Guida per l'utente

AWS Certificate Manager

Version 1.0

AWS Certificate Manager: Guida per l'utente

Table of Contents

Che cos'è AWS Certificate Manager?

AWS Certificate Manager (ACM) gestisce la complessità della creazione, dell'archiviazione e del rinnovo di certificati e chiavi SSL TLS X.509 pubblici e privati per proteggere i AWS siti Web e le applicazioni. È possibile fornire certificati per i AWS servizi integrati emettendoli direttamente ACM o importando certificati di terze parti nel sistema di gestione. ACM ACMi certificati possono proteggere nomi di dominio singoli, più nomi di dominio specifici, domini wildcard o combinazioni di questi. ACMi certificati wildcard possono proteggere un numero illimitato di sottodomini. Puoi anche esportare ACM certificati firmati da CA privata AWS e utilizzarli ovunque nel tuo ambiente interno. PKI

> **Note**
>
> ACMnon è destinato all'uso con un server web autonomo. Se desideri configurare un server sicuro autonomo su un'EC2istanza Amazon, il seguente tutorial contiene le istruzioni: ConfigureSSL/on TLS Amazon Linux 2023.

Argomenti

È ACM 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 utilizzando. TLS ACMi certificati vengono distribuiti tramite Elastic Load Balancing, Amazon CloudFront, API Amazon Gateway e altri AWS servizi integrati. L'applicazione più comune di questo tipo è un sito pubblico sicuro con requisiti di traffico

significativi. ACMsemplifica 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 Guida per l'utente CA privata AWS.

ACMcaratteristiche del certificato

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

> **Note**
>
> Queste caratteristiche si applicano solo ai certificati forniti daACM. Potrebbero non essere applicabili ai certificati in cui si importa ACM.

Autorità e gerarchia dei certificati

I certificati pubblici tramite cui richiedi ACM sono ottenuti da Amazon Trust Services, un'autorità di certificazione pubblica (CA) gestita da Amazon. Amazon Root da CAs 1 a 4 utilizza la firma incrociata di una vecchia radice 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 includa le radici di Amazon o Starfield si fiderà dei certificati pubblici ottenuti daACM.

I certificati leaf o end-entity ACM emessi ai clienti derivano la loro autorità da una CA principale di Amazon Trust Services tramite uno qualsiasi dei numerosi intermediari. CAs ACMassegna casualmente una CA intermedia in base al tipo di certificato (o) richiesto. RSA ECDSA Poiché la CA intermedia viene selezionata casualmente dopo la generazione della richiesta, ACM non fornisce informazioni sulla CA intermedia.

Attendibilità browser e applicazione

ACMi certificati sono considerati affidabili da tutti i principali browser, tra cui Google Chrome, Microsoft Internet Explorer e Microsoft Edge, Mozilla Firefox e Apple Safari. I browser che

considerano attendibili ACM i certificati visualizzano un'icona a forma di lucchetto nella barra di stato o nella barra degli indirizzi quando sono connessi tramiteSSL/TLSa siti che utilizzano ACM certificati. ACMi certificati sono considerati affidabili 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. OCSPe CRLs sono i meccanismi standard utilizzati per verificare se un certificato è stato revocato o meno. OCSPe CRLs 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 URL jolly 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. Cioè, il campo oggetto di un ACM certificato identifica un nome di dominio e nient'altro. Quando richiedi un ACM certificato, devi confermare

di possedere o controllare tutti i domini specificati nella richiesta. Puoi convalidare la proprietà utilizzando l'e-mail o. DNS Per ulteriori informazioni, consulta Convalida e-mail e DNSconvalida.

Periodo di validità

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

Distribuzione e rinnovo gestito

ACMgestisce il processo di rinnovo dei ACM certificati e il rifornimento dei certificati dopo il loro rinnovo. 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 ACM i certificati.

Nomi di dominio multipli

Ogni ACM certificato deve includere almeno un nome di dominio completo (FQDN) ed è possibile aggiungere altri nomi se lo si desidera. Ad esempio, quando crei un ACM certificato per`www.example.com`, puoi anche aggiungere il nome `www.example.net` se i clienti possono raggiungere il tuo sito utilizzando uno dei due nomi. Ciò vale anche per domini essenziali (noti anche come apex di zona o domini nudi). Cioè, puoi richiedere un ACM certificato per www.example.com e aggiungere il nome example.com. Per ulteriori informazioni, consulta Richiesta di un certificato pubblico.

Nomi jolly

ACMconsente di utilizzare un asterisco (*) nel nome di dominio per creare un ACM certificato 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. Attualmente, i seguenti algoritmi a chiave pubblica RSA e Elliptic Curve Digital Signature Algorithm (ECDSA) sono supportati da. ACM ACMpuò richiedere l'emissione di nuovi certificati utilizzando algoritmi contrassegnati da un asterisco (*). Gli algoritmi rimanenti sono supportati solo per i certificati importati.

> **Note**
>
> Quando si richiede un PKI certificato privato firmato da una CA di AWS Private CA, la famiglia (RSAoECDSA) di algoritmi di firma specificata deve corrispondere alla famiglia di algoritmi della chiave segreta della CA.

- RSA1024 bit () `RSA_1024`
- RSA2048 bit (*) `RSA_2048`
- RSA3072 bit () `RSA_3072`
- RSA4096 bit () `RSA_4096`
- ECDSA256 bit (*`EC_prime256v1`)
- ECDSA384 bit (*`EC_secp384r1`)
- ECDSA521 bit () `EC_secp521r1`

ECDSAle chiavi sono più piccole e offrono una sicurezza paragonabile a quella RSA delle chiavi ma con una maggiore efficienza di elaborazione. Tuttavia, non ECDSA è supportato da tutti i client di rete. La tabella seguente, adattata da NIST, mostra il livello di sicurezza rappresentativo di RSA e ECDSA con chiavi di varie dimensioni. Tutti i valori sono in bit.

Confronto della sicurezza per algoritmi e chiavi

Forza di sicurezza	RSAdimensione della chiave	ECDSAdimensione della chiave
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 a 3072 bit che una RSA chiave a 256 bit ECDSA possono essere recuperate con non più di 2.128 ipotesi.

Per informazioni su come scegliere un algoritmo, consulta il post del AWS blog How to assessment and use certificate in. ECDSA 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 IAM o meno. ACM Per ulteriori informazioni, consultare la documentazione di ogni servizio.
>
> - Per Elastic Load Balancing, consulta HTTPSListeners for Your Application Load Balancer.
> - Per CloudFront, consulta SSLTLSSupporti/Protocolli e cifrari.

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	Soddisf #2	Conse o	Nota
esempio.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"
a--esempi o.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"

Nome dominio	Soddisfa #1	Soddisf #2	Conse o	Nota
abc—esemp io.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"
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--"

Eccezioni

Tieni presente quanto segue:

- ACMnon fornisce certificati di convalida estesa (EV) o certificati di convalida dell'organizzazione (OV).
- ACMnon fornisce certificati per qualcosa di diverso dai protocolli SSL TLS /.
- Non è possibile utilizzare ACM certificati per la crittografia delle e-mail.
- ACMattualmente non consente di disattivare il rinnovo gestito dei ACM certificati per i certificati. Inoltre, il rinnovo gestito non è disponibile per i certificati in cui importiACM.
- 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 privata per un ACM certificato.
- Non puoi installare direttamente ACM i certificati sul tuo sito Web o applicazione Amazon Elastic Compute Cloud (AmazonEC2). È possibile comunque utilizzare il proprio certificato con qualsivoglia servizio integrato. Per ulteriori informazioni, consulta Servizi integrati con AWS Certificate Manager.

Regioni supportate

Visita AWS Regioni ed endpoint nella tabella delle regioni Riferimenti generali di AWSo AWS nella tabella delle regioni per vedere la disponibilità regionale perACM.

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 FQDNs più AWS regioni, devi richiedere o importare un certificato per ogni regione. Per i certificati forniti daACM, ciò significa che è necessario riconvalidare ogni nome di dominio nel certificato per ogni regione. Non è possibile copiare un certificato tra regioni.

Per utilizzare un ACM certificato con Amazon CloudFront, devi richiedere o importare il certificato nella regione Stati Uniti orientali (Virginia settentrionale). ACMi certificati 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 ACM certificato o il CA privata AWS certificato privato direttamente sul sito Web o sull'applicazione AWS basata.

> **Note**
>
> ACMI certificati pubblici possono essere installati su EC2 istanze Amazon collegate a una Nitro Enclave, ma non su altre istanze Amazon. EC2 Per informazioni sulla configurazione di un server Web autonomo su un'EC2istanza Amazon non connessa a una Nitro Enclave, consulta Tutorial: Installa un LAMP server Web su Amazon Linux 2 o Tutorial: Installa un server LAMP Web con Amazon Linux. AMI

ACMi certificati sono supportati dai seguenti servizi:

Sistema di bilanciamento del carico elastico

Elastic Load Balancing distribuisce automaticamente il traffico delle applicazioni in entrata 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 fornire contenuti sicuri suSSL/TLS, i sistemi di bilanciamento del carico richiedono che i TLS certificatiSSL/siano installati sul sistema di bilanciamento del carico o sull'istanza Amazon back-end. EC2 ACMè integrato con Elastic Load Balancing per distribuire ACM certificati 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 distribuire contenuti sicuri tramiteSSL/TLS, è CloudFront necessario che TLS i certificatiSSL/siano installati sulla CloudFront distribuzione o sulla fonte di contenuto supportata. ACMè integrato con CloudFront per distribuire ACM certificati sulla CloudFront distribuzione. Per ulteriori informazioni, consulta Getting anSSL/TLSCertificate.

> **Note**
>
> Per utilizzare un ACM certificato con CloudFront, è necessario richiederlo o importarlo 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 ACM certificato 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, consulta 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 eseguire la distribuzione 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 archiviate inACM. 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 la proliferazione di dispositivi mobili e la crescita dell'Internet of Things (IoT), è diventato sempre più comune creare dispositivi APIs che possano essere utilizzati per accedere ai dati e interagire con i sistemi di back-end. AWS Puoi utilizzare API Gateway per pubblicare, gestire,

monitorare e proteggere i tuoi. APIs Dopo aver distribuito il tuo API su API Gateway, puoi configurare un nome di dominio personalizzato per semplificarne l'accesso. Per configurare un nome di dominio personalizzato, devi fornire un TLS certificato SSL /. È possibile utilizzare ACM per generare o importare il certificato. Per ulteriori informazioni su Amazon API Gateway, consulta la Amazon API Gateway Developer Guide.

AWS Enclavi Nitro

AWS Nitro Enclaves è una EC2 funzionalità di Amazon che consente di creare ambienti di esecuzione isolati, chiamati enclavi, a partire 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 SSH accedere a un'enclave e i processi, le applicazioni o gli utenti dell'istanza principale (inclusi root o admin) non possono accedere ai dati e alle applicazioni all'interno dell'enclave.

EC2le istanze connesse ai certificati di supporto di Nitro Enclaves. ACM Per ulteriori informazioni, consulta AWS Certificate Manager per Nitro Enclaves.

> **Note**
>
> Non è possibile associare ACM certificati a un'EC2istanza che non è connessa a una 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. ACMi certificati sono inclusi come risorsa modello, il che significa che AWS CloudFormation possono richiedere ACM certificati da utilizzare con AWS i servizi per abilitare connessioni sicure. Inoltre, ACM i certificati sono inclusi in molte delle AWS risorse con cui è possibile eseguire la configurazione AWS CloudFormation.

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

Con la potente automazione fornita da AWS CloudFormation, è facile superare la quota dei certificati, soprattutto con nuovi AWS account. Ti consigliamo di seguire le ACM migliori pratiche per AWS CloudFormation.

> **Note**
>
> Se si crea un ACM certificato 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. Per ulteriori informazioni su Amplify, consulta la Guida per l'utente di AWS Amplify.

Se colleghi un dominio personalizzato alla tua applicazione, la console Amplify emette ACM un certificato 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 utilizzarlo 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 Clouds ()VPCs. Per ulteriori informazioni su Firewall di rete, consulta la Guida per gli sviluppatori di AWS Network Firewall.

Il firewall Network Firewall si integra con ACM l'TLSispezione. Se si utilizza l'TLSispezione in Network Firewall, è necessario configurare un ACM certificato per la decrittografia e la ricrittografia del TLS trafficoSSL/che attraversa il firewall. Per informazioni su come funziona Network Firewall ACM per l'TLSispezione, consulta Requisiti per l'utilizzo diSSL/TLScertificates with TLS inspection configurations nella AWS Network Firewall Developer Guide.

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 che puoi 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. Sigilli e badge di questo tipo possono essere copiati su siti che non utilizzano il ACM servizio e possono essere utilizzati in modo inappropriato per creare fiducia con falsi pretesti. 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 AWS account.

Per vedere quali quote possono essere modificate, consultate la tabella delle ACM quote nella Guida AWS generale di riferimento. Per richiedere aumenti delle quote, creare un caso nel Centro AWS Support.

Quote generali

Elemento	Quota predefinita
Numero di certificati ACM I certificati scaduti e revocati continuano a contare ai fini del totale. I certificati firmati da una CA di CA privata AWS non vengono conteggiati ai fini di questo totale.	2500
Numero di ACM certificati all'anno (ultimi 365 giorni) Puoi richiedere fino al doppio della tua quota di ACM certificati per anno, regione e account. Ad esempio, se la tua quota è di 2.500, puoi richiedere fino a 5.000 ACM certificati all'anno in una determinata regione e in un determinato account. È possibile avere solo 2.500 certifica ti 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 Centro AWS Support. I certificati firmati da una CA di CA privata AWS non vengono conteggiati ai fini di questo totale.	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 ACM certificato	10

Elemento	Quota predefinita
La quota predefinita è di 10 nomi di dominio per ogni ACM certificato. La tua quota potrebbe essere maggiore. 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. È possibile richiedere fino a 100 nomi di dominio. Per richiedere un aumento della quota, crea una richiesta nella console Service Quotas per il ACM servizio. 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 Convalida del dominio. La quota per il numero di nomi di dominio per ACM certificato si applica solo ai certificati forniti daACM. Questa quota non si applica ai certificati in cui si importanoACM. Le seguenti sezioni si applicano solo ai ACM certificati.	

