

Se lo stato della richiesta del certificato ACM è Convalida in attesa, la richiesta è in attesa di un'operazione da parte dell'utente. Se quando è stata effettuata la richiesta è stata scelta la convalida e-mail, l'utente o un rappresentante autorizzato devono rispondere ai messaggi e-mail di convalida. Questi messaggi sono stati inviati agli indirizzi di contatto WHOIS registrati e ad altri indirizzi di posta elettronica comuni per il dominio richiesto. Per ulteriori informazioni, consulta [Convalida e-mail](#). Se è stata scelta la convalida DNS, è necessario scrivere il record CNAME creato da ACM per l'utente nel database DNS. Per ulteriori informazioni, consulta [Convalida DNS](#).

**⚠ Important**

L'utente deve convalidare la proprietà o il controllo di ogni nome di dominio incluso nella richiesta di certificato. Se si sceglie la convalida e-mail, si riceveranno messaggi e-mail di convalida per ogni dominio. In caso contrario, consultare [Mancata ricezione dell'e-mail di convalida](#). Se si sceglie la convalida DNS, è necessario creare un record CNAME per ogni dominio.

**ℹ Note**

I certificati ACM pubblici possono essere installati su istanze Amazon EC2 connesse a [Nitro Enclave](#), ma non su altre istanze di Amazon EC2. Per informazioni sulla configurazione di un server Web autonomo su un'istanza Amazon EC2 non connessa a Nitro Enclave, vedi [Tutorial: Installa un server Web LAMP su Amazon Linux 2](#) o [Tutorial: installa un server Web LAMP con Amazon Linux AMI](#).

Si consiglia di utilizzare la convalida DNS anziché la convalida e-mail.

Consultate i seguenti argomenti in caso di problemi di convalida.

Argomenti

- [Risoluzione dei problemi di convalida DNS](#)
- [Risoluzione dei problemi di convalida e-mail](#)

## Risoluzione dei problemi di convalida DNS

Consultare la seguente guida se si riscontrano problemi nel convalidare un certificato con DNS.

La prima fase nella risoluzione dei problemi DNS consiste nel verificare lo stato corrente del dominio con i seguenti strumenti:

- dig — [Linux](#), [Windows](#)
- nslookup — [Linux](#), [Windows](#)
- whois — [Linux](#), [Windows](#)

## Argomenti

- [Trattini bassi proibiti dal provider DNS](#)
- [Periodo finale predefinito aggiunto dal provider DNS](#)
- [Convalida DNS in caso di errore GoDaddy](#)
- [La console ACM non visualizza il pulsante "Crea record in Route 53"](#)
- [La convalida di Route 53 non riesce su domini privati \(non attendibili\)](#)
- [La convalida ha esito positivo ma l'emissione o il rinnovo falliscono](#)
- [La convalida non riesce per il server DNS su una VPN](#)

## Trattini bassi proibiti dal provider DNS

Se il provider DNS non consente l'utilizzo di trattini bassi iniziali di valori CNAME, è possibile eliminarli dal valore fornito da ACM e convalidare il dominio senza. Ad esempio, il valore CNAME `_x2.acm-validations.aws` può essere modificato in `x2.acm-validations.aws` per la convalida. Tuttavia, il parametro del nome CNAME deve essere iniziare con un trattino basso.

Per convalidare un dominio è possibile utilizzare uno dei valori a destra della tabella qui di seguito.

Nome	Type	Valore
<code>_ _&lt;random value&gt;.ex ample.com.</code>	CNAME	<code>_ _&lt;random value&gt;.acm-validat ions.aws.</code>
<code>_ _&lt;random value&gt;.ex ample.com.</code>	CNAME	<code>&lt;random value&gt;.acm-validat ions.aws.</code>

## Periodo finale predefinito aggiunto dal provider DNS

Alcuni provider DNS aggiungono per impostazione predefinita un periodo finale al valore CNAME fornito. Di conseguenza, l'aggiunta del periodo provoca un errore. Ad esempio, "`<random_value>.acm-validations.aws.`" viene rifiutato mentre "`<random_value>.acm-validations.aws`" è accettato.

## Convalida DNS in caso di errore GoDaddy

La convalida DNS per i domini registrati con GoDaddy e altri registri potrebbe non riuscire a meno che non si modifichino i valori CNAME forniti da ACM. Prendendo `example.com` come nome di dominio, il record CNAME emesso ha la seguente forma:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:  
_cjhwo20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

È possibile creare un record CNAME compatibile con GoDaddy troncando il dominio apex (incluso il punto) alla fine del campo NAME, come segue:

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:  
_cjhwo20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

## La console ACM non visualizza il pulsante "Crea record in Route 53"

Se scegli Amazon Route 53 come provider DNS, AWS Certificate Manager puoi interagire direttamente con Amazon Route 53 per convalidare la proprietà del dominio. In alcune circostanze, il pulsante Crea registri in Route 53 della console potrebbe non essere disponibile. In questo caso, verificare le seguenti possibili cause.

- Non stai utilizzando Route 53 come provider DNS.
- Hai eseguito l'accesso ad ACM e a Route 53 con account diversi.
- Mancano le autorizzazioni IAM per la creazione di registri in una zona ospitata da Route 53.
- L'utente o un'altra persona ha già convalidato il dominio.
- Il dominio non è indirizzabile pubblicamente.

## La convalida di Route 53 non riesce su domini privati (non attendibili)

Durante la convalida DNS, ACM cerca un CNAME in una zona ospitata pubblicamente. Quando non ne trova uno, viene eseguito il timeout dopo 72 ore con uno stato di Validation timed out (Timeout della convalida). Non è possibile utilizzarlo per l'hosting dei record DNS per domini privati, comprese risorse in una [zona ospitata privata](#) di Amazon VPC, domini non attendibili nel proprio PKI privato o certificati autofirmati.

AWS fornisce supporto per domini pubblicamente non attendibili tramite il servizio. [CA privata AWS](#)

## La convalida ha esito positivo ma l'emissione o il rinnovo falliscono

Se l'emissione del certificato fallisce e viene visualizzato il messaggio "Convalida in sospeso" anche se il DNS è corretto, verifica che l'emissione non sia bloccata da un record CAA (Certification Authority Authorization). Per ulteriori informazioni, consulta [\(Opzionale\) Configurazione di un registro CAA](#).

## La convalida non riesce per il server DNS su una VPN

Se individui un server DNS su una VPN e ACM non riesce a convalidare un certificato, verifica se il server è accessibile pubblicamente. Per l'emissione di certificati pubblici con la convalida DNS ACM è necessario che i registri di dominio siano risolvibili tramite Internet pubblico.

## Risoluzione dei problemi di convalida e-mail

Consulta la seguente guida se hai problemi nel convalidare il dominio di un certificato tramite e-mail.

### Argomenti

- [Mancata ricezione dell'e-mail di convalida](#)
- [E-mail inviata al sottodominio](#)
- [Informazioni di contatto nascoste](#)
- [Rinnovo dei certificati](#)
- [Limitazione di WHOIS](#)
- [Timestamp iniziale persistente per la convalida tramite e-mail](#)
- [Risolvere i problemi relativi al dominio di primo livello .IO](#)
- [Se non si riesce a passare alla convalida del DNS](#)

## Mancata ricezione dell'e-mail di convalida

Quando richiedi un certificato ad ACM e scegli la convalida dell'e-mail, un'e-mail di convalida del dominio viene inviata a tre indirizzi di contatto specificati in WHOIS e cinque indirizzi di amministrazione comuni. Per ulteriori informazioni, consulta [Convalida e-mail](#). In caso di problemi di ricezione dell'e-mail di convalida, consulta i suggerimenti riportati di seguito.

