aws

Guide de l’utilisateur

AWS Certificate Manager

Version 1.0

AWS Certificate Manager: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Certificate Manager ?

AWS Certificate Manager (ACM) gère la complexité de la création, du stockage et du renouvellement des certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et vos applications. AWS Vous pouvez émettre des certificats pour vos services AWS intégrés dans ACM, ou importer des certificats tiers dans le système de gestion ACM. Les certificats ACM peuvent sécuriser des noms de domaine uniques, plusieurs noms de domaine spécifiques, des domaines génériques ou des combinaisons de ceux-ci. Les certificats génériques ACM peuvent protéger un nombre illimité de sous-domaines. Vous pouvez également exporter des certificats ACM signés Autorité de certification privée AWS pour les utiliser n'importe où dans votre PKI interne.

> **Note**
>
> ACM n'est pas destiné à être utilisée avec un serveur web autonome. Si vous souhaitez configurer un serveur sécurisé autonome sur une instance Amazon EC2, le didacticiel suivant contient des instructions : Configurer SSL/TLS sur Amazon Linux 2023.

Rubriques

ACM est-il le bon service pour moi ?

AWS propose deux options aux clients déployant des certificats X.509 gérés. Choisissez le meilleur selon vos besoins.

1. AWS Certificate Manager (ACM) —Ce service est destiné aux entreprises clientes qui ont besoin d'une présence Web sécurisée à l'aide du protocole TLS. Les certificats ACM sont déployés via

Elastic Load Balancing CloudFront, Amazon, Amazon API Gateway et d'autres AWS services intégrés. L'application la plus courante de ce type est un site web public sécurisé avec des exigences de trafic importantes. ACM simplifie également la gestion de la sécurité en automatisant le renouvellement des certificats arrivant à expiration. Vous êtes au bon endroit pour ce service.

2. Autorité de certification privée AWS—Ce service est destiné aux entreprises clientes qui créent une infrastructure à clé publique (PKI) dans le AWS cloud et destinée à un usage privé au sein d'une organisation. Vous pouvez ainsi créer votre propre hiérarchie d'autorités de certification (CA) et émettre des certificats à l'aide de celle-ci pour authentifier les utilisateurs, les ordinateurs, les applications, les services, les serveurs et autres appareils. Autorité de certification privée AWS Les certificats émis par une autorité de certification privée ne peuvent pas être utilisés sur Internet. Pour plus d'informations, consultez le Guide de l'utilisateur Autorité de certification privée AWS.

Caractéristiques d'un certificat ACM

Les certificats publics fournis par ACM présentent les caractéristiques décrites dans cette section.

> **Note**
>
> Ces caractéristiques s'appliquent uniquement aux certificats fournis par ACM. Elles ne peuvent pas s'appliquer aux certificats que vous importez dans ACM.

Autorité de certification et hiérarchie

Les certificats publics demandés via ACM sont obtenus auprès d'Amazon Trust Services, une autorité de certification publique (CA) gérée par Amazon. Les autorités de certification racine Amazon 1 à 4 sont signées par une racine plus ancienne nommée Starfield G2 Root Certificate Authority - G2. La racine Starfield est approuvée sur les appareils Android à partir des versions ultérieures de Gingerbread, et sur iOS à partir de la version 4.1. Les racines Amazon sont approuvées par iOS à partir de la version 11. Tout navigateur, application ou système d'exploitation incluant les racines Amazon ou Starfield fera confiance aux certificats publics obtenus auprès d'ACM.

Les certificats feuille ou d'entité finale qu'ACM délivre aux clients tirent leur autorité d'une autorité de certification racine Amazon Trust Services via l'une des nombreuses autorités de certification intermédiaires. De manière aléatoire, ACM attribue une autorité de certification intermédiaire en fonction du type de certificat (RSA ou ECDSA) demandé. Comme la sélection de l'autorité de

certification intermédiaire est faite de manière aléatoire après la génération de la demande, ACM ne fournit pas d'informations liées à l'autorité de certification intermédiaire.

Approbation du navigateur et de l'application

Les certificats ACM sont approuvés par tous les principaux navigateurs, notamment Google Chrome, Microsoft Internet Explorer et Microsoft Edge, Mozilla Firefox et Apple Safari. Les navigateurs qui approuvent les certificats ACM affichent une icône de verrouillage dans leur barre d'état ou barre d'adresse lorsqu'ils sont connectés par SSL/TLS aux sites qui utilisent les certificats ACM. Les certificats ACM sont également approuvés par Java.

Rotation des autorités de certification intermédiaires et racine

Afin de maintenir une infrastructure de certificats résiliente et agile, Amazon est capable à tout moment de mettre fin à une autorité de certification intermédiaire sans préavis. Ces modifications n'ont aucun impact sur les clients. Pour plus d'informations, consultez la rubrique, "Amazon introduit des autorités de certification intermédiaires dynamiques."