Elemento	Quota predefinita
Numero di privati CAs ACMè integrato con AWS Private Certifica te Authority (CA privata AWS). È possibile utilizzare la ACM console o richiedere certifica ti privati ACM API a un'autorità di certificazione (CA) privata esistente ospitata da CA privata AWS. AWS CLI Questi certificati sono gestiti all'interno dell'ACMambiente e hanno le stesse restrizioni dei certificati pubblici emessi daACM. Per ulteriori informazioni, consulta Richiesta di un certificato privato PKI. È inoltre possibile emettere certificati privati utilizzando il CA privata AWS servizio standalone. Per ulteriori informazioni, consulta Emissione di un certifica to privato. Un CA privato eliminato verrà conteggiato ai fini della quota fino alla fine del periodo di ripristino. Per ulteriori informazioni consulta Eliminazione del CA privato.	200
Numero di certificati privati per CA (durata)	1.000.000

APIquote tariffarie

Le seguenti quote si applicano a ciascuna regione e account. ACM API ACMlimita le API richieste a quote diverse a seconda dell'operazione. API La limitazione significa che ACM rifiuta una richiesta altrimenti valida perché la richiesta supera la quota dell'operazione per il numero di richieste al secondo. Quando una richiesta viene limitata, restituisce un errore. ACM `ThrottlingException` La tabella seguente elenca ogni API operazione e la quota alla quale limita ACM le richieste per tale operazione.

> **Note**
>
> Oltre alle API azioni elencate nella tabella seguente, ACM può anche richiamare l'`IssueCertificate`azione esterna da. CA privata AWS Per informazioni sulle quote up-to-date tariffarie relative a`IssueCertificate`, consulta gli endpoint e le quote per. CA privata AWS

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

APIchiamata	Richieste al secondo
`AddTagsToCertificate`	5
`DeleteCertificate`	10
`DescribeCertificate`	10
`ExportCertificate`	5
`GetAccountConfiguration`	1
`GetCertificate`	10
`ImportCertificate`	1
`ListCertificates`	8
`ListTagsForCertificate`	10
`PutAccountConfiguration`	1
`RemoveTagsFromCertificate`	5
`RenewCertificate`	5
`RequestCertificate`	5
`ResendValidationEmail`	1
`UpdateCertificateOptions`	5

Per ulteriori informazioni, vedere AWS Certificate Manager APIReference.

Prezzi per AWS Certificate Manager

Non sei soggetto a costi aggiuntivi per i TLS certificati SSL /con AWS Certificate Manager cui gestisci la tua attività. Paghi solo per le AWS risorse che crei per far funzionare il tuo sito web o la tua applicazione. Per le informazioni più recenti ACM sui prezzi, 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 maggiori informazioni sui programmi di conformità applicabili AWS Certificate Manager, consulta la sezione AWS Servizi rientranti 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

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. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. 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 AWS servizi.
- 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 AWS servizi 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 dispositivo AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle

autorizzazioni) a utilizzare le risorse. ACM IAMè un dispositivo AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi. ACM

Utente del servizio: se utilizzi il ACM servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più ACM funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità inACM, consultaRisoluzione dei problemi relativi AWS Certificate Manager all'identità e all'accesso.

Amministratore del servizio: se sei responsabile delle ACM risorse della tua azienda, probabilmente hai pieno accesso aACM. È tuo compito determinare a quali ACM funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM conACM, consultaCome AWS Certificate Manager funziona con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accessoACM. Per visualizzare esempi di policy ACM basate sull'identità che puoi utilizzare inIAM, consulta. Esempi di policy basate sull'identità per AWS Certificate Manager

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso 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 l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo 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, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

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 IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

Ruoli IAM

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli 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 informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire

un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. 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 azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 collegata 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. AWS servizi

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

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e 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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM 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 nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta How SCPs work nella AWS Organizations User Guide.
- 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 le politiche di sessione nella Guida IAM per l'utente.

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 determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come AWS Certificate Manager funziona con IAM

Prima di utilizzare IAM per gestire l'accesso aACM, scopri con quali IAM funzionalità è disponibile l'usoACM.

IAMfunzionalità che puoi usare con AWS Certificate Manager

Caratteristica IAM	ACMsupporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
☻Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale del funzionamento ACM e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Policy basate su identità per ACM

Supporta politiche basate sull'identità: Sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. 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 ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate su identità per ACM

Per visualizzare esempi di politiche ACM basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Certificate Manager

Policy basate su risorse all'interno di ACM

Supporta politiche basate sulle risorse: No

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 collegata 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. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad 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 la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Operazioni di policy per ACM

Supporta azioni politiche: Sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Per visualizzare un elenco di ACM azioni, vedere Azioni definite da AWS Certificate Manager nel Service Authorization Reference.

Le azioni politiche in ACM uso utilizzano il seguente prefisso prima dell'azione:

```
acm
```

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

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

Per visualizzare esempi di politiche ACM basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Certificate Manager

Risorse relative alle policy per ACM

Supporta le risorse relative alle politiche: Sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (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 dei tipi di ACM risorse e relativiARNs, consulta Resources defined by AWS Certificate Manager nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, vedere Azioni definite da AWS Certificate Manager.

Per visualizzare esempi di politiche ACM basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Certificate Manager

Chiavi di condizione delle policy per ACM

Supporta le chiavi delle condizioni delle policy specifiche del servizio: Sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. 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 si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. 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, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Per visualizzare un elenco di chiavi di ACM condizione, consulta Condition keys for AWS Certificate Manager nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Certificate Manager.

Per visualizzare esempi di politiche ACM basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Certificate Manager

ACLs in ACM

Supporti: No ACLs

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

ABACcon ACM

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo

passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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 Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con ACM

Supporta credenziali temporanee: Sì

Alcune AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni del principale tra servizi per ACM

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per ACM

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. ACM Modifica i ruoli di servizio solo quando viene ACM fornita una guida in tal senso.

Ruoli collegati ai servizi per l'ACM

Supporta ruoli collegati ai servizi: Sì

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

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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 sull'identità per AWS Certificate Manager

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

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti daACM, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Certificate Manager nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di 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 politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare ACM risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie 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 per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della console di ACM

Per accedere alla AWS Certificate Manager console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle ACM risorse del 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 concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la ACM console, collega anche la policy ACM *AWSCertificateManagerReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

```
{
    "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 seguente politica consente a un utente di elencare tutti i ACM certificati presenti nell'account dell'utente.

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

> **Note**
>
> Questa autorizzazione è necessaria per la visualizzazione ACM dei certificati in Elastic Load Balancing e CloudFront nelle console.

Recupero di un certificato

La seguente politica consente a un utente di recuperare un certificato specifico. 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 seguente politica consente a un utente di eliminare un ACM certificato specifico.

```
{
            "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
AddTagsToCertificate	`acm:AddTagsToCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/`*certificate_ID*
DeleteCertificate	`acm:DeleteCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/`*certificate_ID*
DescribeCertificate	`acm:DescribeCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/`*certificate_ID*
ExportCertificate	`acm:ExportCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/`*certificate_ID*
GetAccountConfiguration	`acm:GetAccountConfiguration`	`*`
GetCertificate	`acm:GetCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/`*certificate_ID*

ImportCertificate	`acm:ImportCertificate`	`arn:aws:acm:`*region*`:`*account*`:certificate/*`
		oppure
		`*`

ListCertificates	`acm:ListCertificates`	`*`

Operazioni dell'API ACM	Autorizzazioni obbligatorie (Operazioni API)	Risorse
ListTagsForCertificate	acm:ListTagsForCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
PutAccountConfiguration	acm:PutAccountConfiguration	*
RemoveTagsFromCertificate	acm:RemoveTagsFromCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
RequestCertificate	acm:RequestCertificate	arn:aws:acm: *region*:*account*:certificate/* oppure *
ResendValidationEmail	acm:ResendValidationEmail	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
UpdateCertificateOptions	acm:UpdateCertificateOptions	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*

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 AWS servizio 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 `GetAccountConfiguration` per la policy AWSCertificateManagerReadOnly.	La policy `AWSCertificateManagerReadOnly` ora include l'autorizzazione per chiamare l'azione dell'API `GetAccountConfiguration` .	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
`acm:ValidationMethod`	RequestCertificate	Stringa (`EMAIL`, `DNS`)	Filtra le richieste in base al metodo di convalida ACM
`acm:DomainNames`	RequestCertificate	ArrayOfString	Filtra in base ai nomi di dominio nella richiesta ACM
`acm:KeyAlgorithm`	RequestCertificate	Stringa	Filtra le richieste in base all'algoritmo della chiave e alle dimensioni ACM
`acm:CertificateTransparencyLogging`	RequestCertificate	Stringa (`ENABLED`, `DISABLED`)	Filtra le richieste in base alle preferenze di registrazione della trasparenza del certificato ACM
`acm:CertificateAuthority`	RequestCertificate	ARN	Filtra le richieste in base alle autorità di certificazione 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 SLR.

> **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 CertificateManagerServiceRolePolicyuse case.
- Utilizzando l'API IAM CreateServiceLinkedRoleo 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

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

Risoluzione dei problemi relativi AWS Certificate Manager all'identità e all'accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con ACM eIAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione in ACM