### Dove cercare l'e-mail

L'e-mail di convalida viene inviata agli indirizzi di contatto elencati in WHOIS e agli indirizzi di amministrazione comuni per il dominio. L'e-mail non viene inviata al proprietario dell' AWS

account a meno che il proprietario non sia elencato anche come contatto di dominio in WHOIS. Consulta l'elenco degli indirizzi e-mail visualizzati nella console ACM (o restituiti dalla CLI o dall'API) per determinare dove trovare l'e-mail di convalida. Per visualizzare l'elenco, fai clic sull'icona accanto al nome del dominio nella casella Validation not complete (Convalida non completata).

L'e-mail è contrassegnata come spam

Controlla la cartella spam per verificare se contiene l'e-mail di convalida.

GMail ordina automaticamente l'e-mail

Se utilizzi GMail, l'e-mail di convalida potrebbe essere stata ordinata automaticamente nella scheda Updates (Aggiornamenti) o Promotions (Promozioni).

Il registrar di dominio non visualizza le informazioni di contatto o la protezione della privacy è abilitata

In alcuni casi, i contatti tecnici e amministrativi del registrante del dominio in WHOIS potrebbero non essere disponibili al pubblico e AWS pertanto non essere in grado di raggiungere tali contatti. A tua discrezione, puoi scegliere di configurare il registrar per elencare il tuo indirizzo e-mail in WHOIS, anche se non tutti i registrar supportano questa opzione. È possibile che tu debba apportare una modifica direttamente nel registro del dominio. In altri casi, le informazioni di contatto del dominio potrebbero utilizzare un indirizzo di privacy, come quelli forniti tramite WhoisGuard o PrivacyGuard

Per i domini acquistati da Route 53, la protezione della privacy è abilitata di default e l'indirizzo e-mail è associato a un indirizzo e-mail `whoisprivacyservice.org`, `contact.gandi.net` o `identity-protect.org`. Assicurati che l'indirizzo e-mail del registrant sul file con il registrar del dominio sia aggiornato in modo che l'e-mail inviata a questi indirizzi e-mail oscurati possa essere inoltrata a un indirizzo e-mail che controlli.

#### Note

La protezione della privacy per alcuni domini acquistati con Route 53 verrà abilitata anche se decidi di rendere pubbliche le tue informazioni di contatto. Ad esempio, la protezione della privacy per il dominio di primo livello `.ca` non può essere disabilitata in modo programmatico da Route 53. Devi contattare il [Centro di supporto AWS](#) e richiedere che la protezione della privacy sia disabilitata.

Se le informazioni di contatto e-mail per il dominio non sono disponibili tramite WHOIS o se l'e-mail inviata alle informazioni di contatto non raggiunge il proprietario del dominio né un rappresentante autorizzato, ti consigliamo di configurare il dominio o il sottodominio in modo da ricevere l'e-mail inviata a uno o più indirizzi di amministrazione comuni creato antepoendo `admin@`, `administrator@`, `hostmaster@`, `webmaster@` e `postmaster@` al nome del dominio richiesto. Per ulteriori informazioni sulla configurazione dell'e-mail per il dominio, consulta la documentazione per il tuo fornitore di servizi di e-mail e segui le istruzioni riportate in [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#). Se utilizzi Amazon WorkMail, consulta [Working with Users](#) nella Amazon WorkMail Administrator Guide.

Dopo aver reso disponibile almeno uno degli otto indirizzi e-mail a cui AWS invia e-mail di convalida e aver verificato che ricevi e-mail per tale indirizzo, potrai richiedere un certificato tramite ACM. Dopo aver effettuato una richiesta di certificato, assicurati che l'indirizzo e-mail previsto sia visualizzato nell'elenco degli indirizzi e-mail nella AWS Management Console. Mentre il certificato è in stato Pending validation (Convalida in sospeso), puoi espandere l'elenco per visualizzarlo facendo clic sull'icona accanto al nome del dominio nella casella Validation not complete (Convalida non completata). Puoi anche visualizzare l'elenco nella Fase 3: Convalida della procedura guidata Richiedi certificato di ACM. Gli indirizzi e-mail elencati sono quelli a cui è stata inviata l'e-mail.

## Record MX mancanti o configurati in modo non corretto

Un record MX è un record della risorsa nel database Domain Name System (DNS) che specifica uno o più server di posta elettronica che accettano messaggi e-mail per il dominio. Se il record MX è mancante o configurato in modo non corretto, l'e-mail non può essere inviata a uno dei cinque indirizzi di amministrazione del sistema comuni specificati in [Convalida e-mail](#). Correggi il record MX mancante o configurato in modo non corretto e prova a inviare nuovamente l'e-mail o a richiedere di nuovo il certificato.

### Note

Attualmente, ti consigliamo di attendere almeno un'ora prima di tentare di inviare di nuovo l'e-mail o di richiedere il certificato.

### Note

Per evitare di richiedere un record MX, puoi utilizzare l'`ValidationDomain` opzione nell'[RequestCertificate](#) API o il AWS CLI comando [request-certificate](#) per specificare il



nome di dominio a cui ACM invia le e-mail di convalida. Se si utilizza l'API o AWS CLI, AWS non esegue una ricerca MX.

## Contattare il Centro di supporto

Se, dopo aver esaminato i consigli precedenti, ancora non ricevi l'e-mail di convalida dei domini, visita il [Centro AWS Support](#) e immetti una richiesta. Se non disponi di un contratto di assistenza, pubblica un messaggio nel [Forum di discussione di ACM](#).

## E-mail inviata al sottodominio

Se stai usando la console e richiedi un certificato per un sottodominio con un nome come `sub.test.example.com`, ACM verifica se è presente un registro MX per `sub.test.example.com`. In caso contrario, viene controllato il dominio padre `test.example.com` e così via, fino al dominio di base `example.com`. Se viene trovato un record MX, la ricerca viene interrotta e un'e-mail di convalida viene inviata agli indirizzi di amministrazione comuni per il sottodominio. Se ad esempio viene trovato un record MX per `test.example.com`, l'e-mail viene inviata agli indirizzi `admin@test.example.com`, `administrator@test.example.com` e agli altri indirizzi amministrativi specificati in [Convalida e-mail](#). Se non viene trovato alcun record MX in nessuno dei sottodomini, l'e-mail viene inviata al sottodominio per il quale hai richiesto il certificato in origine. Per una spiegazione completa di come configurare la tua e-mail e come utilizzare ACM con DNS e il database WHOIS, consulta [\(Facoltativo\) Configurazione dell'e-mail per il dominio in uso](#).

Invece di utilizzare la console, è possibile utilizzare l'`ValidationDomain` opzione nell'[RequestCertificate](#) API o il AWS CLI comando [request-certificate](#) per specificare il nome di dominio a cui ACM invia le e-mail di convalida. Se si utilizza l'API o AWS CLI, AWS non esegue una ricerca MX.