Dans le cas peu probable où Amazon mettrait fin à une autorité de certification racine, le changement se produira aussi rapidement que les circonstances l'exigent.. En raison de l'impact important d'un tel changement, Amazon utilisera tous les mécanismes disponibles pour informer les AWS clients, notamment en envoyant un e-mail aux propriétaires de comptes et en contactant les responsables techniques des comptes. AWS Health Dashboard

Accès au pare-feu pour révocation

Si un certificat d'entité finale n'est plus fiable, il sera révoqué. L'OCSP et les CRL sont les mécanismes standard utilisés afin de vérifier la révocation ou non d'un certificat. L'OCSP et les CRL sont les mécanismes standard utilisés afin de publier les informations de révocation. Certains pare-feux clients peuvent nécessiter des règles supplémentaires susceptibles de faire fonctionner ces mécanismes.

Les exemples de modèles de caractères génériques d'URL suivants sont utilisables afin d'identifier le trafic de révocation. Un astérisque (*) représente un ou plusieurs caractères alphanumériques, un point d'interrogation (?) représente un seul caractère alphanumérique et un dièse (#) représente un chiffre.

- OCSP

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

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

- CRL

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

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

Validation du domaine

Les certificats ACM sont validés par domaine. Autrement dit, le champ d'objet d'un certificat ACM identifie un nom de domaine et rien de plus. Lorsque vous demandez un certificat ACM, vous devez valider que vous possédez ou contrôlez tous les domaines spécifiés dans votre demande. Vous pouvez valider la propriété à l'aide d'un courriel ou de DNS. Pour de plus amples informations, consultez Validation par courriel et Validation DNS.

Période de validité

La période de validité des certificats ACM est actuellement de 13 mois (395 jours).

Renouvellement et déploiement gérés

ACM gère le processus de renouvellement des certificats ACM et la mise en service des certificats après leur renouvellement. Le renouvellement automatique peut vous aider à éviter les temps d'arrêt dus aux certificats mal configurés, révoqués ou expirés. Pour plus d'informations, consultez Renouvellement géré des certificats ACM.

Plusieurs noms de domaine

Chaque certificat ACM doit inclure au moins un nom de domaine complet (FQDN). Si vous le souhaitez, vous pouvez également y ajouter d'autres noms. Par exemple, lorsque vous créez un certificat ACM pour `www.example.com`, vous pouvez également ajouter le nom `www.example.net` si les clients peuvent accéder à votre site en utilisant l'un ou l'autre de ces noms. C'est également vrai pour les noms de domaine stricts (aussi appelés domaines de zone apex ou domaines naked). Autrement dit, vous pouvez demander un certificat ACM pour www.example.com et ajouter le nom example.com. Pour de plus amples informations, consultez Demande de certificat public.

Noms de caractère générique

ACM vous permet d'utiliser un astérisque (*) dans le nom de domaine pour créer un certificat ACM contenant un nom de caractère générique permettant de protéger plusieurs sites au sein du même domaine. Par exemple, `*.example.com` protège `www.example.com` et `images.example.com`.

> **Note**
>
> Lorsque vous demandez un certificat générique, l'astérisque (*****) doit se trouver à la position la plus à gauche du nom de domaine et ne peut protéger qu'un seul niveau de sous-domaine. Par exemple, ***.example.com** peut protéger **login.example.com** et **test.example.com**, mais il ne peut pas protéger **test.login.example.com**. Notez aussi que ***.example.com** protège uniquement les sous-domaines de **example.com**, il ne protège pas le domaine strict ou apex (**example.com**). Cependant, vous pouvez demander un certificat qui protège un domaine strict ou apex et ses sous-domaines en indiquant plusieurs noms de domaines dans votre demande. Par exemple, vous pouvez demander un certificat qui protège **example.com** et ***.example.com**.

Algorithme de clés

Un certificat doit indiquer un algorithme et la taille de la clé. Actuellement, les algorithmes de clés publiques RSA et Elliptic Curve Digital Signature Algorithm (ECDSA) et sont pris en charge par ACM. ACM peut demander l'émission de nouveaux certificats à l'aide d'algorithmes marqués d'un astérisque (*). Les autres algorithmes sont pris en charge uniquement par les certificats importés.

> **Note**
>
> Lorsque vous demandez un certificat PKI privé signé par une autorité de certification AWS Private CA, la famille d'algorithmes de signature spécifiée (RSA ou ECDSA) doit correspondre à la famille d'algorithmes de la clé secrète de l'autorité de certification.

- 1 024 bits RSA (`RSA_1024`)
- 2 048 bits RSA (`RSA_2048`)*
- 3 072 bits RSA (`RSA_3072`)
- 4 096 bits RSA (`RSA_4096`)
- 256 bits ECDSA (`EC_prime256v1`) *
- 384 bits ECDSA (`EC_secp384r1`) *
- 521 bits ECDSA (`EC_secp521r1`)

Les clés ECDSA sont plus petites et offrent une sécurité comparable à celle des clés RSA, mais avec une efficacité informatique supérieure. Cependant, l'ECDSA n'est pas pris en charge

par tous les clients du réseau. Le tableau suivant, tiré du NIST, montre le niveau de sécurité représentatif de RSA et ECDSA avec des clés de différentes tailles. Toutes les valeurs sont exprimées en bits.