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'`mateojackson`IAMutente tenta di utilizzare la console per visualizzare i dettagli su una *`my-example-widget`* risorsa fittizia ma non dispone delle autorizzazioni fittizie`acm:`*`GetWidget`*.

```
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`*.

Se hai bisogno di assistenza, 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 il tuo ACM PKI amministratore ha impostato delle regole che impediscono di richiedere il certificato nello stato attuale.

L'errore di esempio seguente si verifica quando un IAM utente tenta di utilizzare la console per richiedere un certificato utilizzando opzioni configurate con a `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 messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo aACM.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel 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 IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione 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`.

Se hai bisogno di assistenza, contatta AWS l'amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie ACM risorse

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se ACM supporta queste funzionalità, consulta. Come AWS Certificate Manager funziona con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM 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 temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse 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	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimen

Quale utente necessita dell'accesso programmatico?	Per	Come
		to agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

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

- Separazione a livello di account
- 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

Separazione a livello di account

Utilizza la separazione a livello di account nelle tue politiche per controllare chi può accedere ai certificati a livello di account. Conserva i certificati di produzione in account separati rispetto ai certificati di test e sviluppo. Se non puoi utilizzare la separazione a livello di account, puoi limitare l'accesso a ruoli specifici negando l'`kms:CreateGrant`intervento nelle tue politiche. Ciò limita i ruoli in un account che possono firmare certificati di alto livello. Per informazioni sulle sovvenzioni, inclusa la terminologia relativa alle sovvenzioni, consulta Grants AWS KMS nella Developer Guide.AWS Key Management Service

Se desideri un controllo più granulare rispetto alla limitazione dell'uso `kms:CreateGrant` per account, puoi limitarti `kms:CreateGrant` a certificati specifici utilizzando kms: condition keys. EncryptionContext Specificate `arn:aws:acm` come chiave e il valore dell'ARN da limitare. La seguente politica di esempio impedisce l'uso di un certificato specifico, ma ne consente altri.

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

AWS CloudFormation

Con AWS CloudFormation puoi creare un modello che descriva le AWS risorse che desideri utilizzare. AWS CloudFormation quindi fornisce 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 ACM i certificati 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, consulta DNSconvalida 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-optionscomando o l'operazione UpdateCertificateOptionsAPI 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-optionscomando. 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 InterfaceÈ 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 in che modo 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) puoi fornire e gestire i TLS certificatiSSL/per i tuoi siti Web e applicazioni AWS basati su di te. Si utilizza ACM per creare o importare e quindi gestire un certificato. È necessario utilizzare altri AWS servizi per distribuire il certificato sul sito Web o sull'applicazione. Per ulteriori informazioni sui servizi integrati conACM, vedereServizi integrati con AWS Certificate Manager. Nelle sezioni seguenti vengono illustrati i passaggi da eseguire prima dell'usoACM.

Argomenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
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.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i AWS servizi nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. 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.

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Attiva l'autenticazione a più fattori (MFA) per il tuo utente root.

   Per istruzioni, consulta Abilitare un MFA dispositivo virtuale per l'utente Account AWS root (console) nella Guida per l'IAMutente.

Crea un utente con accesso amministrativo

1. Abilita IAM Identity Center.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con i valori predefiniti IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

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

  Per informazioni sull'accesso tramite un utente di IAM Identity Center, consulta Accesso al portale di AWS accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Registrare un nome di dominio

Un nome di dominio completo (FQDN) è il nome univoco di un'organizzazione o di un individuo su Internet seguito da un'estensione di dominio di primo livello come .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 chiede se WHOIS la richiesta è disponibile. FQDN 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**
>
> I seguenti passaggi sono necessari solo se utilizzi la convalida e-mail per affermare di possedere o controllare il FQDN (nome di dominio completo) specificato nella richiesta di certificato. ACMrichiede la convalida della proprietà o del controllo prima di emettere un certificato. Puoi utilizzare la convalida o la convalida via e-mail. DNS
> Se sei in grado di modificare la DNS configurazione, ti consigliamo di utilizzare la convalida del DNS dominio anziché la convalida via e-mail. DNSla convalida elimina la necessità di

configurare l'e-mail per il nome di dominio. Per ulteriori informazioni sulla DNS convalida, vedere. DNSconvalida

Convalida del dominio

Per configurare la convalida delle e-mail per il tuo dominio, usa la console o configura DomainValidationOptionnella chiamata a. RequestCertificate ACMinvia messaggi e-mail di convalida al nome di dominio richiesto. Puoi anche specificare un superdominio come dominio di convalida se desideri invece ricevere queste e-mail su quel dominio. Qualsiasi sottodominio fino all'indirizzo minimo del sito Web è valido e viene utilizzato come dominio per l'indirizzo e-mail come suffisso successivo. @ Ad esempio, puoi ricevere un'e-mail all'indirizzo admin@example.com se specifichi example.com come dominio di convalida per subdomain.example.com. In caso di problemi relativi alla convalida e-mail, vedere Risoluzione dei problemi di convalida e-mail.

(CAAFacoltativo) Configura un record

Facoltativamente, puoi configurare un DNS record di autorizzazione dell'autorità di certificazione (CAA) per specificare che AWS Certificate Manager (ACM) è autorizzato a emettere un certificato per il tuo dominio o sottodominio. Dopo aver convalidato il tuo dominio, ACM verifica la presenza di un CAA record per assicurarti che possa emettere un certificato per te. Puoi scegliere di non configurare un CAA record per il tuo dominio se non desideri abilitare il CAA controllo.

Un CAA record contiene i seguenti campi di dati:

flags

Speciifica se il valore del campo tag è supportato daACM. 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 ACM CA specificata nel campo del valore è autorizzata a emettere un certificato per il dominio o il sottodominio.

issuewild

Indica che la ACM CA specificata nel campo del valore è autorizzata a emettere un certificato wildcard per il dominio o il 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 CAA record che specifichi uno dei seguenti quattro AmazonCAs, ACM non puoi emettere un certificato per il tuo 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.

Se è presente un CAA record issuewild che non include un valore ACM CA, non è possibile emettere wild card da. ACM Se non è presente alcun issuewild, ma è presente un CAA record di emissione perACM, le wild card possono essere emesse da. ACM

Example CAAEsempi di record

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

nome di dominio di un server CA nel campo del valore, il CAA record indica che il server specificato è autorizzato a emettere il certificato richiesto. Se si digita un punto e virgola «;» nel campo del valore, il CAA record indica che nessuna CA è autorizzata a emettere un certificato. La configurazione dei CAA record varia in base al 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 DNS i record, rivolgiti al tuo DNS provider. Route 53 supporta i CAA record. Se Route 53 è il tuo DNS provider, consulta CAAFormat per ulteriori informazioni sulla creazione di un record.

Rilascio e gestione dei certificati

ACMi certificati possono essere utilizzati per stabilire comunicazioni sicure su Internet o all'interno di una rete interna. È possibile richiedere un certificato pubblicamente attendibile direttamente da ACM (un "ACMcertificato») o importare un certificato pubblicamente attendibile emesso da una terza parte. Sono supportati anche i certificati autofirmati. Per effettuare il provisioning interno dell'organizzazionePKI, è possibile emettere ACM certificati 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**
>
> ACMI certificati pubblici possono essere installati su EC2 istanze Amazon collegate a una Nitro Enclave, ma non su altre istanze Amazon. EC2 Per informazioni sulla configurazione di un server Web autonomo su un'EC2istanza Amazon non connessa a una Nitro Enclave, consulta Tutorial: Installa un LAMP server Web su Amazon Linux 2 o Tutorial: Installa un server LAMP Web 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 da casa. ACM https://console.aws.amazon.com/acm/ Se viene visualizzata la pagina introduttiva, scegli Get Started (Inizia). Altrimenti, scegli Certificate Manager o Privato CAs nel riquadro di navigazione a sinistra.

Argomenti

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

- Eliminazione dei certificati gestiti da ACM
- Installazione ACM dei certificati

Richiesta di un certificato pubblico

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

ACMI certificati pubblici seguono lo standard X.509 e sono soggetti alle seguenti restrizioni:

- Nomi: è necessario utilizzare nomi di soggetti conformi a DNS -compliant. Per ulteriori informazioni, consulta Nomi di dominio.
- Algoritmo: per la crittografia, l'algoritmo della chiave privata del certificato deve essere a 2048 bitRSA, 256 bit o 384 bit. ECDSA ECDSA
- 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 PKI uso privato CA privata AWS, vediRichiesta di un certificato privato PKI.

> **Note**
>
> Gli amministratori possono utilizzare le politiche a chiave ACM condizionale 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**
>
> A meno che non si scelga di disattivarli, ACM i certificati pubblicamente attendibili vengono registrati automaticamente in almeno due database sulla trasparenza dei certificati. Al momento, non è possibile utilizzare la console per annullare. È necessario utilizzare AWS

CLI o il ACMAPI. 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
- Richiedi un certificato pubblico utilizzando il CLI

Richiedere un certificato pubblico utilizzando la console

Per richiedere un certificato ACM pubblico (console)

1. Accedi alla console di AWS gestione e apri la ACM console da https://console.aws.amazon.com/acm/casa.

   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), ad esempio**`www.example.com`**, oppure un nome di dominio semplice 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 wild-card verrà visualizzato nel campo Oggetto e nell'estensione Subject Alternative Name 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 alla norma RFC5280, 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 nome alternativo del soggetto successivo (SAN) fornito, come nel passaggio successivo, può avere una lunghezza massima di 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 Metodo di convalida, scegli tra convalida consigliata o DNS Convalida via e-mail, a seconda delle tue esigenze.

> **Note**
>
> Se sei in grado di modificare la DNS configurazione, ti consigliamo di utilizzare la convalida del DNS dominio anziché la convalida via e-mail. DNSla convalida offre diversi vantaggi rispetto alla convalida delle e-mail. Per informazioni, consulta DNSconvalida.

Prima di ACM emettere un certificato, verifica che tu possieda o controlli i nomi di dominio nella richiesta di certificato. Puoi utilizzare la convalida o la convalida via e-mail. DNS

Se scegli la convalida e-mail, ACM invia l'e-mail di convalida al dominio specificato nel campo del nome di dominio. Se specifichi un dominio di convalida, ACM invia invece l'e-mail a quel dominio di convalida. Per ulteriori informazioni sulla convalida e-mail, consultare Convalida e-mail.

Se utilizzi la DNS convalida, aggiungi semplicemente un CNAME record fornito da ACM alla tua configurazione. DNS Per ulteriori informazioni sulla DNS convalida, consulta. DNSconvalida

4. Nella sezione Key algorithm (Algoritmo chiave), scegli uno dei tre algoritmi disponibili:

- RSA2048 (impostazione predefinita)
- ECDSAP 256
- ECDSAP 384

Per informazioni su come scegliere un algoritmo, consulta Algoritmi chiave il post AWS sul blog Come valutare e utilizzare ECDSA i certificati 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 ACM tag 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. ACMeffettua ripetuti tentativi di convalida di un certificato per 72 ore e poi scade il timeout. Se un certificato mostra lo stato Non riuscito o Validazione scaduta, elimina la richiesta, correggi il problema con la convalida o la DNSconvalida tramite 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.

Richiedi un certificato pubblico utilizzando il CLI

Utilizzare il comando request-certificate per richiedere un nuovo ACM certificato pubblico sulla riga di comando. I valori opzionali per il metodo di convalida sono e. DNS EMAIL I valori opzionali per l'algoritmo chiave sono RSA _2048 (l'impostazione predefinita se il parametro non viene fornito in modo esplicito), EC_Prime256v1 e EC_SECP384R1.

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

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

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

Richiesta di un certificato privato PKI

Se hai accesso a una CA privata esistente creata da CA privata AWS, ACM puoi richiedere un certificato adatto all'uso in ambito privatoPKI. 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.

I certificati firmati da una CA privata non sono considerati attendibili per impostazione predefinita e ACM non supportano alcuna forma di convalida. Di conseguenza, un amministratore deve intervenire per installarli negli archivi attendibili dei clienti dell'organizzazione.

ACMI certificati privati seguono lo standard X.509 e sono soggetti alle seguenti restrizioni:

- Nomi: è necessario utilizzare nomi di soggetti conformi a DNS -compliant. Per ulteriori informazioni, consulta Nomi di dominio.
- Algoritmo: per la crittografia, l'algoritmo della chiave privata del certificato deve essere a 2048 bitRSA, 256 bit o 384 bit. ECDSA ECDSA

> **Note**
>
> La famiglia di algoritmi di firma specificata (RSAoECDSA) 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

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

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

  Per abilitare l'emissione e il rinnovo di un account singolo, l' CA privata AWS amministratore deve concedere l'autorizzazione al responsabile del ACM servizio per creare, recuperare ed elencare i certificati. Questa operazione viene eseguita utilizzando l' CA privata AWS APIazione CreatePermissiono il comando create-permission. AWS CLI Il proprietario dell'account assegna queste autorizzazioni a un IAM utente, gruppo o ruolo responsabile dell'emissione dei certificati.
- Più account: la CA firmataria e il ACM certificato 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 politica basata sulle risorse utilizzando l'azione o il comando put-policy. CA privata AWS API PutPolicyAWS CLI La policy specifica le entità principali degli altri account a cui è consentito l'accesso limitato alla CA. Per ulteriori informazioni, vedere Using a Resource Based Policy with Private CA. ACM

  Lo scenario tra account diversi richiede inoltre ACM la configurazione di un ruolo collegato al servizio (SLR) per interagire come principale con la policy. PCA ACMlo crea SLR automaticamente durante l'emissione del primo certificato.

  ACMpotrebbe avvisarti che non è in grado di determinare se SLR esiste un account. Se l'`iam:GetRole`autorizzazione richiesta è già stata concessa al ACM SLR tuo account, l'avviso non

si ripeterà dopo la SLR creazione. Se l'errore si ripresenta, tu o l'amministratore del tuo account potreste dover concedere l'`iam:GetRole`autorizzazione o associare il vostro account alla ACM politica gestitaACM. `AWSCertificateManagerFullAccess`

Per ulteriori informazioni, vedere Using a Service Linked Role with. ACM

> **Important**
>
> Il ACM certificato deve essere associato attivamente a un AWS servizio supportato prima di poter essere rinnovato automaticamente. Per informazioni sulle risorse ACM supportate, consultaServizi integrati con AWS Certificate Manager.

Richiedi un PKI certificato privato utilizzando la ACM console

1. Accedi alla console AWS di gestione e apri la ACM console da https://console.aws.amazon.com/acm/casa.

   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 Dettagli dell'autorità di certificazione, fai clic sul menu Autorità di certificazione e scegli una delle opzioni private disponibiliCAs. Se la CA è condivisa da un altro account, ARN è preceduta dalle 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), ad esempio**`www.example.com`**, oppure un nome di dominio semplice 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 wild-card verrà visualizzato nel campo Oggetto e nell'estensione Subject Alternative Name 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:

   - RSA2048 (impostazione predefinita)
   - ECDSAP 256
   - ECDSAP 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 ACM tag 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 PKI certificati privati firmati con la CA selezionata. Per ulteriori informazioni, vedere Utilizzo di un ruolo collegato al servizio 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.

Richiedi un PKI certificato privato utilizzando il CLI

Usa il comando request-certificate per richiedere un certificato privato in. ACM

> **Note**
>
> Quando richiedi un PKI certificato privato firmato da una CA da AWS Private CA, la famiglia di algoritmi di firma specificata (RSAoECDSA) 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 genera l'Amazon Resource Name (ARN) del tuo nuovo certificato privato.

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

Nella maggior parte dei casi, associa ACM automaticamente un ruolo collegato al servizio (SLR) al tuo account la prima volta che utilizzi una CA condivisa. SLRAbilita il rinnovo automatico dei certificati

di entità finale emessi dall'utente. Per verificare se SLR è presente, puoi eseguire una query IAM con il seguente comando:

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

Se 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 SLR manca, vedere Using a Service Linked Role with ACM.

Convalida della proprietà del dominio

Prima che l'autorità di certificazione Amazon (CA) possa emettere un certificato per il tuo sito, AWS Certificate Manager (ACM) deve dimostrare che possiedi o controlli tutti i nomi di dominio specificati

nella richiesta. Puoi scegliere di dimostrare la tua proprietà con la convalida del Domain Name System (DNS) o tramite e-mail nel momento in cui richiedi un certificato.

> **Note**
>
> La convalida si applica solo ai certificati pubblicamente affidabili emessi da. ACM ACMnon convalida la proprietà del dominio per i certificati importati o per i certificati firmati da una CA privata. ACMnon può convalidare le risorse in una zona ospitata VPC privata di Amazon o in qualsiasi altro dominio privato. Per ulteriori informazioni, consulta Risoluzione dei problemi di convalida dei certificati.

In generale, consigliamo di utilizzare la DNS convalida rispetto alla convalida via e-mail per i seguenti motivi:

- Se utilizzi Amazon Route 53 per gestire i tuoi DNS record pubblici, puoi aggiornarli ACM direttamente.
- ACMrinnova automaticamente i certificati DNS convalidati per tutto il tempo in cui un certificato rimane in uso e il DNS record rimane valido.
- Per essere rinnovati, i certificati convalidati tramite e-mail richiedono un'azione da parte del proprietario del dominio. ACMinizia a inviare avvisi di rinnovo 45 giorni prima della scadenza. Questi avvisi vengono inviati agli indirizzi delle WHOIS cassette postali del dominio e a un massimo di cinque indirizzi amministrativi 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 emette un certificato rinnovato con gli stessi. ARN

Se non sei autorizzato a modificare il DNS database del tuo dominio, devi invece utilizzare la convalida via e-mail.

> **Note**
>
> Dopo aver creato un certificato con convalida via e-mail, non puoi passare alla convalida con. DNS Per utilizzare DNS la convalida, elimina il certificato e creane uno nuovo che utilizzi la convalida. DNS

Argomenti

DNSconvalida

Il Domain Name System (DNS) è un servizio di directory per risorse connesse a una rete. Il DNS provider gestisce un database contenente i record che definiscono il dominio. Quando scegli DNS la convalida, ti ACM fornisce uno o più CNAME record che devono essere aggiunti a questo 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 via e-mail, non è possibile passare alla convalida con. DNS Per utilizzare DNS la convalida, elimina il certificato e creane uno nuovo che utilizzi la convalida. DNS

Ad esempio, se richiedi un certificato per il `example.com` dominio con `www.example.com` un nome aggiuntivo, ACM crea due CNAME record per te. 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 ACM utilizzato per rinnovare automaticamente il certificato. I CNAME record devono essere aggiunti al DNS database una sola volta. ACMrinnova automaticamente il certificato fintanto che il certificato è in uso e il CNAME record rimane valido.

> **Important**
>
> Se non utilizzi Amazon Route 53 per gestire i tuoi DNS record pubblici, contatta il tuo DNS provider per scoprire come aggiungere record. Se non hai l'autorità per modificare il DNS database del tuo dominio, devi invece utilizzare la convalida delle e-mail.

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

È possibile interrompere il rinnovo automatico rimuovendo il certificato dal AWS servizio a cui è associato o eliminando il record. CNAME Se Route 53 non è il tuo DNS provider, contatta il tuo provider per scoprire come eliminare un record. 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 ACM i certificati.

> **Note**
>
> CNAMEla risoluzione fallirà se nella DNS configurazione ne CNAMEs sono concatenati più di cinque. Se hai bisogno di un concatenamento più lungo, ti consigliamo di usare convalidaonvalida e-mail.

Come funzionano CNAME i record ACM

> **Note**
>
> Questa sezione è dedicata ai clienti che non utilizzano Route 53 come DNS provider.

Se non utilizzi Route 53 come DNS provider, devi inserire manualmente i CNAME record forniti da ACM nel database del provider, di solito tramite un sito Web. CNAMEi record vengono utilizzati per diversi scopi, tra cui come meccanismi di reindirizzamento e come contenitori per metadati specifici del fornitore. Questi recordACM, infatti, consentono la convalida iniziale della proprietà del dominio e il rinnovo automatico continuo dei certificati.

La tabella seguente mostra alcuni CNAME record di esempio per sei nomi di 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. Ciò illustra che per un dominio wild-card, ad esempio`*.example.com`, le stringhe create da ACM sono le stesse create per il relativo dominio di base,. `example.com` In caso contrario, la coppia Nome registro e Valore registro differiscono per ciascun nome di dominio.

Record di esempio CNAME

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

Il *xN* i valori che seguono il carattere di sottolineatura (_) sono stringhe lunghe 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 DNS record.

> **Note**
>
> Se il tuo DNS provider non supporta CNAME i valori con un carattere di sottolineatura iniziale, consulta Risoluzione dei problemi DNS di convalida.

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

Nome dominio	Nome registro	Tipo di registro	Valore registro
esempio.om	_a79865eb4cd1a6ab990a45779b4e0b96.example.com.	CNAME	_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.

Il nome di dominio è quello 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 (Domain Name, Record Name e Record Value) devono essere inseriti nei campi appropriati dell'interfaccia web del DNS provider per aggiungere DNS record. 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.

Impostazione della convalida DNS

Questa sezione descrive come configurare un certificato pubblico per utilizzare la DNS convalida.

Per configurare la DNS convalida 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 DNS provider.
      - Hai l'autorizzazione per scrivere nella zona ospitata da Route 53.
      - Il tuo non FQDN è già stato convalidato.

      > **Note**
      >
      > Se usi Route 53 ma il pulsante Crea registri in Route 53 manca o è disattivato, consulta ACMLa console 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 di stato del certificato dovrebbe aprirsi con un banner di stato che riporta i DNSrecord 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 la creazione ACM automatica del record in Route 53. Tuttavia, è possibile effettuare una API chiamata AWS CLI o a Route 53 per creare il record nel database Route 53DNS. Per ulteriori informazioni sui set di registri di Route 53, consulta Lavorare con set di registri della risorsa.

b. (Facoltativo) Se non si utilizza Route 53 come DNS provider, è necessario recuperare le CNAME informazioni e aggiungerle al DNS database. Nella pagina dei dettagli del nuovo certificato, è possibile farlo in due modi:

- Copia i CNAME componenti visualizzati nella sezione Domini. Queste informazioni devono essere aggiunte manualmente al DNS database.
- In alternativa, scegli Esporta in CSV. Le informazioni nel file risultante devono essere aggiunte manualmente al DNS database.

> **Important**
>
> Per evitare problemi di convalida, Come funzionano CNAME i record ACM consulta prima di aggiungere informazioni al database del DNS provider. Se riscontri problemi, consulta Risolvi i problemi DNS di convalida.

Se non ACM è in grado di convalidare il nome di dominio entro 72 ore dal momento in cui genera un CNAME valore per te, ACM modifica lo stato del certificato in Validazione scaduta. La ragione più probabile di questo risultato è che non hai aggiornato correttamente la DNS configurazione con il valore generato. ACM Per risolvere questo problema, è necessario richiedere un nuovo certificato dopo aver esaminato le CNAME istruzioni.

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. Puoi eseguire la verifica tramite e-mail oDNS. Questo argomento tratta la convalida tramite e-mail.

In caso di problemi con la convalida dell'email, consulta Risoluzione dei problemi di convalida e-mail.

Come funziona la convalida delle e-mail

ACMinvia messaggi e-mail di convalida ai seguenti cinque messaggi di posta elettronica di sistema comuni per ogni dominio. In alternativa, puoi specificare un superdominio come dominio di convalida se desideri ricevere invece queste e-mail in quel dominio. Qualsiasi sottodominio fino all'indirizzo minimo del sito Web è valido e viene utilizzato come dominio per l'indirizzo e-mail come suffisso successivo. @ Ad esempio, puoi ricevere un'e-mail all'indirizzo admin@example.com se specifichi example.com come dominio di convalida per subdomain.example.com.

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

Per dimostrare di essere il proprietario del dominio, devi selezionare il link di convalida incluso in queste e-mail. ACMinvia inoltre e-mail di convalida a questi stessi indirizzi per rinnovare il certificato quando il certificato è a 45 giorni dalla scadenza.

La convalida e-mail per le richieste di certificati multidominio che utilizzano ACM API or CLI comporta l'invio di un messaggio e-mail da parte di ciascun dominio richiesto, anche se la richiesta include sottodomini di altri domini nella richiesta. Il proprietario del dominio deve convalidare un messaggio e-mail per ciascuno di questi domini prima di poter emettere il certificato. ACM

Eccezione a questo processo

Se richiedi un ACM certificato per un nome di dominio che inizia con **www** o con un asterisco wild-card (*****), ACM rimuove l'iniziale **www** o l'asterisco e invia 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 ACM certificato per www.example.com, l'e-mail viene inviata a admin@example.com anziché a admin@www.example.com. Allo stesso modo, se richiedi un ACM certificato per *.test.example.com, l'e-mail viene inviata a admin@test.example.com. Gli altri indirizzi amministrativi comuni vengono formati in modo analogo.

> **Important**
>
> A partire da giugno 2024, ACM non supporta più la nuova convalida delle e-mail tramite gli indirizzi di contatto. WHOIS Per i certificati esistenti, a partire da ottobre 2024, ACM non invieremo avvisi di rinnovo agli indirizzi di contatto del dominio. WHOIS ACMcontinuerà a inviare e-mail di convalida ai cinque indirizzi di sistema comuni per il dominio richiesto. Per ulteriori dettagli, consulta AWS Certificate Manager Interromperà la WHOIS ricerca di certificati convalidati tramite e-mail

Considerazioni

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 affidabili emessi da. ACM ACMnon convalida la proprietà del dominio per i certificati importati o per i certificati firmati da una CA privata. ACMnon può convalidare le risorse in una zona ospitata VPC privata di Amazon o in 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 puoi passare alla convalida con. DNS Per utilizzare DNS la convalida, elimina il certificato e creane uno nuovo che utilizzi la convalida. DNS

Scadenza e rinnovo dei certificati

ACMi certificati sono validi per 13 mesi (395 giorni). Il rinnovo di un certificato richiede l'intervento del proprietario del dominio. ACMinizia a inviare avvisi di rinnovo agli indirizzi e-mail associati al dominio 45 giorni prima della scadenza. Le notifiche contengono un link su cui il proprietario del dominio può fare clic per il rinnovo. Una volta convalidati tutti i domini elencati, ACM emette un certificato rinnovato con gli stessi. ARN

(Facoltativo) Invia nuovamente l'email 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 informazioni su come inviare nuovamente un'e-mail di convalida, consulta Rinvio dell'e-mail di convalida

Per problemi persistenti con la convalida tramite e-mail, consulta la sezione Risoluzione dei problemi di convalida e-mail in Risoluzione dei problemi.

Elenco dei certificati gestiti da ACM

È possibile utilizzare la ACM console o AWS CLI elencare i certificati gestiti daACM. La console può elencare fino a 500 certificati in una pagina e 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 di 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 ACM certificato è associato attivamente a un AWS servizio come Elastic Load Balancing o. CloudFront Il valore può essere No o Sì.
- Idoneità al rinnovo: se il certificato può essere rinnovato automaticamente ACM quando si avvicina la scadenza. I valori possibili sono: Idoneo | Non idoneo. Per le regole di idoneità, consulta Rinnovo gestito per ACM i certificati.

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: l'ora in cui è stato richiesto il certificato. ACM
- 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, utilizzare il AWS CLI

Utilizzate il comando list-certificates per elencare i vostri certificati ACM -managed, come mostrato 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 keyTypesRSA_1024o 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 usare la ACM console o il AWS CLI per elencare i metadati dettagliati sui tuoi certificati.

Per visualizzare i dettagli del certificato nella console

1. Apri la ACM console all'indirizzo https://console.aws.amazon.com/acm/per visualizzare i tuoi certificati. 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 ACM certificato. I valori possibili sono:Rilasciato da Amazon|Privato|Importato. Per ulteriori informazioni, consulta Richiesta di un certificato pubblico, Richiesta di un certificato privato PKI 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
     - 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 unservizio integrato AWS I valori possibili sono: Sì | No
     - Nome di dominio: il primo nome di dominio completo (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 ACM integrati 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 ACM i certificati.
- 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: la ARN 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 privato PKI o è autofirmato e non necessita di convalida.

Per visualizzare i dettagli del certificato, 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/E12KXPQHVLSYVC"
        ],
        "SignatureAlgorithm": "SHA256WITHRSA",
        "CreatedAt": 1450212224.0,
        "IssuedAt": 1450212292.0,
        "KeyUsages": [
            {
                "Name": "DIGITAL_SIGNATURE"
            },
            {
                "Name": "KEY_ENCIPHERMENT"
            }
        ],
        "Serial": "07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b",
        "Issuer": "Amazon",
        "Type": "AMAZON_ISSUED",
        "ExtendedKeyUsages": [
            {
                "OID": "1.3.6.1.5.5.7.3.1",
                "Name": "TLS_WEB_SERVER_AUTHENTICATION"
            },
```