## Informazioni di contatto nascoste

Un problema comune si verifica quando si cerca di creare un nuovo certificato. Alcuni registrar consentono di nascondere le informazioni di contatto nell'elenco WHOIS. Altri consentono di sostituire l'indirizzo e-mail reale con un indirizzo riservato (o proxy). In questo modo non potrai ricevere l'e-mail di convalida agli indirizzi di contatto registrati.

Per ricevere e-mail, assicurati che le informazioni di contatto siano pubbliche in WHOIS oppure, se nell'elenco WHOIS è visualizzato un indirizzo e-mail riservato, assicurati che l'e-mail inviata

all'indirizzo riservato venga inoltrata al tuo indirizzo e-mail reale. Una volta completata la configurazione WHOIS e finché non si verifica il timeout della richiesta di certificato, puoi scegliere di inviare di nuovo l'e-mail di convalida. ACM esegue una nuova ricerca WHOIS/MX e invia e-mail di convalida all'indirizzo di contatto ora diventato pubblico.

## Rinnovo dei certificati

Se hai reso pubbliche le informazioni WHOIS quando hai richiesto un nuovo certificato e successivamente hai nascosto le tue informazioni, ACM non può recuperare i tuoi indirizzi di contatto registrati quando tenti di rinnovare il certificato. ACM invia e-mail di convalida a questi indirizzi di contatto e a cinque indirizzi di amministrazione comuni formati utilizzando il tuo registro MX. Per risolvere questo problema, rendi di nuovo pubbliche le tue informazioni WHOIS e invia di nuovo le e-mail di convalida. ACM esegue una nuova ricerca WHOIS/MX e invia e-mail di convalida agli indirizzi di contatto ora diventati pubblici.

## Limitazione di WHOIS

A volte ACM non è in grado di contattare il server WHOIS neanche dopo aver inviato più richieste per l'e-mail di convalida. Questo problema è esterno a AWS. In altre parole, AWS non controlla i server WHOIS e non è in grado di impedire il throttling del server WHOIS. Se si verifica questo problema, inserisci una richiesta presso il [Centro AWS Support](#) per trovare una soluzione.

## Timestamp iniziale persistente per la convalida tramite e-mail

Il timestamp della prima richiesta di convalida e-mail di un certificato persiste attraverso le richieste successive di rinnovo della convalida. Non costituisce la prova di un errore nelle operazioni ACM.

## Risolvere i problemi relativi al dominio di primo livello .IO

Il dominio di primo livello .IO viene assegnato al Territorio britannico dell'Oceano Indiano. Al momento, il registro del dominio non visualizza le informazioni pubbliche dal database WHOIS. Ciò è valido sia che la protezione della privacy per il dominio sia abilitata o meno. I registrar possono visualizzare queste informazioni nei propri output WHOIS se la protezione della privacy è disabilitata, ma questa pratica varia da un registrar all'altro. ACM non è in grado di inviare e-mail di convalida ai seguenti tre indirizzi di contatto registrati se non sono resi disponibili dal registrar in WHOIS.

- Registrant del dominio
- Contatto tecnico
- Contatto amministrativo

ACM, tuttavia, invia un'e-mail di convalida ai seguenti cinque indirizzi di sistema comunemente usati in cui *your\_domain* è il nome del dominio inserito quando viene inizialmente richiesto un certificato e *.io* è il dominio di primo livello.

- administrator@*your\_domain*.IO
- hostmaster@*your\_domain*.IO
- postmaster@*your\_domain*.IO
- webmaster@*your\_domain*.IO
- admin@*your\_domain*.IO

Per ricevere l'e-mail di convalida mail per un dominio .IO, assicurati di disporre di uno degli ultimi 5 account e-mail abilitati. In caso contrario, non riceverai l'e-mail di convalida e non sarà emesso un certificato ACM.

#### Note

Si consiglia di utilizzare la convalida DNS anziché la convalida e-mail. Per ulteriori informazioni, consulta [Convalida DNS](#).

## Se non si riesce a passare alla convalida del DNS

Dopo aver creato un certificato con convalida e-mail, non è possibile passare alla convalida con DNS.

## Risoluzione dei problemi relativi al rinnovo dei certificati gestiti

ACM cerca di rinnovare automaticamente i tuoi certificati ACM prima della scadenza, in modo che non sia richiesta alcuna azione da parte tua. Consulta i seguenti argomenti in caso di problemi con [Rinnovo gestito per i certificati ACM](#).

## Preparazione per la convalida automatica dei domini

Prima che ACM possa rinnovare i certificati automaticamente, le seguenti condizioni devono essere soddisfatte:

- Il certificato deve essere associato a un AWS servizio integrato con ACM. Per ulteriori informazioni sulle risorse supportate da ACM, consultare [Servizi integrati con AWS Certificate Manager](#).

- Per i certificati convalidati tramite e-mail, ACM deve essere in grado di contattarti a un indirizzo e-mail amministratore per ciascun dominio elencato nel tuo certificato. Gli indirizzi e-mail che verranno provati sono elencati in [Convalida e-mail](#).
- Per i certificati convalidati tramite DNS, assicurati che la configurazione DNS contenga i registri CNAME corretti come descritto in [Convalida DNS](#).

## Gestione degli errori relativi al rinnovo gestito dei certificati

Quando il certificato si avvicina alla data di scadenza (60 giorni per DNS, 45 per EMAIL e 60 giorni per Private), ACM tenta di rinnovarlo se soddisfa i [criteri di idoneità](#). Affinché il rinnovo riesca, potrebbe essere necessario intraprendere delle azioni. Per ulteriori informazioni, consulta [Rinnovo gestito per i certificati ACM](#).

### Rinnovo gestito del certificato per i certificati convalidati tramite e-mail

I certificati ACM sono validi per 13 mesi (395 giorni). Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACM inizia a inviare avvisi di rinnovo 45 giorni prima della scadenza, utilizzando gli indirizzi della casetta postale WHOIS del dominio e a cinque indirizzi amministratore comuni. Le notifiche contengono un link su cui il proprietario del dominio può cliccare per il rinnovo. Una volta convalidati tutti i domini elencati, ACM rilascia un certificato rinnovato con lo stesso ARN.

Consulta [Convalida tramite e-mail](#) per le istruzioni su come identificare i domini che sono nello stato PENDING\_VALIDATION e ripetere il processo di convalida per quei domini.

### Rinnovo gestito del certificato per i certificati convalidati tramite DNS

ACM non tenta la convalida TLS per i certificati convalidati da DNS. Se ACM non riesce a rinnovare un certificato convalidato tramite DNS, è molto probabilmente dovuto a registri CNAME mancanti o inesatti nella configurazione DNS. In questo caso, ACM ti avverte che il certificato non può essere rinnovato automaticamente.

#### Important

Devi inserire i record CNAME corretti nel database DNS. Per informazioni su come fare, consulta il tuo registrar di dominio.

Puoi trovare i record CNAME per i tuoi domini espandendo il certificato e le voci di dominio nella console ACM. Fai riferimento alle illustrazioni seguenti per i dettagli. Puoi anche recuperare i record CNAME utilizzando l'[DescribeCertificate](#) operazione nell'API ACM o il [comando describe-certificate](#) nella CLI ACM. Per ulteriori informazioni, consulta [Convalida DNS](#).