Comparaison de la sécurité des algorithmes et des clés

Niveau de sécurité	Taille de clé RSA	Taille de clé ECDSA
128	3072	256
192	7680	384
256	15360	512

La force de sécurité, comprise comme une puissance de 2, est liée au nombre de suppositions nécessaires pour casser le chiffrement. Par exemple, une clé RSA de 3 072 bits et une clé ECDSA de 256 bits peuvent être récupérées avec un maximum de 2^{128} suppositions.

Pour obtenir des informations qui vous aideront à choisir un algorithme, consultez le billet de AWS blog Comment évaluer et utiliser les certificats ECDSA dans. AWS Certificate Manager

> **Important**
>
> Notez que les services intégrés autorisent uniquement les algorithmes et tailles de clés qu'ils prennent en charge pour les associer à leurs ressources. De plus, leur prise en charge diffère selon que le certificat est importé dans IAM ou dans ACM. Pour plus d'informations, consultez la documentation pour chaque service.
>
> - Pour Elastic Load Balancing, consultez Écouteurs HTTPS pour votre instance d'Application Load Balancer.
> - Pour CloudFront, voir Protocoles et chiffrements SSL/TLS pris en charge.

Punycode

Les exigences Punycode suivantes relatives aux noms de domaine internationalisés doivent être remplies :

1. Les noms de domaine commençant par le modèle « <character><character>-- » doivent correspondre à « xn-- ».

2. Les noms de domaine commençant par « xn-- » doivent également être des noms de domaine internationalisés valides.

Exemples de Punycode

Nom de domaine	Remplit #1	Remplit #2	Autoris	Remarque
example.com	N/A	s/o	✓	Ne commence pas par « <characte r><character>-- »
a--exampl e.com	N/A	s/o	✓	Ne commence pas par « <characte r><character>-- »
abc--exam ple.com	N/A	s/o	✓	Ne commence pas par « <characte r><character>-- »
xn--xyz.com	Oui	Oui	✓	Nom de domaine internationalisé valide (se résout sur 简.com)
xn--examp le.com	Oui	Non	✗	Nom de domaine internationalisé non valide
ab--examp le.com	Non	Non	✗	Doit commencer par « xn-- »

Exceptions

Notez ce qui suit :

- ACM ne fournit pas de certificats de validation étendue (EV) ou de certificats de validation d'organisation (OV).
- Les certificats fournis par ACM s'appliquent uniquement aux protocoles SSL/TLS.
- Vous ne pouvez pas utiliser de certificats ACM pour le chiffrement de courriels.
- Pour le moment, ACM ne vous permet pas de refuser le renouvellement géré des certificats ACM. De plus, le renouvellement géré n'est pas disponible pour les certificats que vous importez dans ACM.

- Vous ne pouvez pas demander de certificats pour les noms de domaine qui sont la propriété d'Amazon, par exemple ceux qui se terminent par amazonaws.com, cloudfront.net ou elasticbeanstalk.com.
- Vous ne pouvez pas télécharger la clé privée pour un certificat ACM.
- Vous ne pouvez pas installer des certificats ACM directement sur votre site web ou application Amazon Elastic Compute Cloud (Amazon EC2). Toutefois, vous pouvez utiliser votre certificat avec n'importe quel service intégré. Pour plus d'informations, consultez Services intégrés à AWS Certificate Manager.

Régions prises en charge

Consultez Régions et points de terminaison AWS dans le Références générales AWS ou le Tableau des régions AWS pour voir la disponibilité régionale d'ACM.

Les certificats d'ACM sont des ressources régionales. Pour utiliser un certificat avec Elastic Load Balancing pour le même nom de domaine complet (FQDN) ou le même ensemble de FQDN dans plusieurs AWS régions, vous devez demander ou importer un certificat pour chaque région. Pour les certificats fournis par ACM, cela signifie que vous devez revalider chaque nom de domaine dans le certificat pour chaque région. Vous ne pouvez pas copier de certificat entre les régions.

Pour utiliser un certificat ACM avec Amazon CloudFront, vous devez demander ou importer le certificat dans la région USA Est (Virginie du Nord). Les certificats ACM de cette région associés à une CloudFront distribution sont distribués à tous les emplacements géographiques configurés pour cette distribution.

Services intégrés à AWS Certificate Manager

AWS Certificate Manager prend en charge un nombre croissant de AWS services. Vous ne pouvez pas installer votre certificat ACM ou votre Autorité de certification privée AWS certificat privé directement sur le site Web ou l'application que vous AWS utilisez.

> **Note**
>
> Les certificats ACM publics peuvent être installés sur des instances Amazon EC2 connectées à une enclave Nitro, mais pas à d'autres instances Amazon EC2. Pour plus d'informations sur la configuration d'un serveur web autonome sur une instance Amazon EC2 non connectée à

une enclave Nitro, consultez Tutoriel : Installation d'un serveur web LAMP sur Amazon Linux 2 ou Tutoriel : Installation d'un serveur web LAMP avec une AMI Amazon Linux.