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

Eliminazione dei certificati gestiti da ACM

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

> **Important**
>
> - Non è possibile eliminare un ACM certificato utilizzato da un altro AWS servizio. Per eliminare un certificato in uso, è necessario prima rimuovere l'associazione del certificato. Questa operazione viene eseguita utilizzando la console o 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 relativa a un ACM certificato, quindi scegli 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 ACM dei certificati

Non è possibile ACM installare un certificato pubblico direttamente sul sito Web o sull'applicazione AWS basata. È necessario utilizzare uno dei servizi integrati conACM. Per ulteriori informazioni, consulta Servizi integrati con AWS Certificate Manager.

ACMi certificati firmati da una CA CA privata AWS e destinati a uso privato PKI possono essere esportati e installati manualmente su qualsiasi sistema a cui si dispone di accesso amministrativo. Questi certificati non sono attendibili su Internet pubblico.

Rinnovo gestito per ACM i certificati

ACMfornisce il rinnovo gestito per i certificatiSSL/TLSemessi da Amazon. Ciò significa che ACM rinnoverà automaticamente i tuoi certificati (se utilizzi la DNS convalida) oppure ti invierà notifiche via e-mail quando la scadenza si avvicina. Questi servizi sono forniti sia per certificati pubblici che privati. ACM

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

- ELIGIBLEse associato a un altro AWS servizio, come Elastic Load Balancing o. CloudFront
- ELIGIBLEse esportato dopo l'emissione o l'ultimo rinnovo.
- ELIGIBLEse si tratta di un certificato privato rilasciato chiamando ACM RequestCertificateAPIe poi esportato o associato a un altro AWS servizio.
- ELIGIBLEse si tratta di un certificato privato emesso tramite la console di gestione e quindi esportato o associato a un altro AWS servizio.
- NOTELIGIBLEse si tratta di un certificato privato emesso chiamando il CA privata AWS IssueCertificateAPI.
- NOTELIGIBLEse importato.
- NOTELIGIBLEse 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	Conse o	Nota
esempio.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"

Nome dominio	Soddisfa #1	Soddisfa #2	Conse o	Nota
a--esempi o.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"
abc—esemp io.com	N/A	n/a	✓	Non inizia con "<character><chara cter>--"
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 si ACM rinnova un certificato, l'Amazon Resource Name (ARN) del certificato rimane lo stesso. 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 modalità privata PKI
- 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 DNSconvalida o convalida via e-mail. Quando un certificato 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 da DNS

Il rinnovo gestito è completamente automatizzato per ACM i certificati originariamente emessi tramite la convalida. DNS

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

- Il certificato è attualmente utilizzato da un AWS servizio.
- Tutti i DNS CNAME record ACM forniti obbligatoriamente (uno per ogni nome alternativo del soggetto univoco) sono presenti e accessibili in modalità pubblicaDNS.

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

ACMinvia AWS Health eventi ed EventBridge eventi Amazon quando non è in grado di convalidare automaticamente un dominio durante il rinnovo (ad esempio, a causa della presenza di CAA record). 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

ACMi certificati sono validi per 13 mesi (395 giorni). Il rinnovo di un certificato richiede l'intervento del proprietario del dominio. ACMinizia a inviare avvisi di rinnovo agli indirizzi e-mail associati al dominio 45 giorni prima della scadenza. Le notifiche contengono un link su cui il proprietario del dominio può fare clic per il rinnovo. Una volta convalidati tutti i domini elencati, ACM emette un certificato rinnovato con gli stessi. 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 .

Rinvio dell'e-mail di convalida

Dopo aver configurato la convalida dell'e-mail per il tuo dominio quando richiedi un certificato (vedi(Facoltativo) Configurazione dell'e-mail per il dominio in uso), puoi utilizzare il comando AWS

Certificate Manager API per richiedere che ti ACM invii un'email di convalida del dominio per il rinnovo del certificato. Devi seguire questa procedura nei seguenti casi:

- Hai utilizzato la convalida via 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 riesci a trovare il messaggio e-mail originale di convalida del dominio ACM inviato per il rinnovo del certificato.

Per inviare e-mail di convalida a un dominio diverso da quello originariamente configurato nella richiesta di certificato, puoi utilizzare l'ResendValidationEmailoperazione in ACM API AWS CLI, o. AWS SDKs ACMinvierà e-mail al dominio di convalida specificato. Puoi accedervi AWS CLI nel browser utilizzando AWS CloudShell nelle regioni supportate.