The screenshot shows the AWS Certificate Manager console. At the top, there is a table listing certificates. The third row, for the certificate 'amzn3.example.biz', is highlighted with a red border. Below the table, the 'Status' section shows the certificate is 'Issued' and provides a 'Detailed status' of 'The certificate was issued at 2018-03-22T22:42:12UTC'. A table under 'Domain' shows the domain 'amzn3.example.biz' with a 'Success' validation status. The 'Details' section provides various metadata including 'Type', 'In use?', 'Domain name', 'Number of additional names', 'Identifier', 'Serial number', 'Requested at', 'Issued at', 'Not before', 'Not after', 'Public key info', 'Signature algorithm', 'ARN', and 'Validation state'. At the bottom, there is a 'Tags' section with an 'Edit' button and a text input field.

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
amzn1.example.biz	amzn1.example.biz		Issued	Amazon Issued	No	Ineligible
amzn2.example.biz	amzn2.example.biz		Validation timed out	Amazon Issued	No	Ineligible
amzn3.example.biz	amzn3.example.biz		Issued	Amazon Issued	No	Ineligible

**Status**

**Status** Issued  
**Detailed status** The certificate was issued at 2018-03-22T22:42:12UTC

Domain	Validation status
amzn3.example.biz	Success

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

**Details**

<b>Type</b>	Amazon Issued	<b>Requested at</b>	2018-03-22T22:38:52UTC
<b>In use?</b>	No	<b>Issued at</b>	2018-03-22T22:42:12UTC
<b>Domain name</b>	amzn3.example.biz	<b>Not before</b>	2018-03-22T00:00:00UTC
<b>Number of additional names</b>	0	<b>Not after</b>	2019-04-22T12:00:00UTC
<b>Identifier</b>	1fae4ec1-6db6-4d3d-967a-ee5e53ecd45	<b>Public key info</b>	RSA 2048-bit
<b>Serial number</b>	0e:10:30:f3:1c:b4:1e:b7:54:bb:f3:99:62:5b:7f:fb	<b>Signature algorithm</b>	SHA256WITHRSA
		<b>ARN</b>	arn:aws:acm:us-west-2:140948901414:certificate/1fae4ec1-6db6-4d3d-967a-ee5e53ecd45
		<b>Validation state</b>	None

**Tags**

Name

Scegli il certificato di destinazione dalla console.

Domain	Validation status
amzn3.example.biz	Success

Add the following CNAME record to the DNS configuration for your domain. The procedure for adding CNAME records depends on your DNS service Provider. [Learn more.](#)

Name	Type	Value
_dc8d107e33e2a83816b6a2a395a5cf5d.amzn.example.biz.	CNAME	_dadbc0aaa5530cf8b0964967cf1d4ed8.acm-validations.aws.

**Note:** Changing the DNS configuration allows ACM to issue certificates for this domain name for as long as the DNS record exists. You can revoke permission at any time by removing the record. [Learn more.](#)

[Create record in Route 53](#) **Amazon Route 53 DNS Customers** ACM can update your DNS configuration for you. [Learn more.](#)

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file

Espandi la finestra del certificato per trovare le informazioni CNAME del certificato.

Se il problema persiste, contatta il [Centro di supporto](#).

## Informazioni sulla tempistica di rinnovo

[Rinnovo gestito per i certificati ACM](#) è un processo asincrono. Ciò significa che i passaggi non si verificano consecutivamente. Dopo che tutti i nomi del dominio in un certificato ACM sono stati convalidati, potrebbe esserci un ritardo prima che ACM ottenga il nuovo certificato. Si può verificare un ritardo aggiuntivo tra il momento in cui ACM ottiene il certificato rinnovato e il momento in cui il certificato viene distribuito alle risorse AWS che lo utilizzano. Di conseguenza, è possibile che le modifiche allo stato del certificato impieghino diverse ore prima di essere visualizzate nella console.

## Risoluzione di altri problemi

In questa sezione vengono fornite indicazioni per i problemi non correlati al rilascio o alla convalida dei certificati ACM.

## Argomenti

- [Problemi di autorizzazione per Certification Authority \(CAA\)](#)
- [Problemi di importazione dei certificazioni](#)
- [Problemi di associazione dei certificati](#)
- [Problemi con API Gateway](#)
- [Cosa fare quando un certificato smette di funzionare in modo imprevisto](#)
- [Problemi con il ruolo collegato al servizio ACM](#)

## Problemi di autorizzazione per Certification Authority (CAA)

È possibile utilizzare record DNS di tipo CAA per specificare che l'autorità di certificazione (CA) di Amazon può emettere certificati ACM per il dominio e per il sottodominio. Se si riceve un messaggio di errore durante l'emissione di certificati che avvisa che uno o più nomi di dominio non sono stati convalidati a causa di un errore relativo all'Autenticazione dell'autorità di certificazione (CAA), verificare i record CAA del DNS. Se si riceve questo errore dopo che la richiesta del certificato ACM è stata convalidata correttamente, sarà necessario aggiornare i registri CAA e richiedere nuovamente un certificato. Il campo valore deve contenere uno dei seguenti nomi di dominio in nel record CAA:

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

Per ulteriori informazioni relative alla creazione di record CAA, consultare [\(Opzionale\) Configurazione di un registro CAA](#).

### Note

Puoi scegliere di non configurare un record CAA per il dominio se non vuoi consentire il controllo CAA.

## Problemi di importazione dei certificazioni

Puoi importare certificati di terze parti in ACM e associarli ai [servizi integrati](#). In caso di problemi, consulta gli argomenti correlati ai [prerequisiti](#) e [al formato dei certificati](#). In particolare, tieni presente quanto segue:

- Puoi importare solo i certificati SSL/TLS X.509 versione 3.
- Il certificato può essere autofirmato oppure può essere firmato da un'autorità di certificazione (CA).
- Se il certificato è firmato da una CA, devi includere una catena di certificati intermedia che fornisce un percorso alla radice dell'autorità.
- Se il certificato è autofirmato, devi includere la chiave privata in testo normale.
- Ogni certificato nella catena deve certificare direttamente quello precedente.
- Non includere il certificato dell'entità finale nella catena di certificati intermedia.
- I tuoi certificati, la catena di certificati e la chiave privata devono essere codificati con PEM. In generale, la codifica PEM è costituita da blocchi di testo ASCII codificati Base64 che iniziano e terminano con header e footer di testo normale. Non è necessario aggiungere righe o spazi o apportare altre modifiche a un file PEM durante la copia o il caricamento. È possibile verificare le catene di certificati utilizzando l'[utility di verifica OpenSSL](#).
- La chiave privata (se presente) non deve essere crittografata. (Suggerimento: se ha una passphrase, è crittografata.)
- I servizi [integrati](#) con ACM devono utilizzare algoritmi e dimensioni delle chiavi supportati da ACM-supported. Consulta la Guida per AWS Certificate Manager l'utente e la documentazione di ciascun servizio per assicurarti che il certificato funzioni.
- Il supporto del certificato da parte dei servizi integrati può variare a seconda se il certificato è importato in IAM o in ACM.
- Il certificato deve essere valido quando viene importato.
- Le informazioni dettagliate per tutti i tuoi certificati sono visualizzate nella console. Per impostazione predefinita, tuttavia, se richiami l'[ListCertificates](#) API o il AWS CLI comando [list-certificates](#) senza specificare il keyTypes filtro, vengono visualizzati solo RSA\_1024 o RSA\_2048 i certificati.