Les certificats ACM sont pris en charge par les services suivants :

Elastic Load Balancing

Elastic Load Balancing distribue automatiquement le trafic applicatif entrant sur plusieurs instances Amazon EC2. Il détecte les instances non saines et redirige le trafic vers des instances saines jusqu'à ce que les instances non saines soient restaurées. Elastic Load Balancing met automatiquement à l'échelle la capacité de traitement des demandes en réponse au trafic entrant. Pour plus d'informations sur l'équilibrage de charge, consultez Guide de l'utilisateur Elastic Load Balancing.

En général, pour servir du contenu sécurisé via SSL/TLS, les équilibreurs de charge requièrent que les certificats SSL/TLS soient installés sur l'équilibreur de charge ou l'instance Amazon EC2 principale. ACM est intégré à Elastic Load Balancing pour déployer les certificats ACM sur l'équilibreur de charge. Pour plus d'informations, consultez Création d'une instance d'Application Load Balancer.

Amazon CloudFront

Amazon CloudFront est un service Web qui accélère la distribution de votre contenu Web dynamique et statique aux utilisateurs finaux en diffusant votre contenu à partir d'un réseau mondial de sites périphériques. Lorsqu'un utilisateur final demande du contenu que vous diffusez CloudFront, il est redirigé vers l'emplacement périphérique offrant la latence la plus faible. Le contenu est ainsi remis avec le meilleur niveau de performance possible. Si le contenu se trouve actuellement à cet emplacement périphérique, CloudFront diffusez-le immédiatement. Si le contenu ne se trouve pas actuellement à cet emplacement périphérique, il est CloudFront extrait du compartiment Amazon S3 ou du serveur Web que vous avez identifié comme la source de contenu définitive. Pour plus d'informations CloudFront, consultez le manuel Amazon CloudFront Developer Guide.

Pour diffuser du contenu sécurisé via SSL/TLS, CloudFront les certificats SSL/TLS doivent être installés sur la CloudFront distribution ou sur la source de contenu sauvegardée. ACM est intégré CloudFront pour déployer les certificats ACM sur la CloudFront distribution. Pour plus d'informations, consultez Obtention d'un certificat SSL/TLS.

> **Note**
>
> Pour utiliser un certificat ACM avec CloudFront, vous devez demander ou importer le certificat dans la région USA Est (Virginie du Nord).

Amazon Cognito

Amazon Cognito assure l'authentification, l'autorisation et la gestion des utilisateurs pour vos applications web et mobiles. Les utilisateurs peuvent se connecter directement à l'aide de vos Compte AWS informations d'identification ou par le biais d'un tiers tel que Facebook, Amazon, Google ou Apple. Pour plus d'informations sur Amazon Cognito, consultez le guide Amazon Cognito Developer.

Lorsque vous configurez un groupe d'utilisateurs Cognito pour utiliser un CloudFront proxy Amazon, vous CloudFront pouvez mettre en place un certificat ACM pour sécuriser le domaine personnalisé. Dans ce cas, sachez que vous devez supprimer l'association du certificat avec CloudFront avant de pouvoir le supprimer.

AWS Elastic Beanstalk

Elastic Beanstalk vous aide à déployer et à gérer des applications AWS dans le cloud sans vous soucier de l'infrastructure qui exécute ces applications. AWS Elastic Beanstalk réduit la complexité de gestion. Il vous suffit de charger votre application, et Elastic Beanstalk gère automatiquement les informations du dimensionnement des capacités, de la répartition de charge, de la mise à l'échelle et de la surveillance de l'état de l'application. Elastic Beanstalk utilise le service Elastic Load Balancing pour créer un équilibreur de charge. Pour plus d'informations sur Elastic Beanstalk, consultez le Guide du développeur AWS Elastic Beanstalk.

Pour choisir un certificat, vous devez configurer l'équilibreur de charge de votre application dans la console Elastic Beanstalk. Pour plus d'informations, consultez Configuration de l'équilibreur de charge de votre environnement Elastic Beanstalk pour mettre la connexion HTTPS hors service.

AWS App Runner

App Runner est un AWS service qui fournit un moyen rapide, simple et économique de déployer directement à partir du code source ou d'une image de conteneur vers une application Web évolutive et sécurisée dans le AWS cloud. Vous n'avez pas besoin d'apprendre de nouvelles technologies, de choisir le service informatique à utiliser ou de savoir comment approvisionner et configurer les AWS ressources. Pour plus d'informations sur App Runner, consultez Guide du développeur AWS App Runner.

Lorsque vous associez des noms de domaine personnalisés à votre service App Runner, celui-ci crée en interne des certificats qui suivent la validité du domaine. Ces certificats sont stockés dans ACM. App Runner les conserve sept jours après la dissociation d'un domaine de votre service ou après la suppression du service. L'ensemble de ce processus est automatisé et vous n'avez pas besoin d'ajouter ou de gérer vous-même des certificats. Pour plus d'informations, consultez Gestion des noms de domaine personnalisés pour un service App Runner dans le Guide du développeur AWS App Runner .