Per richiederlo, ACM invia nuovamente il messaggio e-mail di convalida del dominio (console)

1. Apri la AWS Certificate Manager console a casahttps://console.aws.amazon.com/acm/.
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 richiederlo invia ACM nuovamente l'email di convalida del dominio () ACM API

Usa l'ResendValidationEmailoperazione in. ACM API A tal fine, fornisci il ARN certificato, il dominio che richiede la convalida manuale e il dominio in cui desideri ricevere le e-mail di convalida del dominio. 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 modalità privata PKI

ACMi certificati firmati da una CA privata di CA privata AWS sono idonei per il rinnovo gestito. A differenza dei ACM certificati pubblicamente attendibili, un certificato privato non PKI 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 ACM console o l'RequestCertificateazione di ACM API sono idonei per il rinnovo gestito. I certificati emessi direttamente CA privata AWS utilizzando l'IssueCertificateazione di non CA privata AWS API sono gestiti daACM.

Quando mancano 60 giorni alla scadenza di un certificato gestito, tenta ACM 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'RenewCertificateazione di. ACM API 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 ACM integrato, il nuovo certificato sostituisce quello precedente senza ulteriori interventi da parte del cliente.
- Se il certificato non è associato a un servizio ACM integrato, è necessario l'intervento del cliente per esportare e installare il certificato rinnovato. Puoi eseguire queste azioni manualmente o con l'assistenza AWS Healthdi Amazon EventBridge e AWS Lambdacome 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 PKI certificati privati al momento del ACM rinnovo. Questo esempio esporta solo un certificato e la relativa chiave privata daACM; dopo l'esportazione, il certificato deve ancora essere installato sul dispositivo di destinazione.

Per automatizzare l'esportazione dei certificati utilizzando la console

1. Seguendo le procedure della AWS Lambda Developer Guide, crea e configura una funzione Lambda che chiama export. ACM API

   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 in uso per recuperare il certificato e la chiave privata rinnovati richiamando l'ExportCertificateazione di. ACM API

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

2. Crea una regola in Amazon per EventBridge ascoltare gli eventi ACM sanitari e richiama la funzione Lambda quando ne rileva uno. ACMscrive 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, rinnovo gestito dei certificati privatiPKI.

Puoi utilizzare ACM API o AWS CLI per testare manualmente la configurazione del flusso di lavoro di rinnovo ACM gestito. In questo modo, puoi confermare che i tuoi certificati verranno rinnovati automaticamente ACM prima della scadenza.

> **Note**
>
> Puoi testare solo il rinnovo dei certificati emessi ed esportati da CA privata AWS.

Quando si utilizzano API le azioni o CLI i comandi 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 in output. API Se il certificato è associato a un servizio ACM integrato, il nuovo certificato viene distribuito e viene generato un evento di rinnovo in Amazon CloudWatch Events. Se il rinnovo fallisce, ACM restituisce un errore e suggerisce azioni correttive. (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 certificatiACM, devi prima concedere al ACM servizio le autorizzazioni principali per farlo. Per ulteriori informazioni, vedere Assegnazione delle autorizzazioni di rinnovo dei certificati a. ACM

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 del certificato () ACM API

- Invia una RenewCertificaterichiesta, specificando il ARN certificato privato da rinnovare. Quindi utilizza l'DescribeCertificateoperazione 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 con le informazioni sullo stato del rinnovo nei dettagli del certificato. È possibile utilizzare la AWS Certificate Manager console, il ACM API AWS CLI, o il AWS Health Dashboard per verificare lo stato di rinnovo di un ACM certificato. Se utilizzi la console, oppure AWS CLI ACMAPI, 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

ACMsta tentando di convalidare automaticamente i nomi di dominio nel certificato. Per ulteriori informazioni, consulta Rinnovo per domini convalidati da DNS. Non è richiesta alcuna operazione aggiuntiva.

Convalida in attesa

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

Riuscito

Tutti i nomi di dominio nel certificato vengono convalidati e il certificato viene ACM rinnovato. Non è richiesta alcuna operazione aggiuntiva.

Non riuscito

Uno o più nomi di dominio non sono stati convalidati prima della scadenza del certificato e ACM non hanno 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)

La procedura seguente illustra come utilizzare la ACM console per verificare lo stato di rinnovo di un certificato. ACM

1. Apri la AWS Certificate Manager console a https://console.aws.amazon.com/acm/casa.
2. Espandere un certificato per visualizzare i dettagli.
3. Trova lo Stato di rinnovo nella sezione Dettagli. Se non vedi lo stato, significa che ACM non è stato avviato il processo di rinnovo gestito per questo certificato.

Controlla lo stato (API)

Per un esempio in Java che mostra come utilizzare l'DescribeCertificateazione per controllare lo stato, vedeteDescrizione di un certificato.

Controlla lo stato (CLI)

L'esempio seguente mostra come verificare lo stato del rinnovo del ACM certificato 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 vedi il `RenewalStatus` campo, significa che non ACM ha avviato il processo di rinnovo gestito per il tuo certificato.

Controlla lo stato utilizzando Personal Health Dashboard (PHD)

ACMtenta di rinnovare automaticamente il ACM certificato 60 giorni prima della scadenza. Se ACM non riesce a 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**
>
> ACMscrive avvisi di rinnovo successivi relativi a un singolo evento nella PHD cronologia. Ogni avviso sovrascrive quello precedente fino a quando il rinnovo non ha esito positivo.

Per utilizzare AWS Health Dashboard:

1. Accedi a AWS Health Dashboard at 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

ACMI certificati convalidati tramite posta elettronica richiedono in genere un'azione 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.

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
and follow the instructions on the page.

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

Sincerely,
Amazon Web Services

--
```

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

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

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

Una volta ricevuto un nuovo messaggio di convalida da AWS, ti consigliamo di utilizzarlo come modello più autorevole per il tuo up-to-date 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 lineette o trattini.
- `Certificate Identifier`Ora presenta l'intero certificato ARN anziché un formato abbreviato, ad esempio, anziché. *`arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369`* *`3b4d78e1-0882-4f51-954a-298ee44ff369`*
- L'approvazione del certificato URL ora contiene `acm-certificates.amazon.com` invece di. `certificates.amazon.com`
- Il modulo di approvazione aperto facendo clic sull'approvazione del certificato URL ora contiene 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 ACM console elabora una richiesta di certificato multidominio, invia messaggi e-mail di convalida al nome di dominio o al dominio di convalida specificato quando richiedi un certificato pubblico. Il proprietario del dominio deve convalidare un messaggio e-mail per ogni dominio prima

di ACM poter emettere il certificato. Per ulteriori informazioni, consulta Utilizzo delle e-mail per convalidare la proprietà del dominio.

- La convalida e-mail per le richieste di certificati multidominio che utilizzano ACM API o CLI comporta l'invio di un messaggio e-mail da parte di ciascun dominio richiesto, anche se la richiesta include sottodomini di altri domini nella richiesta. Il proprietario del dominio deve convalidare un messaggio e-mail per ciascuno di questi domini prima di poter emettere il certificato. ACM

  Se invii nuovamente le e-mail per un certificato esistente tramite la ACM console, le e-mail verranno inviate al dominio di convalida specificato nella richiesta di certificato originale o al dominio esatto se non è stato specificato alcun dominio di convalida. Per ricevere e-mail di convalida su un dominio diverso, puoi richiedere un nuovo certificato, specificando il dominio di convalida che desideri utilizzare per la convalida. In alternativa, puoi chiamare ResendValidationEmailcon il `ValidationDomain` parametro utilizzando, o. API SDK CLI Tuttavia, il dominio di convalida specificato nella `ResendValidationEmail` richiesta viene utilizzato solo per quella chiamata e non viene salvato nel certificato Amazon Resource Name (ARN) per future e-mail di convalida. Devi chiamare `ResendValidationEmail` ogni volta che desideri ricevere un'e-mail di convalida su un nome di dominio non specificato nella richiesta originale del certificato.

  > **Note**
  >
  > Prima di novembre 2020, i clienti dovevano convalidare solo il dominio apex ed ACM emettevano 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'opzione ACM API orCLI, puoi forzare l'invio al dominio apex di tutti i messaggi e-mail di convalida per una richiesta di certificato multidominio. InAPI, utilizzate il `DomainValidationOptions` parametro dell'RequestCertificateazione per specificare un valore per`ValidationDomain`, che è un membro del tipo. DomainValidationOption NelCLI, utilizzate il --domain-validation-options parametro del comando request-certificate per specificare un valore per. `ValidationDomain`

Importazione di certificati in AWS Certificate Manager

Oltre a richiedere i TLS certificatiSSL/forniti da AWS Certificate Manager (ACM), puoi importare certificati ottenuti al di fuori di. AWS Potresti farlo perché disponi già di un certificato rilasciato da un'autorità di certificazione (CA) di terze parti o perché hai requisiti specifici dell'applicazione che non sono soddisfatti dai certificati emessi. ACM

È possibile utilizzare un certificato importato con qualsiasi AWS servizio integrato con. ACM I certificati importati funzionano allo stesso modo di quelli forniti daACM, con un'importante eccezione: ACM non prevede il rinnovo gestito per i certificati importati.

Per rinnovare un certificato importato, puoi ottenere un nuovo certificato dall'emittente del certificato e reimportarlo manualmente in. ACM Questa azione preserva l'associazione del certificato e il relativo nome Amazon Resource (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 presenti ACM sono risorse regionali, inclusi i certificati che importi. 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 informazioni su come importare i certificati inACM, consulta i seguenti argomenti. Se si verificano problemi durante l'importazione di un certificato, vedere Problemi di importazione dei certificazione.

Argomenti

- Reimportazione di un certificato

Prerequisiti per l'importazione di certificazione

Per importare un TLS certificatoSSL/autofirmato inACM, è necessario fornire sia il certificato che la relativa 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. ACMsupporta i seguenti algoritmi (APInome tra parentesi):

- RSA1024 bit () `RSA_1024`
- RSA2048 bit () `RSA_2048`
- RSA3072 bit () `RSA_3072`
- RSA4096 bit () `RSA_4096`
- ECDSA256 bit () `EC_prime256v1`
- ECDSA384 bit () `EC_secp384r1`
- ECDSA521 bit () `EC_secp521r1`

Si noti anche i seguenti requisiti aggiuntivi:

- ACMi servizi integrati consentono di associare alle risorse solo gli algoritmi e le dimensioni delle chiavi che supportano. Ad esempio, supporta CloudFront solo chiavi a 1024 bitRSA, 2048 bitRSA, 3072 bit ed Elliptic Prime Curve a 256 bitRSA, mentre Application Load Balancer supporta tutti gli algoritmi disponibili da. ACM Per ulteriori informazioni, consulta la documentazione relativa al servizio che usi.
- Un SSL certificato deve TLS essere un certificato/X.509 versione 3. Deve contenere una chiave pubblica, il nome di dominio completo (FQDN) o l'indirizzo IP del sito Web e 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 PEM codificata.

- 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, chiave privata e catena di certificati) devono essere PEM codificati. Il caricamento di materiali DER codificati 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

ACMrichiede di importare separatamente il certificato, la catena di certificati e la chiave privata (se presente) e di codificare ogni componente nel PEM formato. PEMsta per Privacy Enhanced Mail. Il PEM formato viene spesso utilizzato per rappresentare certificati, richieste di certificati, catene di certificati e chiavi. L'estensione tipica per un file in PEM formato —è`.pem`, ma non è necessario che lo sia.

> **Note**
>
> AWS non fornisce utilità per la manipolazione di PEM file 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), sono facilmente disponibili strumenti gratuiti e open source come Open. SSL

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. Tieni presente che se modifichi uno qualsiasi dei caratteri di un PEM file in modo errato o se aggiungi uno o più spazi alla fine di una riga, il certificato, la catena di certificati o la chiave privata non saranno validi.

Example 1. PEM—certificato codificato

```
-----BEGIN CERTIFICATE-----
```

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

Example 2. PEM—catena di certificati codificati

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. PEM—chiavi private codificate

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. L'esempio seguente mostra una chiave RSA privata.

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

L'esempio successivo mostra una chiave privata con PEM curva ellittica con codifica. A seconda di come viene creata la chiave, il blocco dei parametri potrebbe non essere incluso. Se il blocco di parametri è incluso, lo ACM 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) ACM utilizzando il AWS Management Console AWS CLI, il o il. ACM API Negli argomenti seguenti viene illustrato come utilizzare AWS Management Console e il. AWS CLI Le procedure per ottenere un certificato da un ente non AWS 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 ACM console a https://console.aws.amazon.com/acm/casa. Se è la prima volta che lo usiACM, cerca l'AWS Certificate Managerintestazione e scegli il pulsante Inizia sotto di essa.
2. Seleziona Import a certificate (Importa un certificato).

3. Esegui questa operazione:

   a. Per Certificate body, incolla il certificato PEM -encoded da importare. Dovrebbe iniziare con `-----BEGIN CERTIFICATE-----` e terminare con `-----END CERTIFICATE-----`.

   b. Per la chiave privata del certificato, incolla la chiave privata non PEM crittografata con codifica del certificato. Dovrebbe iniziare con `-----BEGIN PRIVATE KEY-----` e terminare con `-----END PRIVATE KEY-----`.

   c. (Facoltativo) Per Certificate chain, incolla la catena di certificati PEM -encoded.

4. (Facoltativo) Per aggiungere tag al certificato importato, scegli Tag. Un tag è un'etichetta che assegni a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. Puoi utilizzare i tag per organizzare le tue risorse o tenere traccia AWS dei costi.

5. 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 PEM con codifica è archiviato in un file denominato. `Certificate.pem`
- La catena di certificati PEM -encoded è memorizzata in un file denominato. `CertificateChain.pem`
- La chiave privata non PEM crittografata con codifica è memorizzata 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 `import-certificate` comando ha esito positivo, 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 conACM, vedere. 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)

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

1. Apri la ACM console a https://console.aws.amazon.com/acm/casa.
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, incolla il certificato di PEM entità finale con codifica.
5. Per la chiave privata del certificato, incolla la chiave privata non PEM crittografata con codifica associata alla chiave pubblica del certificato.

6. (Facoltativo) Per Certificate chain, incolla la catena di certificati PEM -encoded. 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. 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 PEM -encoded è memorizzato in un file denominato. `Certificate.pem`
- La catena di certificati PEM -encoded è memorizzata in un file denominato. `CertificateChain.pem`
- (Solo certificati privati) La chiave privata non PEM crittografata con codifica è memorizzata in un file denominato. `PrivateKey.pem`
- Hai il ARN certificato che desideri reimportare.

Per utilizzare l'esempio seguente, sostituisci i nomi dei file e la 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 il certificatoARN.