## Problemi di associazione dei certificati

Per rinnovare un certificato, ACM genera una nuova coppia di chiavi di accesso pubblica-privata. Se l'applicazione utilizza [Associazione dei certificati](#), a volte noto come pinning SSL, per bloccare un



certificato ACM, l'applicazione potrebbe non essere in grado di connettersi al dominio dopo il rinnovo del certificato. AWS Per questo motivo, ti consigliamo di non associare un certificato ACM. Se la tua applicazione deve associare un certificato, puoi eseguire quanto indicato di seguito:

- [Importa il tuo certificato su ACM](#), quindi associa l'applicazione al certificato importato. ACM non fornisce il rinnovo gestito per i certificati importati.
- Se stai utilizzando un certificato pubblico, aggiungi la tua applicazione a tutti i [certificati root Amazon](#) disponibili. Se stai utilizzando un certificato privato, aggiungi la tua applicazione a un certificato root CA.

## Problemi con API Gateway

Quando distribuisce un endpoint API ottimizzato per l'edge, API Gateway imposta CloudFront una distribuzione per te. La CloudFront distribuzione è di proprietà di API Gateway, non del tuo account. La distribuzione è associata al certificato ACM utilizzato per la distribuzione dell'API. Per rimuovere l'associazione e permettere ad ACM di eliminare il certificato, devi rimuovere il dominio personalizzato API Gateway associato al certificato.

Quando implementi un endpoint API regionale, API Gateway crea un Application Load Balancer (ALB) a tuo nome. Il load balancer è di proprietà di API Gateway e non è visibile a te. L'ALB è associato al certificato ACM utilizzato per la distribuzione dell'API. Per rimuovere l'associazione e permettere ad ACM di eliminare il certificato, devi rimuovere il dominio personalizzato API Gateway associato al certificato.

## Cosa fare quando un certificato smette di funzionare in modo imprevisto

Se un certificato ACM è stato associato correttamente a un servizio integrato ma il certificato smette di funzionare e il servizio integrato inizia a restituire errori, la causa potrebbe essere una modifica delle autorizzazioni necessarie al servizio per utilizzare un certificato ACM.

Ad esempio, Elastic Load Balancing (ELB) richiede l'autorizzazione per decrittografare e, a sua volta, decripta la chiave privata del certificato. AWS KMS key Questa autorizzazione viene concessa da una policy basata sulle risorse che ACM applica quando si associa un certificato a ELB. Se ELB perde la concessione per tale autorizzazione, non riuscirà al successivo tentativo a decrittare la chiave del certificato.

Per esaminare il problema, controlla lo stato delle tue sovvenzioni utilizzando la console all'indirizzo. AWS KMS <https://console.aws.amazon.com/kms> Esegui una delle seguenti azioni:

- Se ritieni che le autorizzazioni concesse a un servizio integrato siano state revocate, visita la console del servizio integrato, dissocia il certificato dal servizio, quindi associalo nuovamente. In questo modo sarà riapplicata la policy basata sulle risorse e sarà concessa una nuova autorizzazione.
- Se ritieni che le autorizzazioni concesse ad ACM siano state revocate, contattaci all'indirizzo <https://console.aws.amazon.com/support/home#/>. AWS Support

## Problemi con il ruolo collegato al servizio ACM

[Quando emetti un certificato firmato da una CA privata che è stato condiviso con te da un altro account, ACM tenta al primo utilizzo di impostare un ruolo collegato ai servizi \(SLR\) per interagire come principale con una politica di accesso basata sulle risorse. CA privata AWS](#) Se rilasci un certificato privato da una CA condivisa e l'SLR non è disponibile, ACM non sarà in grado di rinnovare automaticamente tale certificato.

ACM potrebbe avvisarti che non è in grado di determinare se esiste un SLR sul tuo account. Se l'autorizzazione `iam:GetRole` richiesta è già stata concessa ad ACM SLR per il tuo account, l'avviso non si ripeterà dopo la creazione del SLR. In caso di ripetizione, l'utente o l'amministratore dell'account potrebbe essere necessario concedere l'autorizzazione `iam:GetRole` ad ACM o associare il proprio account con il `AWSCertificateManagerFullAccess` della policy gestito da ACM.

Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Gestione delle eccezioni

Un AWS Certificate Manager comando potrebbe non riuscire per diversi motivi. Per informazioni su ciascuna eccezione, vedi la tabella riportata di seguito.

### Gestione delle eccezioni per i certificati privati

Le seguenti eccezioni possono verificarsi quando si tenta di rinnovare un certificato PKI privato emesso da CA privata AWS

**Note**

CA privata AWS non è supportato nella regione Cina (Pechino) e nella regione Cina (Ningxia).

Codice di errore ACM	Commento
PCA_ACCESS_DENIED	<p>La CA privata non dispone delle autorizzazioni ACM. Ciò attiva un CA privata AWS <code>AccessDeniedException</code> codice di errore.</p> <p>Per risolvere il problema, concedi le autorizzazioni necessarie al responsabile del servizio ACM che utilizza l'operazione. CA privata AWS <a href="#">CreatePermission</a></p>
PCA_INVALID_DURATION	<p>Il periodo di validità del certificato richiesto supera il periodo di validità della CA privata emittente. Ciò attiva un CA privata AWS <code>ValidationException</code> codice di errore.</p> <p>Per risolvere il problema, <a href="#">installa un nuovo certificato CA</a> con un periodo di validità appropriato.</p>
PCA_INVALID_STATE	<p>La CA privata chiamata non è nello stato corretto per eseguire l'operazione ACM richiesta. Ciò attiva un codice di CA privata AWS <code>InvalidStateException</code> errore.</p> <p>Risolvere il problema come segue:</p> <ul style="list-style-type: none"> <li>• Se la CA ha lo stato <code>CREATING</code>, attendi il completamento della creazione e quindi installa il certificato CA.</li> </ul>

Codice di errore ACM	Commento
	<ul style="list-style-type: none"><li>• Se la CA ha lo stato PENDING_CERTIFICATE, installa il certificato CA.</li><li>• Se la CA ha lo stato DISABLED, aggiornala allo stato ACTIVE.</li><li>• Se la CA ha lo stato DELETED, ripristinala.</li><li>• Se la CA ha lo stato EXPIRED, installa un nuovo certificato</li><li>• Se la CA ha lo stato FAILED e non puoi risolvere il problema, contatta <a href="#">AWS Support</a>.</li></ul>
PCA_LIMIT_EXCEEDED	<p>La CA privata ha raggiunto una quota di emissione. Ciò attiva un codice di CA privata <code>AWS LimitExceededException</code> errore. Prova a ripetere la richiesta prima di procedere con questa guida.</p> <p>Se l'errore persiste, contatta <a href="#">AWS Support</a> per richiedere un aumento della quota.</p>
PCA_REQUEST_FAILED	<p>Si è verificato un errore di rete o di sistema. Ciò attiva un codice di CA privata <code>AWS RequestFailedException</code> errore. Prova a ripetere la richiesta prima di procedere con questa guida.</p> <p>Se l'errore persiste, contatta <a href="#">AWS Support</a>.</p>
PCA_RESOURCE_NOT_FOUND	<p>La CA privata è stata eliminata definitivamente. Ciò attiva un codice di CA privata <code>AWS ResourceNotFoundException</code> errore. Verifica di aver utilizzato l'ARN corretto. Se ciò non riesce, non potrai utilizzare questa CA.</p> <p>Per risolvere il problema, <a href="#">crea una nuova CA</a>.</p>

Codice di errore ACM	Commento
SLR_NOT_FOUND	Per rinnovare un certificato firmato da una CA privata in un altro account, ACM richiede un ruolo collegato al servizio (SLR) sull'account in cui si trova il certificato. Se è necessario ricreare un SLR eliminato, consulta <a href="#">Creazione del SLR per ACM</a> .