Amazon API Gateway

Avec la multiplication des appareils mobiles et la croissance de l'Internet des objets (IoT), il est de plus en plus courant de créer des API vous permettant d'accéder aux données et d'interagir avec les systèmes principaux sur AWS. Vous pouvez utiliser API Gateway pour publier, gérer, surveiller et sécuriser vos API. Après avoir déployé votre API sur API Gateway, vous pouvez configurer un nom de domaine personnalisé pour simplifier l'accès à celui-ci. Pour configurer un nom de domaine personnalisé, vous devez fournir un certificat SSL/TLS. Vous pouvez utiliser ACM pour générer ou importer le certificat. Pour plus d'informations sur Amazon API Gateway, consultez le guide Amazon API Gateway Developer.

AWS Enclaves Nitro

AWS Nitro Enclaves est une fonctionnalité d'Amazon EC2 qui vous permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances Amazon EC2. Les enclaves sont des machines virtuelles distinctes, renforcées et soumises à de fortes contraintes. Elles ne fournissent qu'une connectivité locale sécurisée par socket avec leur instance parente. Elles ne disposent pas de stockage persistant, d'accès interactif ou de réseau externe. Les utilisateurs ne peuvent se connecter à une enclave via SSH, et les processus, applications ou utilisateurs (y compris racine ou admin) de l'instance parente n'ont pas accès aux données et applications de l'enclave.

Les instances EC2 connectées à Nitro Enclaves prennent en charge les certificats ACM. Pour plus d'informations, consultez AWS Certificate Manager pour Nitro Enclaves.

> **Note**
>
> Vous ne pouvez pas associer de certificats ACM à une instance EC2 qui n'est pas connectée à une enclave Nitro.

AWS CloudFormation

AWS CloudFormation vous aide à modéliser et à configurer vos ressources Amazon Web Services. Vous créez un modèle qui décrit les AWS ressources que vous souhaitez utiliser, telles que Elastic Load Balancing ou API Gateway. Ensuite, AWS CloudFormation s'occupe pour vous de la mise en service et de la configuration de ces ressources. Vous n'avez pas besoin de créer et de configurer AWS des ressources individuellement et de déterminer ce qui dépend de quoi ; il AWS CloudFormation gère tout cela. Les certificats ACM sont inclus en tant que ressource modèle, ce qui signifie que vous AWS CloudFormation pouvez demander des certificats ACM que vous pouvez utiliser avec AWS des services pour activer des connexions sécurisées. En outre, les certificats ACM sont inclus dans de nombreuses AWS ressources que vous pouvez configurer. AWS CloudFormation

Pour des informations générales à ce sujet CloudFormation, consultez le guide de AWS CloudFormation l'utilisateur. Pour plus d'informations sur les ressources ACM prises en charge par CloudFormation, consultez AWS::CertificateManager::Certificate.

Grâce à la puissante automatisation fournie par AWS CloudFormation, il est facile de dépasser votre quota de certificats, en particulier avec les nouveaux AWS comptes. Nous vous recommandons de suivre les meilleures pratiques d'ACM pour AWS CloudFormation.

> **Note**
>
> Si vous créez un certificat ACM avec AWS CloudFormation, la AWS CloudFormation pile reste dans l'état CREATE_IN_PROGRESS. Toutes les autres opérations de pile sont retardées jusqu'à ce que vous donniez suite suivant les instructions indiquées dans le courriel de validation pour le certificat. Pour plus d'informations, consultez La ressource n'a pas pu se stabiliser lors d'une opération de création, de mise à jour ou de suppression de pile.

AWS Amplify

Amplify est un ensemble d'outils et de fonctionnalités spécialement conçus qui permettent aux développeurs Web et mobiles frontaux de créer rapidement et facilement des applications complètes. AWS Amplify propose deux services : Amplify Hosting et Amplify Studio. Amplify Hosting fournit un flux de travail basé sur git pour héberger des piles complètes d'applications Web sans serveur avec déploiement continu. Amplify Studio est un environnement de développement visuel qui simplifie la création de piles complètes d'applications Web et mobiles

évolutives. Utilisez Studio pour créer votre interface utilisateur frontale à l'aide d'un ensemble de composants d' ready-to-use interface utilisateur, créer un backend d'application, puis connecter les deux ensemble. Pour plus d'informations sur Amplify, consultez le AWS Amplify guide de l'utilisateur.

Si vous connectez un domaine personnalisé à votre application, la console Amplify émet un certificat ACM pour le sécuriser.

Amazon OpenSearch Service

Amazon OpenSearch Service est un moteur de recherche et d'analyse destiné à des cas d'utilisation tels que l'analyse des journaux, la surveillance des applications en temps réel et l'analyse des flux de clics. Pour plus d'informations, consultez le manuel Amazon OpenSearch Service Developer Guide.