```
$ 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 `import-certificate` comando ha esito positivo, 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)

1. Accedi alla console di AWS gestione e apri la console ACM all'indirizzo 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-----
MIIDTDCCAjSgAwIBAgIRANWuFpqA16g3IwStE3vVpTwwDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNzE5MTYxNTU1WhcNMjAwODE5MTcx
NTU1WjAXMRUwEwYDVQQDDAx3d3cuc3B1ZHMuaW8wggEiMA0GCSqGSIb3DQEBAQUA
...
8UNFQvNoo1VtICL4cwWOdLOkxpwkkKWtcEkQuHE1v5Vn6HpbfFmxkdPEasoDhthH
```

```
FFWIf4/+VOlbDLgjU4HgtmV4IJDtqM9rGOZ42eFYmmc3eQO0GmigBBwwXp3j6hoi
74YM+igvtILnbYkPYhY9qz8h7lHUmannS8j6YxmtpPY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIRAM/jQ/6h2/MI1NYWX3dDaZswDQYJKoZIhvcNAQELBQAw
EzERMA8GA1UECgwIdHJvbG9sb2wwHhcNMTkwNjE5MTk0NTE2WhcNMjkwNjE5MjA0
NTE2WjATMREwDwYDVQQKDAh0cm9sb2xvbDCCASIwDQYJKoZIhvcNAQEBBQADggEP
...
j2PAOviqIXjwr08Zo/rTy/8m6LAsmm3LVVYKLyPdl+KB6M/+H93Z1/Bs8ERqqga/
6lfM6iw2JHtkW+q4WexvQSoqRXFhCZWbWPZTUpBS0d4/Y5q92S3iJLRa/JQ0d4U1
tWZyqJ2rj2RL+h7CE71XIAM//oHGcDDPaQBFD2DTisB/+ppGeDuB
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUMrZb7kZJ8nTZg7aB
1zmaQh4vwloCAggAMB0GCWCGSAFlAwQBKgQQDViroIHStQgNOjR6nTUnuwSCBNAN
JM4SG202YPUiddWeWmX/RKGg3lIdE+A0WLTPskNCdCAHqdhOSqBwt65qUTZe3gBt
...
ZGipF/DobHDMkpwiaRR5sz6nG4wcki0ryYjAQrdGsR6EVvUUXADkrnrrxuHTWjFl
wEuqyd8X/ApkQsYFX/nhepOEIGWf8Xu0nrjQo77/evhG0sHXborGzgCJwKuimPVy
Fs5kw5mvEoe5DAe3rSKsSUJ1tM4RagJj2WH+BC04SZWNH8kxfOC1E/GSLBCixv3v
+Lwq38CEJRQJLdpta8NcLKnFBwmmVs9OV/VXzNuHYg==
-----END ENCRYPTED PRIVATE KEY-----
```

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

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 AWSl'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

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

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'PutAccountConfigurationazione 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 LambdaAttivazione 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 ACM i certificati.

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/, 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. SelezionaCategorie 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 PutAccountConfigurationfunzionamento 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/, 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'AddTagsToCertificateAPI.


```
{

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

```
      }
   ]
}
```

Eliminazione di un certificato (DeleteCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'DeleteCertificateAPI.

```
{

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

Descrizione di un certificato (DescribeCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'DescribeCertificateAPI.

> **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'DescribeCertificateAPI.


```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:42Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"DescribeCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "certificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/
fedcba98-7654-3210-fedc-ba9876543210"
         },
         "responseElements":null,
         "requestID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventID":"fedcba98-7654-3210-fedc-ba9876543210",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Esportazione di un certificato (ExportCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'ExportCertificateAPI.

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

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

```
                  "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 ImportCertificateAPI 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'ListCertificatesAPI.

> **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'ListCertificatesAPI.

```
{
   "Records":[
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:43Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"ListCertificates",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "maxItems":1000,
            "certificateStatuses":[
               "ISSUED"
            ]
         },
         "responseElements":null,
         "requestID":"74c99844-ec9c-11e5-ac34-d1e4dfe1a11b",
         "eventID":"cdfe1051-88aa-4aa3-8c33-a325270bff21",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Elenco di tag per un certificato (ListTagsForCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'ListTagsForCertificateAPI.

> **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'o l'ListTagsForCertificateAPI.


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


Rimozione di tag da un certificato (RemoveTagsFromCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'RemoveTagsFromCertificateAPI.

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


Richiesta di un certificato (RequestCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'RequestCertificateAPI.


```
{
   "Records":[
```

```
      {
         "eventVersion":"1.04",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"Alice"
         },
         "eventTime":"2016-03-18T00:00:49Z",
         "eventSource":"acm.amazonaws.com",
         "eventName":"RequestCertificate",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"192.0.2.0",
         "userAgent":"aws-cli/1.9.15",
         "requestParameters":{
            "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'ResendValidationEmailAPI.

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

Recupero di un certificato (GetCertificate)

L' CloudTrail esempio seguente mostra i risultati di una chiamata all'GetCertificateAPI.

```
{

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

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

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

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

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

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` for a 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 • Valore: ARN del certificato.

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

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

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

         timeSlept += sleepInterval;
      }

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Consultate i seguenti argomenti se riscontrate problemi durante la richiesta di un certificato. ACM

Argomenti

Timeout della richiesta di certificato

Le richieste di ACM certificati 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 DNSconvalida o Convalida e-mail. Ti consigliamo di utilizzare la DNS convalida, se possibile.

Errore nella richiesta di certificato

Se la richiesta non va a buon fine ACM e ricevi uno dei seguenti messaggi di errore, segui i passaggi suggeriti 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

Hai scelto la convalida e-mail quando richiedi un certificato, ma non sei ACM riuscito a trovare un indirizzo e-mail da utilizzare per convalidare uno o più nomi di dominio nella richiesta. Per risolvere questo problema, puoi procedere in uno dei seguenti modi:

- Assicurati di avere un indirizzo email funzionante registrato WHOIS e che l'indirizzo sia visibile quando esegui una WHOIS ricerca 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 del tuo dominio deve avere un record di scambio di posta (record MX) in modo che i server ACM di posta elettronica 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 assicurarsi di ricevere e-mail di convalida del dominio daACM, consulta o. (Facoltativo) Configurazione dell'e-mail per il dominio in uso 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

ACMrichiede informazioni aggiuntive per elaborare questa 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 ACM discussione.

> **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 ACM certificato 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. 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 una nuova discussione nel Forum di ACM discussione.

Risoluzione dei problemi di convalida dei certificati

Se lo stato della richiesta di ACM certificato è In attesa di convalida, la richiesta è in attesa di intervento da parte tua. 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 WHOIS contatto registrati e ad altri indirizzi e-mail comuni per il dominio richiesto. Per ulteriori informazioni, consulta Convalida e-mail. Se hai scelto DNS la convalida, devi scrivere il CNAME record ACM creato per te DNS nel tuo database. Per ulteriori informazioni, consulta DNSconvalida.

> **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 hai scelto DNS la convalida, devi creare un CNAME record per ogni dominio.

> **Note**
>
> ACMI certificati pubblici possono essere installati su EC2 istanze Amazon collegate a una Nitro Enclave, ma non su altre istanze Amazon. EC2 Per informazioni sulla configurazione di un server Web autonomo su un'EC2istanza Amazon non connessa a una Nitro Enclave, consulta Tutorial: Installa un LAMP server Web su Amazon Linux 2 o Tutorial: Installa un server LAMP Web con Amazon Linux. AMI

Ti consigliamo di utilizzare la convalida anziché la DNS convalida via e-mail.

Se riscontri problemi di convalida, consulta i seguenti argomenti.

Argomenti

- Risolvi i problemi DNS di convalida
- Risoluzione dei problemi di convalida e-mail

Risolvi i problemi DNS di convalida

Consulta la seguente guida se hai problemi a convalidare un certificato con. DNS

Il primo passo per la DNS risoluzione dei problemi consiste nel verificare lo stato attuale del dominio con strumenti come i seguenti:

- dig — Linux, Windows
- nslookup — Linux, Windows
- whois—Linux,Windows

Argomenti

Sottolineature proibite dal provider DNS

Se il tuo DNS provider proibisce i caratteri di sottolineatura iniziali nei CNAME valori, puoi rimuovere il carattere di sottolineatura dal valore ACM fornito e convalidare il dominio senza di esso. Ad esempio, il CNAME valore `_x2.acm-validations.aws` può essere modificato a scopo di convalida. `x2.acm-validations.aws` Tuttavia, il parametro CNAME name deve sempre iniziare con un carattere di sottolineatura iniziale.

Per convalidare un dominio è possibile utilizzare uno dei valori a destra della tabella qui di seguito.

Nome	Type	Valore
`_<random value>.example.com.`	CNAME	`_<random value>.acm-validations.aws.`
`_<random value>.example.com.`	CNAME	`<random value>.acm-validations.aws.`

Periodo finale predefinito aggiunto dal provider DNS

Alcuni DNS provider aggiungono per impostazione predefinita un periodo finale al CNAME valore fornito dall'utente. 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.

DNSconvalida in caso di errore GoDaddy

DNSla convalida per i domini registrati con Godaddy e altri registri potrebbe non riuscire a meno che non si modifichino i valori forniti da. CNAME ACM Prendendo example.com come nome di dominio, il record emesso ha il seguente formato: CNAME

```
NAME: _ho9hv39800vb3examplew3vnewoib3u.example.com. VALUE:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

È possibile creare un CNAME record compatibile con GoDaddy troncando il dominio apex (incluso il punto) alla fine del campo, come segue: NAME