# Concetti

In questa sezione vengono fornite le definizioni dei concetti utilizzati da AWS Certificate Manager.

## Argomenti

- [Certificato ACM](#)
- [ACM Root CA](#)
- [Dominio Apex](#)
- [Crittografia delle chiavi asimmetrica](#)
- [Certificate Authority \(Autorità di certificazione\)](#)
- [Registrazione della trasparenza del certificato](#)
- [Domain Name System](#)
- [Nomi di dominio](#)
- [Crittografia e decrittografia](#)
- [Nome di dominio completo \(FQDN\)](#)
- [Infrastruttura a chiave pubblica](#)
- [Certificato root](#)
- [Secure Sockets Layer \(SSL\)](#)
- [HTTPS sicuro](#)
- [Certificati del server SSL](#)
- [Crittografia delle chiavi simmetrica](#)
- [Transport Layer Security \(TLS\)](#)
- [Trust](#)

## Certificato ACM

ACM genera certificati X.509 versione 3, ognuno valido per 13 mesi (395 giorni) e contenente le estensioni indicate di seguito.

- Vincoli di base: consente di specificare se l'oggetto del certificato è un'autorità di certificazione (CA).

- **Identificatore chiave autorità:** consente di identificare la chiave pubblica corrispondente alla chiave privata utilizzata per firmare il certificato.
- **Identificatore chiave oggetto:** consente di identificare certificati che contengono una determinata chiave pubblica.
- **Utilizzo chiave:** definisce lo scopo della chiave pubblica incorporata nel certificato.
- **Utilizzo chiave esteso:** specifica una o più finalità per le quali la chiave pubblica può essere utilizzata in aggiunta alle finalità specificate dall'estensione Utilizzo chiave.
- **Punti di distribuzione CRL:** specifica dove possono essere ottenute le informazioni CRL.

Il testo in chiaro di un certificato rilasciato da ACM è simile al seguente esempio:

```
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
```

## ACM Root CA

I certificati di entità pubblica emessi da ACM derivano la loro fiducia dalle seguenti CA principali di Amazon:



Nome distinto	Algoritmo di crittografia
CN=Amazon Root CA 1,O=Amazon,C=US	RSA a 2048 bit (RSA_2048)
CN=Amazon Root CA 2,O=Amazon,C=US	RSA a 4096 bit (RSA_4096)
CN=Amazon Root CA 3,O=Amazon,C=US	Elliptic Prime Curve a 256 bit (EC_prime256v1 )
CN=Amazon Root CA 4,O=Amazon,C=US	Elliptic Prime Curve a 384 bit (EC_secp384r1 )

La radice predefinita della fiducia per i certificati rilasciati da ACM è CN=Amazon Root CA 1, O = Amazon, C = US, che offre sicurezza RSA a 2048 bit. Le altre radici sono riservate all'uso futuro. Tutte le radici sono sottoscritte dal certificato Starfield Services Root Certificate Authority.

Per ulteriori informazioni, consulta [Amazon Trust Services](#).

## Dominio Apex

Per informazioni, consulta [Nomi di dominio](#).

## Crittografia delle chiavi asimmetrica

A differenza della [Crittografia delle chiavi simmetrica](#), la crittografia asimmetrica utilizza chiavi differenti ma matematicamente correlate per criptare e decriptare i contenuti. Una delle chiavi è pubblica e in genere è disponibile in un certificato X.509 v3. L'altra chiave è privata e archiviata in modo sicuro. Il certificato X.509 associa l'identità di un utente, un computer o altre risorse (l'oggetto del certificato) alla chiave pubblica.

ACM genera certificati X.509 di tipo SSL/TLS che collegano l'identità del sito Web e i dettagli dell'organizzazione alla chiave pubblica inclusa nel certificato. ACM utilizza il tuo AWS KMS key per crittografare la chiave privata. Per ulteriori informazioni, consulta [Sicurezza per le chiavi private dei certificati](#).

## Certificate Authority (Autorità di certificazione)

Un'autorità di certificazione (CA) è un'entità che emette i certificati digitali. Il tipo più comune di certificato digitale disponibile in commercio si basa sullo standard ISO X.509. L'autorità di certificazione emette certificati firmati che confermano l'identità dell'oggetto del certificato stesso e la associano alla chiave pubblica contenuta nel certificato. Un'autorità di certificazione in genere gestisce anche la revoca dei certificati.

## Registrazione della trasparenza del certificato

Come protezione contro i certificati SSL/TLS emessi per errore o da autorità di certificazione compromesse, alcuni browser richiedono che i certificati pubblici emessi per uno specifico dominio vengano aggiunti a un registro di trasparenza dei certificati, in cui viene registrato il nome del dominio, ma non la chiave privata. I certificati non registrati in genere generano un errore all'interno del browser.

È possibile monitorare i registri per fare in modo che per il proprio dominio siano stati emessi solo i certificati autorizzati. Per controllare i registri è possibile utilizzare un servizio apposito, ad esempio [Certificate Search](#).

Prima di emettere un certificato SSL/TLS pubblicamente attendibile per un dominio, Amazon CA invia il certificato ad almeno due server di registrazione della trasparenza. I server aggiungono il certificato al proprio database pubblico e restituiscono alla CA Amazon un timestamp firmato del certificato (SCT). La CA incorpora quindi l'SCT nel certificato, lo firma e lo emette all'utente. I timestamp sono inclusi con altre estensioni X.509.

X509v3 extensions:

CT Precertificate SCTs:

Signed Certificate Timestamp:

Version : v1(0)  
Log ID : *BB:D9:DF:...8E:1E:D1:85*  
Timestamp : Apr 24 23:43:15.598 2018 GMT  
Extensions: none  
Signature : ecdsa-with-SHA256  
*30:45:02:...18:CB:79:2F*

Signed Certificate Timestamp:

Version : v1(0)  
Log ID : *87:75:BF:...A0:83:0F*

```
Timestamp : Apr 24 23:43:15.565 2018 GMT
Extensions: none
Signature : ecDSA-with-SHA256
           30:45:02:...29:8F:6C
```

La registrazione della trasparenza del certificato è automatica al momento della richiesta o del rinnovo di un certificato, a meno che non si decida di disattivarla. Per ulteriori informazioni sulla disattivazione, consultare [Annullamento della registrazione della trasparenza del certificato..](#)

## Domain Name System

Il DNS (Domain Name System) è un sistema di denominazione di distribuzione gerarchica per computer e altre risorse connesse a Internet o a una rete privata. Il DNS viene utilizzato principalmente per convertire nomi di dominio in formato testo, ad esempio `aws.amazon.com`, in indirizzi IP numerici nel formato `111.122.133.144`. Il database DNS per uno specifico dominio, tuttavia, contiene una serie di record che possono essere utilizzati per altri scopi. Ad esempio, con ACM è possibile utilizzare un registro CNAME per confermare che si gestisce o controlla un dominio quando si richiede un certificato. Per ulteriori informazioni, consulta [Convalida DNS](#).