Lorsque vous créez un cluster de OpenSearch services contenant un domaine et un point de terminaison personnalisés, vous pouvez utiliser ACM pour doter l'Application Load Balancer associé d'un certificat.

AWS Network Firewall

AWS Network Firewall est un service géré qui facilite le déploiement des protections réseau essentielles pour tous vos Amazon Virtual Private Clouds (VPC). Pour plus d'informations sur Network Firewall, consultez le Guide du développeur AWS Network Firewall.

Le pare-feu Network Firewall s'intègre à ACM pour l'inspection TLS. Si vous utilisez l'inspection TLS dans Network Firewall, vous devez configurer un certificat ACM pour le déchiffrement et le rechiffrement du trafic SSL/TLS passant par votre pare-feu. Pour plus d'informations sur la façon dont Network Firewall fonctionne avec ACM pour l'inspection TLS, consultez la section Exigences relatives à l'utilisation de certificats SSL/TLS avec des configurations d'inspection TLS dans le Guide du développeur AWS Network Firewall .

Sceaux de site et sceaux de confiance

Amazon ne fournit pas de sceau de site et n'autorise pas que sa marque soit utilisée à ce titre :

- AWS Certificate Manager (ACM) ne fournit pas de sceau de site sécurisé que vous pouvez utiliser sur votre site Web. Si vous voulez utiliser un sceau de site, vous pouvez en obtenir un auprès d'un fournisseur tiers. Nous vous conseillons de choisir un fournisseur qui évalue et fait valoir la sécurité de votre site web et de vos pratiques métier.

- Amazon n'autorise pas à utiliser sa marque ou son logo comme insigne de certification, sceau de site ou sceau de confiance. Ce type de sceau et d'insigne peut être copié sur les sites qui n'utilisent pas le service ACM, et peut être utilisé de manière inappropriée pour établir une approbation sous de faux prétextes. Pour protéger nos clients et la réputation d'Amazon, nous n'autorisons pas à utiliser notre marque ni notre logo de cette manière.

Quotas

Les quotas de service AWS Certificate Manager (ACM) suivants s'appliquent à chaque AWS région et à chaque AWS compte.

Pour savoir quels quotas peuvent être ajustés, consultez le tableau des quotas ACM dans le AWS Guide de référence générale. Pour demander des augmentations de quota, créez un dossier au Centre AWS Support.

Quotas généraux

Élément	Quota par défaut
Nombre de certificats ACM Les certificats qui ont expiré et qui ont été révoqués sont toujours pris en compte dans ce total. Les certificats signés par une autorité de certification Autorité de certification privée AWS ne sont pas pris en compte dans ce total.	2500
Nombre de certificats ACM par an (au cours des 365 derniers jours) Vous pouvez demander jusqu'à deux fois votre quota de certificats ACM par année, région et compte. Par exemple, si votre quota est de 2 500, vous pouvez demander jusqu'à 5 000 certificats ACM par an dans une région et un compte donnés. Vous ne pouvez obtenir que	Deux fois le quota de votre compte

Élément	Quota par défaut
2 500 certificats à la fois. Si vous demandez 5 000 certificats en un an, vous devez en supprimer 2 500 au cours de l'année pour rester dans le quota. Si vous avez besoin de plus de 2 500 certificats à la fois, vous devez contacter le Centre AWS Support. Les certificats signés par une autorité de certification Autorité de certification privée AWS ne sont pas pris en compte dans ce total.	
Nombre de certificats importés	2 500
Nombre de certificats importés par an (au cours des 365 derniers jours)	Deux fois le quota de votre compte

Élément	Quota par défaut
Nombre de noms de domaine par certificat ACM Le quota par défaut est de 10 noms de domaine par certificat ACM. Votre quota peut être plus élevé. Le premier nom de domaine que vous envoyez est inclus en tant que nom commun d'objet (CN) du certificat. Tous les noms sont inclus dans l'extension Subject Alternative Name. Vous pouvez demander jusqu'à 100 noms de domaine. Pour demander une augmentation de votre quota, créez une demande dans la console Service Quotas pour le service ACM. Cependant, avant de créer une demande, assurez-vous de bien comprendre que l'ajout de noms de domaine peut augmenter votre charge de travail administratif si vous utilisez la validation par courriel. Pour de plus amples informations, consultez Validation de domaine. Le quota appliqué au nombre de noms de domaine par certificat ACM s'applique uniquement aux certificats fournis par ACM. Ce quota ne s'applique pas aux certificats que vous importez dans ACM. Les sections suivantes s'appliquent uniquement aux certificats ACM.	10

Élément	Quota par défaut
Nombre d'autorités de certification privées ACM est intégré à AWS Private Certificate Authority (Autorité de certification privée AWS). Vous pouvez utiliser la console ACM ou l'API ACM pour demander des certificats privés à une autorité de certification privée (CA) existante hébergée par. AWS CLI Autorité de certification privée AWS Ces certificats sont gérés au sein de l'environnement ACM et présentent les mêmes restrictions que les certificats publics émis par ACM. Pour plus d'informations, consultez Demande de certificat privé PKI. Vous pouvez également émettre des certificats privés à l'aide du Autorité de certification privée AWS service autonome. Pour plus d'informations, consultez Émission d'un certificat d'entité finale privé. Une autorité de certification privée qui a été supprimée est prise en compte pour votre quota jusqu'à la fin de sa période de restauration. Pour plus d'informations, consultez Suppression de votre autorité de certification privée.	200
Nombre de certificats privés par autorité de certification (durée de vie)	1 000 000