```
NAME: _ho9hv39800vb3examplew3vnewoib3u VALUE:
 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws.
```

ACMLa console non visualizza il pulsante «Crea record in Route 53"

Se scegli Amazon Route 53 come DNS provider, 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 DNS provider.
- Hai effettuato l'accesso a ACM Route 53 tramite account diversi.
- Non hai le IAM autorizzazioni per creare record 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 DNS convalida, 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 puoi utilizzarlo per ospitare DNS record per domini privati, incluse risorse in una zona ospitata VPC privata di Amazon, domini non attendibili nei tuoi certificati privati PKI e 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 non va a buon fine con l'indicazione «In attesa di convalida» anche se DNS è corretta, verifica che l'emissione non sia bloccata da un record di Certification Authority Authorization (). CAA Per ulteriori informazioni, consulta (CAAFacoltativo) Configura un record.

La convalida non riesce per il server su un DNS VPN

Se trovi un DNS server su un server VPN e ACM non riesci a convalidare un certificato in base ad esso, controlla se il server è accessibile pubblicamente. L'emissione di certificati pubblici mediante la ACM DNS convalida richiede che i record del dominio siano risolvibili sulla rete Internet pubblica.

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
- Throttling WHOIS
- Timestamp iniziale persistente per la convalida tramite e-mail
- Risolvere i problemi relativi al dominio di primo livello .IO
- Non riesco a passare alla convalida DNS

Mancata ricezione dell'e-mail di convalida

Quando si richiede un certificato ACM e si sceglie la convalida e-mail, l'e-mail di convalida del dominio viene inviata a tre indirizzi di contatto specificati in WHOIS e a cinque indirizzi amministrativi 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 amministrativi comuni del 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 inWHOIS. Controlla

l'elenco di indirizzi e-mail visualizzati nella ACM console (o restituiti da CLI oAPI) per determinare dove cercare 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.

GMailordina automaticamente le tue e-mail

Se la utilizziGMail, l'e-mail di convalida potrebbe essere stata ordinata automaticamente nelle schede Aggiornamenti o 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 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 tuo registrar in modo che inserisca il tuo indirizzo e-mailWHOIS, sebbene non tutti i registrar supportino 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 tuo dominio non sono disponibili tramite WHOIS o se l'e-mail inviata alle informazioni di contatto non raggiunge il proprietario del dominio o un rappresentante autorizzato, ti consigliamo di configurare il tuo dominio o sottodominio per

ricevere e-mail inviate a uno o più indirizzi amministrativi comuni formati anteponendo admin@, administrator@, hostmaster@, webmaster@ e postmaster@ al nome di 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 inviare l'e-mail di convalida e aver confermato che puoi ricevere e-mail per quell'indirizzo, sei pronto per 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). È inoltre possibile visualizzare l'elenco nella Fase 3: Convalida della procedura guidata di ACM richiesta di certificato. 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 di risorse nel database Domain Name System (DNS) che specifica uno o più server di posta che accettano messaggi e-mail per il tuo 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 la richiesta di un record MX, è possibile utilizzare l'`ValidationDomain`opzione RequestCertificateAPIo il AWS CLI comando request-certificate per specificare il nome di dominio a cui ACM inviare le e-mail di convalida. Se si utilizza 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 ACM discussione.

E-mail inviata al sottodominio

Se utilizzi la console e richiedi un certificato per un nome di sottodominio`sub.test.example.com`, ad esempio, ACM verifica se esiste un record 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 discussione approfondita su come configurare la posta elettronica e su come ACM funziona il DNS WHOIS database, consulta(Facoltativo) Configurazione dell'e-mail per il dominio in uso.

Invece di utilizzare la console, puoi utilizzare l'`ValidationDomain`opzione in RequestCertificateAPIo il AWS CLI comando request-certificate per specificare il nome di dominio a cui ACM inviare le e-mail di convalida. Se si utilizza 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 ti consentono di nascondere le tue informazioni di contatto nella tua WHOIS scheda. 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 posta, assicurati che le tue informazioni di contatto siano pubbliche oWHOIS, se la tua WHOIS inserzione mostra un indirizzo email riservato, assicurati che le email inviate all'indirizzo riservato vengano inoltrate al tuo indirizzo email reale. Una volta completata la WHOIS configurazione e purché la richiesta del certificato non sia scaduta, puoi scegliere di inviare nuovamente l'e-mail di convalida. ACMesegue una nuova ricerca WHOIS /MX e invia un'e-mail di convalida all'indirizzo di contatto attualmente pubblico.

Rinnovo dei certificati

Se hai reso pubbliche WHOIS le tue informazioni quando hai richiesto un nuovo certificato e successivamente le hai offuscate, ACM non puoi recuperare gli indirizzi di contatto registrati quando tenti di rinnovare il certificato. ACMinvia e-mail di convalida a questi indirizzi di contatto e a cinque indirizzi amministrativi comuni formati utilizzando il record MX. Per risolvere questo problema, rendi nuovamente pubbliche WHOIS le tue informazioni e invia nuovamente le e-mail di convalida. ACMesegue una nuova ricerca WHOIS /MX e invia e-mail di convalida ai vostri indirizzi di contatto ora pubblici.

Throttling WHOIS

A volte non ACM è in grado di contattare il WHOIS server anche dopo aver inviato più richieste di e-mail di convalida. Questo problema è esterno a. AWS Cioè, AWS non controlla i WHOIS server e non può impedire la limitazione WHOIS del server. 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. Questa non è una prova di un errore nelle ACM operazioni.

Risolvere i problemi relativi al dominio di primo livello .IO

Il dominio di primo livello .IO viene assegnato al Territorio britannico dell'Oceano Indiano. Attualmente, il registro dei domini non visualizza le informazioni pubbliche del WHOIS database. Ciò è valido sia che la protezione della privacy per il dominio sia abilitata o meno. I registrar possono visualizzare queste informazioni nei propri WHOIS output se la protezione della privacy è disabilitata, ma questa pratica varia tra i registrar. ACMnon è in grado di inviare e-mail di convalida ai seguenti tre indirizzi di contatto registrati se non sono disponibili presso il registrar in. WHOIS

- Registrant del dominio
- Contatto tecnico
- Contatto amministrativo

ACMinvia tuttavia un'e-mail di convalida ai seguenti cinque indirizzi di sistema comuni dove *`your_domain`* è il nome di dominio che hai inserito quando hai richiesto inizialmente un certificato ed `.io` è il dominio di primo livello.

- amministratore@*your_domain*.io
- hostmaster @*your_domain*.io
- direttore delle poste@*your_domain*.io
- webmaster@*your_domain*.io
- amministratore@*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 ti verrà rilasciato un certificato. ACM

> **Note**
>
> Ti consigliamo di utilizzare la DNS convalida anziché la convalida tramite e-mail. Per ulteriori informazioni, consulta DNSconvalida.

Non riesco a passare alla convalida DNS

Dopo aver creato un certificato con convalida e-mail, non puoi passare alla convalida con. DNS Per utilizzare DNS la convalida, elimina il certificato e creane uno nuovo che utilizzi la convalida. DNS

Risoluzione dei problemi relativi al rinnovo dei certificati gestiti

ACMtenta di rinnovare automaticamente i ACM certificati prima che scadano, in modo da non richiedere alcuna azione da parte dell'utente. Consulta i seguenti argomenti in caso di problemi con Rinnovo gestito per ACM i certificati.

Preparazione per la convalida automatica dei domini

Prima di ACM poter rinnovare automaticamente i certificati, deve essere vero quanto segue:

- Il certificato deve essere associato a un AWS servizio integrato conACM. Per informazioni sulle risorse che ACM supporta, vedereServizi integrati con AWS Certificate Manager.
- Per i certificati convalidati tramite posta elettronica, ACM devi essere in grado di contattarti a un indirizzo email di amministratore per ogni dominio elencato nel certificato. Gli indirizzi e-mail che verranno provati sono elencati in Convalida e-mail.

- Per i certificati DNS convalidati, assicurati che la DNS configurazione contenga i record correttiCNAME, come descritto in. DNSconvalida

Gestione degli errori relativi al rinnovo gestito dei certificati

Quando il certificato si avvicina alla scadenza (60 giorni perDNS, 45 per EMAIL e 60 giorni per Privato), 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 ACM i certificati.

Rinnovo gestito del certificato per i certificati convalidati tramite e-mail

ACMi certificati sono validi per 13 mesi (395 giorni). Il rinnovo di un certificato richiede l'intervento del proprietario del dominio. ACMinizia a inviare avvisi di rinnovo agli indirizzi e-mail associati al dominio 45 giorni prima della scadenza. Le notifiche contengono un link su cui il proprietario del dominio può fare clic per il rinnovo. Una volta convalidati tutti i domini elencati, ACM emette un certificato rinnovato con gli stessi. ARN

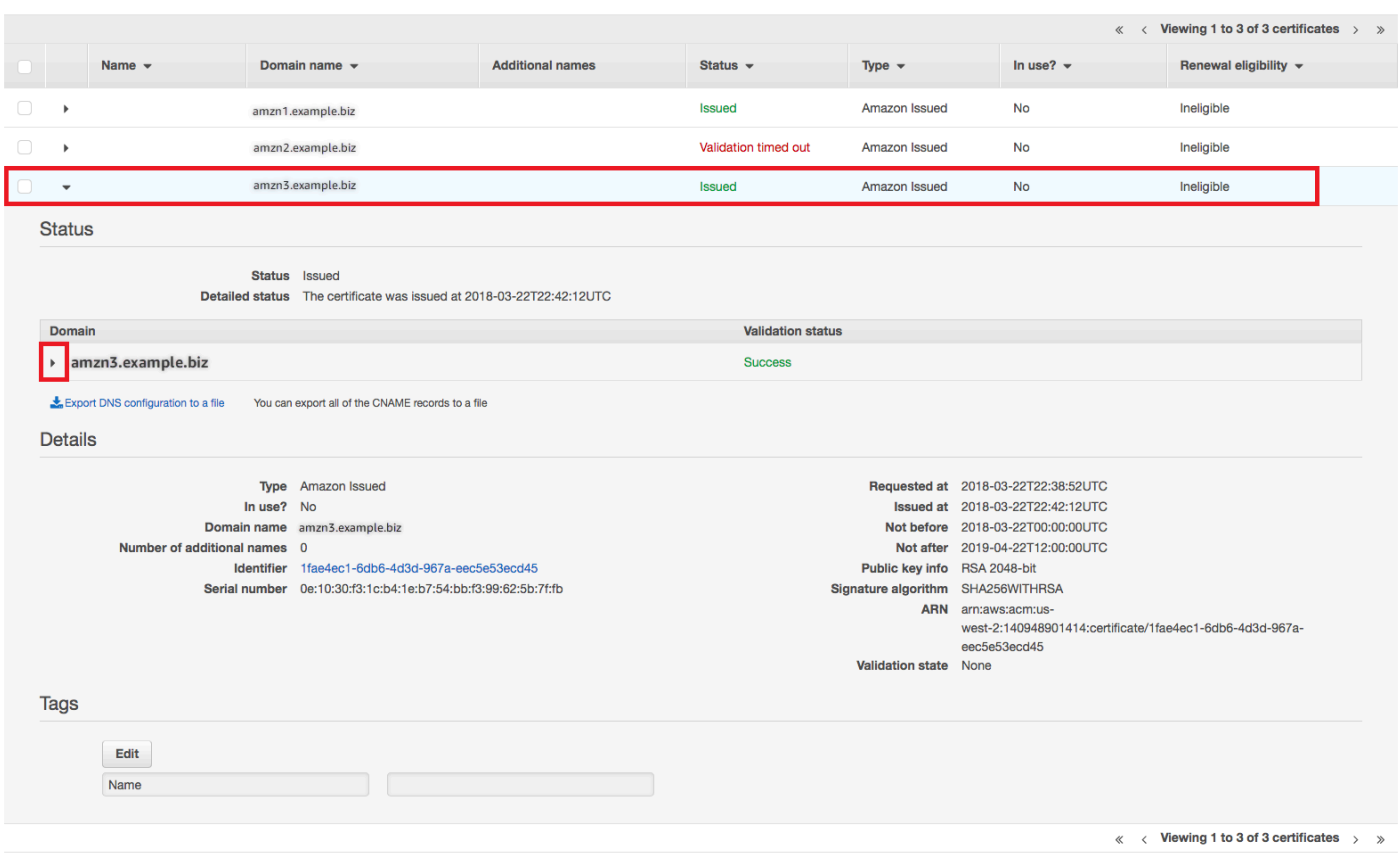
Consulta Convalida tramite e-mail per le istruzioni su come identificare i domini che sono nello stato `PENDING_VALIDATION` e ripetere il processo di convalida per quei domini.

Rinnovo gestito dei certificati per DNS certificati convalidati

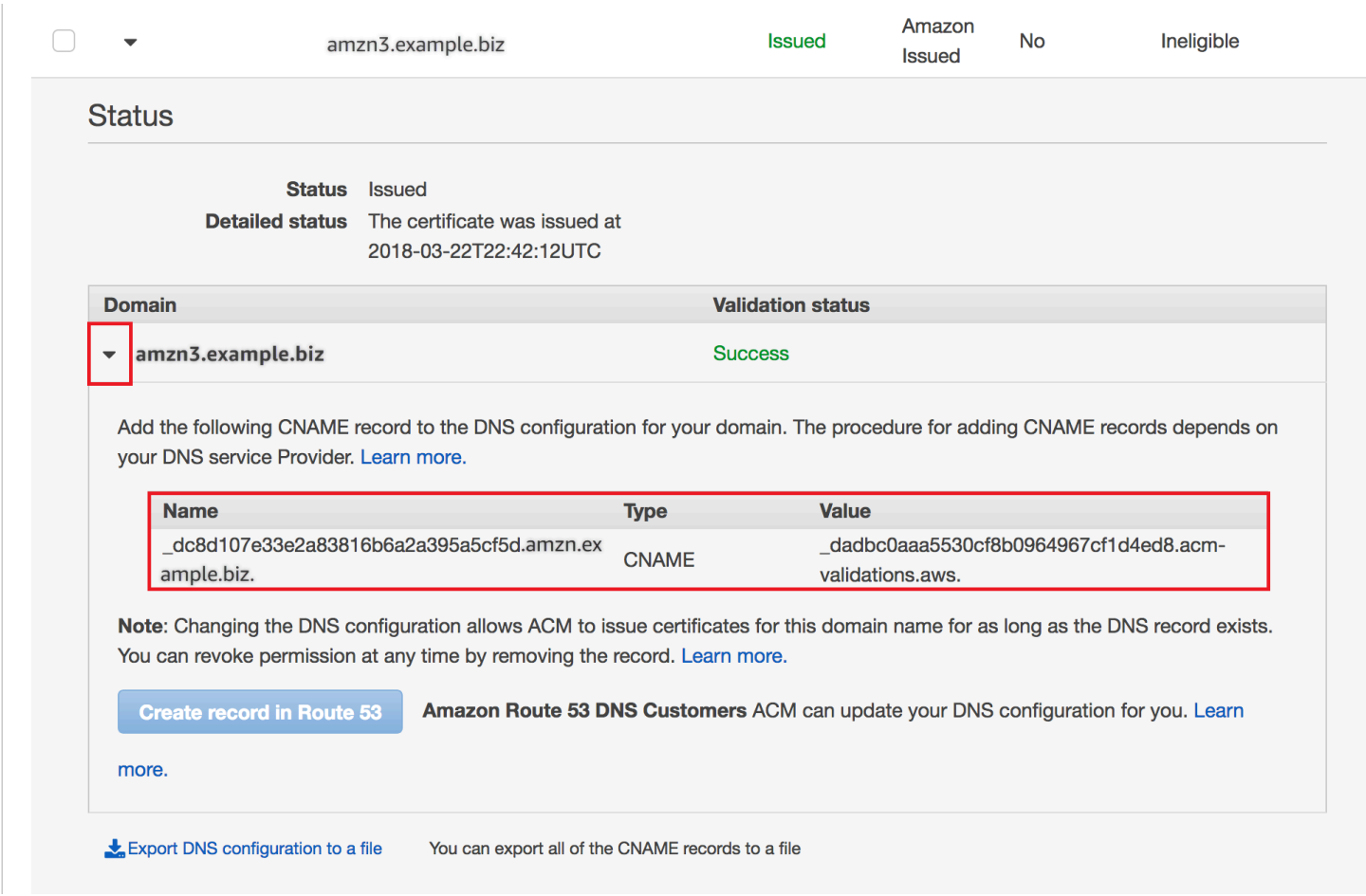
ACMnon tenta la convalida per i certificati TLS -validatedDNS. Se ACM non riesci a rinnovare un certificato che hai convalidato con la DNS convalida, è molto probabilmente dovuto a record mancanti o imprecisi nella tua configurazione. CNAME DNS In tal caso, ti ACM avvisa che il certificato non può essere rinnovato automaticamente.

> **Important**
>
> È necessario inserire i CNAME record corretti nel DNS database. Per informazioni su come fare, consulta il tuo registrar di dominio.

Puoi trovare i CNAME record dei tuoi domini espandendo il certificato e le relative voci di dominio nella ACM console. Fai riferimento alle illustrazioni seguenti per i dettagli. Puoi anche recuperare CNAME i record utilizzando l'DescribeCertificateoperazione in ACM API o il comando describe-certificate in. ACM CLI Per ulteriori informazioni, consulta DNSconvalida.



Scegli il certificato di destinazione dalla console.



Espandi la finestra del certificato per trovare le CNAME informazioni sul certificato.

Se il problema persiste, contatta il Centro di supporto.

Informazioni sulla tempistica di rinnovo

Rinnovo gestito per ACM i certificati è un processo asincrono. Ciò significa che i passaggi non si verificano consecutivamente. Dopo che tutti i nomi di dominio contenuti in un ACM certificato sono stati convalidati, potrebbe verificarsi un ritardo nell'ACMottenimento del nuovo certificato. Può verificarsi un ulteriore ritardo tra il momento in cui si ACM ottiene il certificato rinnovato e il momento in cui il certificato viene distribuito alle AWS risorse 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

Questa sezione include linee guida per problemi non correlati all'emissione o alla convalida dei certificati. ACM

Argomenti

Problemi relativi all'autorizzazione dell'Autorità di certificazione () CAA

Puoi utilizzare CAA DNS i record per specificare che l'autorità di certificazione Amazon (CA) può emettere ACM certificati per il tuo dominio o sottodominio. Se durante l'emissione del certificato ricevi un errore che indica che la convalida di uno o più nomi di dominio non è riuscita a causa di un errore di autorizzazione dell'Autorità di certificazione (CAA), controlla i tuoi record. CAA DNS Se ricevi questo errore dopo che la richiesta di ACM certificato è stata convalidata con successo, devi aggiornare i CAA record e richiedere nuovamente un certificato. Il campo del valore nel CAA record deve contenere uno dei seguenti nomi di dominio:

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

Per ulteriori informazioni sulla creazione di un CAA record, vedere(CAAFacoltativo) Configura un record.

> **Note**
>
> Puoi scegliere di non configurare un CAA record per il tuo dominio se non desideri abilitare il CAA controllo.

Problemi di importazione dei certificazione

Puoi importare certificati di terze parti ACM e associarli a servizi integrati. In caso di problemi, consulta gli argomenti correlati ai prerequisiti e al formato dei certificati. In particolare, tieni presente quanto segue:

- È possibile importare solo certificati X.509 versione 3 SSL TLS /.
- 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.
- Il certificato, la catena di certificati e la chiave privata (se presente) devono essere PEM codificati. In generale, la PEM codifica consiste in blocchi di testo codificato in Base64 che iniziano e finiscono con righe di intestazione e piè di pagina in ASCII testo semplice. Non è necessario aggiungere linee o spazi o apportare altre modifiche a un file durante la copia o il caricamento. PEM È possibile verificare le catene di certificati utilizzando l'utilità Open SSL verify.
- 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 di chiave ACM supportati. Consulta la Guida per l' AWS Certificate Manager utente e la documentazione di ogni servizio per assicurarti che il tuo certificato funzioni.