## Nomi di dominio

Un nome di dominio è una stringa di testo come `www.example.com` che il DNS (Domain Name System) può convertire in un indirizzo IP. Le reti di computer, inclusa Internet, utilizzano gli indirizzi IP anziché i nomi di testo. Un nome di dominio è composto da etichette distinte separate da punti:

### TLD

L'etichetta più a destra viene denominata dominio di primo livello (TLD). Esempi comuni comprendono `.com`, `.net` e `.edu`. Inoltre, il TLD per le entità registrate in alcuni paesi è l'abbreviazione del nome del paese e viene denominato codice paese. Esempi includono `.uk` per il Regno Unito, `.ru` per la Russia e `.fr` per la Francia. Quando si utilizzano i codici paese, viene spesso introdotta per il TLD una gerarchia di secondo livello per identificare il tipo di entità registrata. Ad esempio, il TLD `.co.uk` identifica le imprese commerciali del Regno Unito.

### Dominio apex

Il nome di dominio apex include e si espande nel dominio di primo livello. Per i nomi di dominio che includono un codice paese, il dominio apex include il codice e le etichette, se presenti,

che identificano il tipo di entità registrata. Il dominio apex non include sottodomini (vedere il paragrafo seguente). In `www.example.com`, il nome del dominio apex è `example.com`. In `www.example.co.uk`, il nome del dominio apex è `example.co.uk`. Altri nomi che sono spesso utilizzati al posto di apex includono `base`, `base`, `root`, `root apex` o `apex di zona`.

## Sottodominio

I nomi di sottodominio precedono il nome di dominio apex e sono separati da esso e tra di loro da un punto. Il nome di sottodominio più comune è `www`, ma è possibile usare qualsiasi nome. I nomi di sottodominio possono avere più livelli. Ad esempio, in `jake.dog.animals.example.com`, i sottodomini sono `jake`, `dog` e `animals` in questo ordine.

## Superdominio

Il dominio a cui appartiene un sottodominio.

## FQDN

Un nome di dominio completo (FQDN) è il nome DNS completo di un computer, sito Web o altre risorse connessi a una rete o a Internet. Ad esempio `aws.amazon.com` è il nome di dominio completo (FQDN) per Amazon Web Services. Un FQDN include tutti i domini fino al dominio di primo livello. Ad esempio, `[subdomain1].[subdomain2]. . . [subdomainn].[apex domain].[top-level domain]` rappresenta il formato generale di un nome di dominio completo (FQDN).

## PQDN

Un nome di dominio non completo si definisce nome di dominio parzialmente qualificato (PQDN) ed è ambiguo. Un nome come `[subdomain1.subdomain2.]` è un nome di dominio parzialmente qualificato (PQDN) poiché non è possibile determinare il dominio root.

## Registration (Registrazione)

Il diritto di utilizzare un nome di dominio è delegato ai registrar dei nomi di dominio. I registrar sono in genere accreditati dalla ICANN (Internet Corporation for Assigned Names and Numbers). Inoltre, altre organizzazioni denominate registri gestiscono i database TLD. Quando si richiede un nome di dominio, il registrar invia le informazioni al registro TLD appropriato. Il registro assegna un nome di dominio, aggiorna il database TLD e pubblica le informazioni su WHOIS. Di solito, i nomi di dominio devono essere acquistati.

# Crittografia e decrittografia

La crittografia è il processo che garantisce la riservatezza dei dati. La decrittografia è il processo inverso e consente di recuperare i dati originali. I dati non criptati in genere vengono definiti "testo normale", anche se non sono testi veri e propri. I dati crittografati in genere vengono definiti "testo cifrato". La crittografia HTTPS dei messaggi tra client e server utilizza algoritmi e chiavi. Gli algoritmi definiscono la step-by-step procedura mediante la quale i dati in chiaro vengono convertiti in testo cifrato (crittografia) e il testo cifrato viene riconvertito nel testo normale originale (decrittografia). Durante il processo di crittografia o decrittografia, gli algoritmi utilizzano delle chiavi, che possono essere private o pubbliche.

## Nome di dominio completo (FQDN)

Per informazioni, consulta [Nomi di dominio](#).

## Infrastruttura a chiave pubblica

Un'infrastruttura a chiave pubblica (PKI) è composta dall'hardware, dal software, dalle persone, dalle policy, dalle procedure e dai documenti necessari per creare, emettere, gestire, distribuire, utilizzare, archiviare e revocare i certificati digitali. La PKI consente il trasferimento sicuro di informazioni su reti di computer.

## Certificato root

Un'autorità di certificazione (CA) esiste in genere all'interno di una struttura gerarchica che contiene altre CA con relazioni padre-figlio chiaramente definite tra loro. Le CA figlio o subordinate sono certificate dalle CA padre, creando così una catena di certificati. La CA al livello più alto della gerarchia è detta CA root e il suo certificato viene denominato certificato root. Questo certificato generalmente è autofirmato.

## Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono protocolli di crittografia che garantiscono la sicurezza delle comunicazioni su una rete di computer. TLS è il successore di SSL. Entrambi utilizzano i certificati X.509 per autenticare il server. Entrambi i protocolli negoziano tra il client e il server una chiave simmetrica che viene utilizzata per crittografare il flusso di dati tra due entità.

## HTTPS sicuro

HTTPS sta per HTTP su SSL/TLS, un formato sicuro di HTTP che è supportato da tutti i principali browser e server. Tutte le richieste e risposte HTTP sono crittografate prima che vengano inviate attraverso una rete. HTTPS combina il protocollo HTTP con tecniche di crittografia simmetrica, asimmetrica e basata su certificati X.509. HTTPS funziona inserendo un livello di sicurezza crittografico sotto il livello di applicazione HTTP e sopra il livello di trasporto TCP nel modello OSI (Open Systems Interconnection). Il livello di protezione usa il protocollo Secure Sockets Layer (SSL) o il protocollo Transport Layer Security (TLS).

## Certificati del server SSL

Le transazioni HTTPS richiedono certificati del server per autenticare un server. Un certificato del server è una struttura di dati X.509 v3 che associa la chiave pubblica nel certificato all'oggetto del certificato. Un certificato SSL/TLS viene firmato da un'autorità di certificazione (CA) e contiene il nome del server, il periodo di validità, la chiave pubblica, l'algoritmo di firma e altri elementi.

## Crittografia delle chiavi simmetrica

La crittografia delle chiavi simmetrica utilizza la stessa chiave sia per crittografare che per decriptare i dati digitali. Consulta anche [Crittografia delle chiavi asimmetrica](#).

## Transport Layer Security (TLS)

Per informazioni, consulta [Secure Sockets Layer \(SSL\)](#).

## Trust

Per poter considerare attendibile l'identità di un sito Web, un browser Web deve essere in grado di verificare il certificato di tale sito. I browser, tuttavia, considerano attendibili solo un ristretto numero di certificati noti come certificati root CA. Una terza parte attendibile, nota come autorità di certificazione (CA), convalida l'identità del sito Web ed emette un certificato digitale firmato all'operatore del sito Web. Il browser può quindi verificare la firma digitale per convalidare l'identità del sito Web. Se la convalida riesce, verrà visualizzata un'icona a forma di lucchetto nella barra degli indirizzi.