Quotas de taux de l'API

Les quotas suivants s'appliquent à l'API ACM pour chaque région et chaque compte. ACM limite les demandes d'API à différents quotas en fonction de l'opération d'API. La limitation signifie qu'ACM rejette une demande normalement valide car elle dépasse le quota de l'opération en termes de nombre de demandes par seconde. Lorsqu'une demande est limitée, ACM renvoie une erreur

`ThrottlingException`. Le tableau suivant répertorie chaque opération d'API et le quota à partir duquel ACM limite les demandes pour cette opération.

> **Note**
>
> Outre les actions d'API répertoriées dans le tableau ci-dessous, ACM peut également appeler `IssueCertificate` l'action externe à partir de Autorité de certification privée AWS. Pour obtenir des informations sur les quotas up-to-date tarifaires`IssueCertificate`, consultez les points de terminaison et les quotas pour Autorité de certification privée AWS.

equests-per-second Quota R pour chaque opération d'API ACM

Appel d'API	Demandes par seconde
`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

Appel d'API	Demandes par seconde
`ResendValidationEmail`	1
`UpdateCertificateOptions`	5

Pour plus d'informations, veuillez consulter AWS Certificate Manager Référence d'API .

Tarification pour AWS Certificate Manager

Vous n'avez pas de frais supplémentaires à régler pour des certificats SSL/TLS que vous gérez avec AWS Certificate Manager. Vous ne payez que pour les AWS ressources que vous créez pour exécuter votre site Web ou votre application. Pour obtenir les dernières informations sur les tarifs d'ACM, consultez la page AWS Certificate Manager de tarification des services sur le AWS site Web.

Sécurité dans AWS Certificate Manager

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Certificate Manager, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Certificate Manager (ACM). Les rubriques suivantes expliquent comment configurer ACM pour qu'il réponde à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources ACM.

Rubriques

Protection des données dans AWS Certificate Manager

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Certificate Manager. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec ACM ou une autre entreprise à Services AWS l'aide de la console, de l'API ou des AWS SDK. AWS CLI Toutes les données

que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Sécurité des clés privées des certificats

Lorsque vous demandez un certificat public, AWS Certificate Manager (ACM) génère une paire de clés publique/privée. Pour les imported certificates (certificats importés), vous générez la paire de clés. La clé publique devient partie intégrante du certificat. ACM stocke le certificat et la clé privée correspondante, et utilise AWS Key Management Service (AWS KMS) pour protéger la clé privée. Voici comment cela fonctionne :

1. La première fois que vous demandez ou importez un certificat dans une AWS région, ACM crée un certificat géré AWS KMS key avec l'alias aws/acm. Cette clé KMS est unique dans chaque AWS compte et dans chaque AWS région.
2. ACM utilise cette clé KMS pour chiffrer la clé privée du certificat. ACM stocke une version chiffrée de la clé privée ; il ne la stocke pas en texte brut. ACM utilise la même clé KMS pour chiffrer les clés privées de tous les certificats d'un AWS compte et d'une région spécifiques AWS .
3. Lorsque vous associez le certificat à un service intégré à AWS Certificate Manager, ACM envoie le certificat et la clé privée chiffrée à ce service. Une autorisation est également créée pour permettre au service d'utiliser la clé KMS pour déchiffrer la clé privée du certificat. AWS KMS Pour plus d'informations sur les octrois, consultez Utilisation d'octrois dans le AWS Key Management Service Guide du développeur. Pour plus d'informations sur les services pris en charge par ACM, consultez Services intégrés à AWS Certificate Manager.

   > **Note**
   >
   > Vous avez le contrôle de la AWS KMS subvention créée automatiquement. Si vous le supprimez pour une raison quelconque, vous perdez la fonctionnalité ACM pour le service intégré.

4. Les services intégrés utilisent la clé KMS pour déchiffrer la clé privée. Le service utilise ensuite le certificat et la clé privée déchiffrée (texte brut) pour établir des canaux de communication sécurisés (sessions SSL/TLS) avec ses clients.

5. Lorsque le certificat est dissocié d'un service intégré, la subvention créée à l'étape 3 est retirée. Cela signifie que le service ne peut plus utiliser la clé KMS pour déchiffrer la clé privée du certificat.

Identity and Access Management pour AWS Certificate Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (dotées d'autorisations) à utiliser des ressources ACM. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans ACM.

Utilisateur du service : si vous utilisez le service ACM pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctions ACM pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une

fonctionnalité dans ACM, consultez Résolution des problèmes AWS Certificate Manager d'identité et d'accès.