- Il supporto dei certificati da parte dei servizi integrati potrebbe differire a seconda che il certificato venga importato IAM o menoACM.
- 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 si chiama il comando ListCertificatesAPIo il AWS CLI comando list-certificates senza specificare il `keyTypes` filtro, vengono visualizzati solo `RSA_2048` i certificati `RSA_1024` o.

Problemi di associazione dei certificati

Per rinnovare un certificato, ACM genera una nuova coppia di chiavi pubblica-privata. Se l'applicazione utilizza un certificatoAssociazione dei certificati, a volte noto come SSL pinning, per

bloccare un ACM certificato, l'applicazione potrebbe non essere in grado di connettersi al dominio dopo AWS il rinnovo del certificato. Per questo motivo, ti consigliamo di non aggiungere un certificato. ACM Se la tua applicazione deve associare un certificato, puoi eseguire quanto indicato di seguito:

- Importa il tuo certificato ACM e aggiungi la tua applicazione al certificato importato. ACMnon 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.

APIProblemi relativi al gateway

Quando distribuisci un API endpoint ottimizzato per l'edge, API Gateway configura una distribuzione per te. CloudFront La CloudFront distribuzione è di proprietà di API Gateway, non del tuo account. La distribuzione è vincolata al ACM certificato che hai utilizzato durante la distribuzione del tuoAPI. Per rimuovere l'associazione e consentire ACM l'eliminazione del certificato, è necessario rimuovere il dominio personalizzato API Gateway associato al certificato.

Quando distribuisci un API endpoint regionale, API Gateway crea un Application Load Balancer (ALB) per tuo conto. Il load balancer è di proprietà di API Gateway e non è visibile all'utente. ALBÈ associato al ACM certificato che hai utilizzato durante la distribuzione del tuo. API Per rimuovere l'associazione e consentire ACM l'eliminazione del certificato, è necessario rimuovere il dominio personalizzato API Gateway associato al certificato.

Cosa fare quando un certificato smette di funzionare in modo imprevisto

Se hai associato correttamente un ACM certificato 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 ACM certificato.

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 è concessa da una politica basata sulle risorse che ACM si applica quando si associa un certificato a. ELB Se ELB perde la concessione di tale autorizzazione, l'autorizzazione avrà esito negativo al successivo tentativo di decrittografare la chiave del certificato.

Per esaminare il problema, controlla lo stato delle tue sovvenzioni utilizzando la console all' AWS KMS indirizzo. 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 ACM siano state revocate, contatta AWS Support at home#/. https://console.aws.amazon.com/support/

Problemi con il ruolo collegato al servizio () ACM SLR

Quando emettete un certificato firmato da una CA privata che è stato condiviso con voi da un altro account, al primo utilizzo ACM tenta di impostare un ruolo collegato al servizio (SLR) per interagire come principale con una CA privata AWS politica di accesso basata sulle risorse. Se emetti un certificato privato da una CA condivisa e SLR questo non esiste, non ACM potrai rinnovarlo automaticamente.

ACMpotrebbe avvisarti che non è in grado di determinare se ne SLR esiste uno sul tuo account. Se l'`iam:GetRole`autorizzazione richiesta è già stata concessa al ACM SLR tuo account, l'avviso non si ripeterà dopo la SLR creazione. Se l'errore si ripresenta, tu o l'amministratore del tuo account potreste dover concedere l'`iam:GetRole`autorizzazione o associare il vostro account alla ACM politica gestitaACM. `AWSCertificateManagerFullAccess`

Per ulteriori informazioni, consulta la sezione Autorizzazioni relative ai ruoli collegati ai servizi nella Guida per l'utente. 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 PKI certificato 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`	La CA privata non ha concesso ACM le autorizzazioni. Ciò attiva un codice di CA privata AWS `AccessDeniedException` errore. Per risolvere il problema, concedi le autorizza zioni necessarie al responsabile del ACM servizio che utilizza l' CA privata AWS CreatePermissionoperazione.
`PCA_INVALID_DURATION`	Il periodo di validità del certificato richiesto supera il periodo di validità della CA privata emittente. Ciò attiva un codice di CA privata AWS `ValidationException` errore. Per risolvere il problema, installa un nuovo certificato CA con un periodo di validità appropriato.
`PCA_INVALID_STATE`	La CA privata chiamata non si trova nello stato corretto per eseguire l'ACMoperazione richiesta. Ciò attiva un codice di CA privata AWS `InvalidStateException` errore. Risolvere il problema come segue: • Se la CA ha lo stato `CREATING`, attendi il completamento della creazione e quindi installa il certificato CA. • Se la CA ha lo stato `PENDING_C ERTIFICATE` , installa il certificato CA. • Se la CA ha lo stato `DISABLED`, aggiornala allo stato `ACTIVE`. • Se la CA ha lo stato `DELETED`, ripristinala.

Codice di errore ACM	Commento
	• Se la CA ha lo stato `EXPIRED`, installa un nuovo certificato • Se la CA ha lo stato `FAILED` e non puoi risolvere il problema, contatta AWS Support.
`PCA_LIMIT_EXCEEDED`	La CA privata ha raggiunto una quota di emissione. Ciò attiva un codice di CA privata AWS `LimitExceededException` errore. Prova a ripetere la richiesta prima di procedere con questa guida. Se l'errore persiste, contatta AWS Support per richiedere un aumento della quota.
`PCA_REQUEST_FAILED`	Si è verificato un errore di rete o di sistema. Ciò attiva un codice di CA privata AWS `RequestFailedException` errore. Prova a ripetere la richiesta prima di procedere con questa guida. Se l'errore persiste, contatta AWS Support.
`PCA_RESOURCE_NOT_FOUND`	La CA privata è stata eliminata definitivamente. Ciò attiva un codice di CA privata AWS `ResourceNotFoundException` errore. Verifica di aver usato il codice correttoARN. Se ciò non riesce, non potrai utilizzare questa CA. Per risolvere il problema, crea una nuova CA.
`SLR_NOT_FOUND`	Per rinnovare un certificato firmato da una CA privata che risiede in un altro account, è ACM necessario un Service Linked Role (SLR) sull'account in cui risiede il certificato. Se devi ricreare un file eliminato, consulta. SLR Creazione del SLR per ACM

Concetti

In questa sezione vengono fornite le definizioni dei concetti utilizzati da AWS Certificate Manager.

Argomenti

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 DNSconvalida.

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, bare, 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, $[subdomain_1].[subdomain_2]...[subdomain_n].[apex\ domain].[top\text{-}level\ domain]$ 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 $[subdomain_1.subdomain_2.]$ 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

La tabella seguente descrive la cronologia dei rilasci della documentazione a AWS Certificate Manager partire dal 2018.

Modifica	Descrizione	Data
Procedura di convalida e-mail aggiornata	La ACM console non supporta più la convalida delle e-mail utilizzando. WHOIS Se desideri convalidare il tuo dominio tramite e-mail, configura la convalida del dominio utilizzando la console,API, SDK o. CLI	11 luglio 2024
Obsoletamento della convalida delle e-mail di Mail Exchanger (MX)	La ACM console non supporta più mail exchanger (MX).	11 luglio 2024
Aggiungere le migliori pratiche in materia di separazione a livello di account	Utilizza la separazione a livello di account nelle tue politiche laddove possibile. Se non è possibile, puoi limitare le autorizzazioni a livello di account o utilizzando le chiavi di condizione del contesto di crittografia nelle tue politiche.	11 giugno 2024
Imminente obsolescenza della verifica via e-mail WHOIS	È stata aggiunta una nota sull'obsolescenza della verifica WHOIS via e-mail a partire da giugno 2024.	5 febbraio 2024
Aggiunto il supporto per le chiavi di condizione	È stato aggiunto il supporto per i tasti IAM Condition durante la richiesta di certifica	24 agosto 2023

	ti. ACM Per un elenco delle condizioni supportate, consulta https://docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported.	
ECDSAsupporto aggiunto	È stato aggiunto il supporto per Elliptic Curve Digital Signature Algorithm (ECDSA) quando si richiede un certificato pubblico. ACM Per un elenco degli algoritmi chiave supportati, consulta https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms.	8 novembre 2022
Nuovi eventi CloudWatch	Sono stati aggiunti gli eventi ACM Certificato scaduto, ACM Certificato disponibile e Azione di rinnovo del ACM certificato richiesta. Per un elenco degli CloudWatch eventi supportati, consultahttps://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	27 ottobre 2022

Aggiornamento dei tipi di algoritmi chiave per l'importazione	I certificati importati in ACM potrebbero ora avere chiavi con algoritmi aggiuntivi RSA e a curva ellittica. Per un elenco degli algoritmi chiave attualmente supportati, consulta https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html.	14 luglio 2021
Promozione di "Monitoraggio e registrazione" come capitolo separato	Documentazione di monitoraggio e registrazione spostata nel capitolo appropriato. Questa modifica riguarda CloudWatch Metrics, CloudWatch Events/ e. EventBridge CloudTrail Per ulteriori informazioni, consulta https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html.	23 marzo 2021
Aggiunto il supporto per CloudWatch metriche ed eventi	Aggiunti DaysToExpiry parametri, eventi e supporto. APIs Per ulteriori informazioni, consulta https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html e https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	3 marzo 2021

Aggiunta del supporto tra account	È stato aggiunto il supporto per più account per l'utilizzo di un modulo privatoCAs. CA privata AWS Per ulteriori informazioni, consulta https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html.	17 agosto 2020
Aggiunta del supporto regionale	È stato aggiunto il supporto regionale per le regioni della AWS Cina (Pechino e Ningxia). Per un elenco completo delle aree supportate, vedere https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region.	4 marzo 2020
Aggiunta del test del flusso di lavoro di rinnovo	I clienti possono ora testare manualmente la configurazione del loro flusso di lavoro di rinnovo ACM gestito. Per ulteriori informazioni, consulta ACMTesting's Managed Renewal Configuration.	14 marzo 2019
Registrazione predefinita della trasparenza del certificato	È stata aggiunta la possibilità di pubblicare certificati ACM pubblici nei registri di trasparenza dei certificati per impostazione predefinita.	24 Aprile 2018

Avvio CA privata AWS	Lancio del ACM Private Certificate Manager (CM) e l'estensione dello AWS Certificate Manager stesso consente agli utenti di creare un'infrastruttura gestita sicura per l'emissione e la revoca di certificati digitali privati. Per ulteriori informazioni, consulta Private Certificate Authority AWS.	4 aprile 2018
Registrazione della trasparenza del certificato	È stata aggiunta la registrazione della trasparenza del certificato alle Best Practice.	27 marzo 2018

La tabella seguente descrive la cronologia dei rilasci della documentazione AWS Certificate Manager precedenti al 2018.

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	È stata aggiunta DNS la convalida a. DNSconvalida	21 Novembre 2017
Nuovo contenuto	Sono stati aggiunti nuovi esempi di codice Java su Utilizzo dell'API (esempi Java).	12 ottobre 2017
Nuovo contenuto	Sono state aggiunte informazioni sui CAA record a. (CAAFacoltativo) Configura un record	21 settembre 2017
Nuovo contenuto	Sono state aggiunte informazioni relative ai domini .io su Risoluzione dei problemi.	07 luglio 2017

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	Sono state aggiunte informazioni relative alla reimportazione di un certificato su Reimportazione di un certificato.	07 luglio 2017
Nuovo contenuto	Sono state aggiunte informazioni relative all'associazione di un certificato su Best practice e su Risoluzione dei problemi.	07 luglio 2017
Nuovo contenuto	Aggiunto AWS CloudFormation aServizi integrati con AWS Certificate Manager.	27 maggio 2017
Aggiornamento	Sono state aggiunte ulteriori informazioni su Quote.	27 maggio 2017
Nuovo contenuto	È stata aggiunta la documentazione relativa a Identity and Access Management per AWS Certificate Manager.	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 Convalida e-mail.	21 Aprile 2017
Aggiornamento	Sono state aggiunte informazioni relative alla configurazione di e-mail per il tuo dominio. Per informazioni, consulta (Facoltativo) Configurazione dell'e-mail per il dominio in uso.	6 Aprile 2017

Modifica	Descrizione	Data di rilascio
Aggiornamento	Sono state aggiunte informazioni relative al controllo dello stato di rinnovo del certificato nella console. Per informazioni, consulta Verifica dello stato di rinnovo di un certificato.	28 marzo 2017
Aggiornamento	Aggiornamento della documentazione per l'utilizzo di Elastic Load Balancing.	21 marzo 2017
Nuovo contenuto	È stato aggiunto il supporto per AWS Elastic Beanstalk Amazon API Gateway. Per informazioni, consulta Servizi integrati con AWS Certificate Manager.	21 marzo 2017
Aggiornamento	È stata aggiornata la documentazione relativa a Rinnovo gestito.	20 febbraio 2017
Nuovo contenuto	È stata aggiunta la documentazione relativa a Importazione di certificati .	13 Ottobre 2016
Nuovo contenuto	È stato aggiunto AWS CloudTrail il supporto per ACM le azioni. Per informazioni, consulta Utilizzo con CloudTrail AWS Certificate Manager.	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.