# Cronologia dei documenti

Nella tabella seguente è descritta la cronologia delle versioni della documentazione di AWS Certificate Manager a partire dal 2018.

Modifica	Descrizione	Data
<a href="#">Imminente deprecazione della verifica via e-mail WHOIS</a>	È stata aggiunta una nota sull'obsolescenza della verifica via e-mail WHOIS a partire da giugno 2024.	5 febbraio 2024
<a href="#">Aggiunto il supporto per le chiavi di condizione</a>	È stato aggiunto il supporto per le chiavi di condizione IAM durante la richiesta di certificati ACM. Per un elenco delle condizioni supportate, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported">https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported</a> .	24 agosto 2023
<a href="#">Aggiunto il supporto ECDSA</a>	Aggiunto il supporto per l'Elliptic Curve Digital Signature Algorithm (ECDSA) quando si richiede un certificato ACM pubblico. Per un elenco degli algoritmi chiave supportati, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms">https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms</a> .	8 novembre 2022
<a href="#">Nuovi eventi CloudWatch</a>	Aggiunti gli eventi ACM Certificate Expired, ACM Certificate Available e ACM	27 ottobre 2022

---

	<p>Certificate Renewal Action Required. Per un elenco degli CloudWatch eventi supportati, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html">https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html</a>.</p>	
<p><a href="#">Aggiornamento dei tipi di algoritmi chiave per l'importazione</a></p>	<p>I certificati importati in ACM possono avere chiavi con algoritmi aggiuntivi RSA ed Elliptic Curve. Per un elenco degli algoritmi chiave attualmente supportati, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html">https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html</a>.</p>	14 luglio 2021
<p><a href="#">Promozione di "Monitoraggio e registrazione" come capitolo separato</a></p>	<p>Documentazione di monitoraggio e registrazione spostata nel capitolo appropriato. Questa modifica riguarda CloudWatch Metriche, CloudWatch Eventi/ EventBridge e CloudTrail Per ulteriori informazioni, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html">https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html</a>.</p>	23 marzo 2021



<a href="#">Aggiunto il supporto per CloudWatch metriche ed eventi</a>	Aggiunti DaysToExpiry parametri ed eventi e API di supporto. Per ulteriori informazioni, consultare <a href="https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html">https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html</a> e <a href="https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html">https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html</a> .	3 marzo 2021
<a href="#">Aggiunta del supporto tra account</a>	Aggiunto il supporto tra account per l'utilizzo di CA private da CA privata AWS. Per ulteriori informazioni, consulta <a href="https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html">https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html</a> .	17 agosto 2020
<a href="#">Aggiunta del supporto regionale</a>	Aggiunto il sostegno regionale per le regioni AWS Cina (Pechino e Ningxia). Per un elenco completo delle aree supportate, vedere <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region</a> .	4 marzo 2020
<a href="#">Aggiunta del test del flusso di lavoro di rinnovo</a>	I clienti ora possono testare manualmente la configurazione del loro flusso di rinnovo gestito da ACM. Per ulteriori informazioni, consulta <a href="#">Test della configurazione dei rinnovi gestiti di ACM</a> .	14 marzo 2019

<a href="#">Registrazione predefinita della trasparenza del certificato</a>	Aggiunta della possibilità di pubblicare certificati pubblici ACM nei registri Trasparenza certificati per impostazione predefinita.	24 Aprile 2018
<a href="#">Avvio di CA privata AWS</a>	Avviato ACM Private Certificate Manager (CM) e l'estensione di AWS Certificate Manager che consente agli utenti di stabilire un'infrastruttura sicura gestita per il rilascio e la revoca di certificati digitali privati. Per ulteriori informazioni, consulta <a href="#">Private Certificate Authority AWS</a> .	4 aprile 2018
<a href="#">Registrazione della trasparenza del certificato</a>	È stata aggiunta la registrazione della trasparenza del certificato alle Best Practice.	27 marzo 2018

Nella tabella seguente è descritta la cronologia delle versioni della documentazione di AWS Certificate Manager prima del 2018.

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	È stata aggiunta la convalida del DNS su <a href="#">Convalida DNS</a> .	21 Novembre 2017
Nuovo contenuto	Sono stati aggiunti nuovi esempi di codice Java su <a href="#">Utilizzo dell'API (esempi Java)</a> .	12 ottobre 2017
Nuovo contenuto	Sono state aggiunte informazioni relative ai record CAA su <a href="#">(Opzionale) Configurazione di un registro CAA</a> .	21 settembre 2017

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	Sono state aggiunte informazioni relative ai domini .io su <a href="#">Risoluzione dei problemi</a> .	07 luglio 2017
Nuovo contenuto	Sono state aggiunte informazioni relative alla reimportazione di un certificato su <a href="#">Reimportazione di un certificato</a> .	07 luglio 2017
Nuovo contenuto	Sono state aggiunte informazioni relative all'associazione di un certificato su <a href="#">Best practice</a> e su <a href="#">Risoluzione dei problemi</a> .	07 luglio 2017
Nuovo contenuto	È stato aggiunto AWS CloudFormation a <a href="#">Servizi integrati con AWS Certificate Manager</a> .	27 maggio 2017
Aggiornamento	Sono state aggiunte ulteriori informazioni su <a href="#">Quote</a> .	27 maggio 2017
Nuovo contenuto	È stata aggiunta la documentazione relativa a <a href="#">Identity and Access Management per AWS Certificate Manager</a> .	28 aprile 2017
Aggiornamento	È stata aggiunta un'immagine per visualizzare l'indirizzo e-mail a cui viene inviata l'e-mail di convalida. Per informazioni, consulta <a href="#">Convalida e-mail</a> .	21 Aprile 2017

Modifica	Descrizione	Data di rilascio
Aggiornamento	Sono state aggiunte informazioni relative alla configurazione di e-mail per il tuo dominio. Per informazioni, consulta <a href="#">(Facoltativo) Configurazione dell'e-mail per il dominio in uso</a> .	6 Aprile 2017
Aggiornamento	Sono state aggiunte informazioni relative al controllo dello stato di rinnovo del certificato nella console. Per informazioni, consulta <a href="#">Verifica dello stato di rinnovo di un certificato</a> .	28 marzo 2017
Aggiornamento	Aggiornamento della documentazione per l'utilizzo di Elastic Load Balancing.	21 marzo 2017
Nuovo contenuto	Aggiunta del supporto per AWS Elastic Beanstalk e Amazon API Gateway. Per informazioni, consulta <a href="#">Servizi integrati con AWS Certificate Manager</a> .	21 marzo 2017
Aggiornamento	È stata aggiornata la documentazione relativa a <a href="#">Rinnovo gestito</a> .	20 febbraio 2017
Nuovo contenuto	È stata aggiunta la documentazione relativa a <a href="#">Importazione di certificati</a> .	13 Ottobre 2016

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	Aggiunta del supporto AWS CloudTrail per le azioni ACM. Per informazioni, consulta <a href="#">Utilizzo con CloudTrail AWS Certificate Manager</a> .	25 marzo 2016
Nuova guida	Questa versione introduce AWS Certificate Manager.	21 gennaio 2016

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.