Administrateur du service : si vous êtes le responsable des ressources ACM de votre entreprise, vous bénéficiez probablement d'un accès total à ACM. Votre responsabilité est de déterminer les fonctionnalités ainsi que les ressources ACM auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec ACM, veuillez consulter Comment AWS Certificate Manager fonctionne avec IAM.

Administrateur IAM : si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des stratégies pour gérer l'accès à ACM. Pour voir des exemples de stratégies basées sur l'identité ACM que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour AWS Certificate Manager.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour

signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour

obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour

obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés

à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui

autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Certificate Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à ACM, découvrez les fonctionnalités IAM que vous pouvez utiliser avec ACM.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Certificate Manager

Fonction IAM	Prise en charge d'ACM
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont ACM et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour ACM

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de stratégies basées sur l'identité pour ACM

Pour voir des exemples de stratégies basées sur l'identité ACM, consultez Exemples de politiques basées sur l'identité pour AWS Certificate Manager.

Stratégies basées sur une ressource dans ACM

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour

contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions de stratégie pour ACM

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour afficher la liste des actions ACM, consultez Actions définies par AWS Certificate Manager dans la Référence de l'autorisation de service.

Les actions de stratégie dans ACM utilisent le préfixe suivant avant l'action :

```
acm
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples de stratégies basées sur l'identité ACM, consultez Exemples de politiques basées sur l'identité pour AWS Certificate Manager.

Ressources de politique pour ACM

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour afficher la liste des types de ressources ACM et leurs ARN, consultez Ressources définies par AWS Certificate Manager dans la Référence de l'autorisation de service. Pour savoir grâce à

quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Certificate Manager.

Pour voir des exemples de stratégies basées sur l'identité ACM, consultez Exemples de politiques basées sur l'identité pour AWS Certificate Manager.

Clés de condition de stratégie pour ACM

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition ACM, consultez Clés de condition pour AWS Certificate Manager dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et

ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Certificate Manager.

Pour voir des exemples de stratégies basées sur l'identité ACM, consultez Exemples de politiques basées sur l'identité pour AWS Certificate Manager.

ACL dans ACM

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec ACM

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation des informations d'identification temporaires avec ACM

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales entre services pour ACM

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour ACM

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'une fonction du service peut altérer la fonctionnalité d'ACM. Ne modifiez des fonctions du service que quand ACM vous le conseille.

Rôles liés à un service pour ACM

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS Certificate Manager

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources ACM. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ACM, y compris le format des ARN pour chacun des types de ressources, veuillez consulter la rubrique Actions, ressources et clés de condition pour AWS Certificate Manager dans la Référence de l'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources ACM dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire

davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console ACM

Pour accéder à la AWS Certificate Manager console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des

ressources ACM de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console ACM, associez également la politique *AWSCertificateManagerReadOnly* AWS gérée par ACM aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Établissement de la liste des certificats

La politique suivante permet à un utilisateur d'établir la liste de tous les certificats ACM figurant dans le compte de l'utilisateur.

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

> **Note**
>
> Cette autorisation est requise pour que les certificats ACM apparaissent dans Elastic Load Balancing et les CloudFront consoles.

Récupération d'un certificat

La politique suivante permet à un utilisateur de récupérer un certificat ACM spécifique.

```
{
            "Version":"2012-10-17",
            "Statement":{
            "Effect":"Allow",
            "Action":"acm:GetCertificate",
```

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

Importation d'un certificat

La politique suivante permet à un utilisateur d'importer un certificat.

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

Suppression d'un certificat

La politique suivante permet à un utilisateur de supprimer un certificat ACM spécifique.

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

Autorisations d'API ACM : référence sur les actions et ressources

Vous pouvez utiliser le tableau ci-dessous comme référence lorsque vous configurez le contrôle d'accès et que vous écrivez des stratégies d'autorisation que vous pouvez attacher à un utilisateur ou un rôle IAM. La première colonne du tableau répertorie chaque opération d'API AWS Certificate Manager. Vous indiquez les actions dans l'élément `Action` d'une politique. Les autres colonnes fournissent les informations supplémentaires suivantes :

Vous pouvez utiliser les éléments de politique IAM dans vos politiques ACM pour exprimer des conditions. Pour en obtenir la liste complète, consultez Clés disponibles dans le Guide de l'utilisateur IAM.

> **Note**
>
> Pour indiquer une action, utilisez le préfixe `acm:` suivi du nom de l'opération d'API (par exemple, `acm:RequestCertificate`).

Opérations et autorisations d'API ACM

Opérations d'API ACM	Autorisations requises (opérations d'API)	Ressources
AddTagsToCertificate (Ajouter des balises au certificat)	`acm:AddTagsToCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/` *certificate_ID*
DeleteCertificate (Supprimer un certificat)	`acm:DeleteCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/` *certificate_ID*
DescribeCertificate (Décrire un certificat)	`acm:DescribeCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/` *certificate_ID*
ExportCertificate (Exporter un certificat)	`acm:ExportCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/` *certificate_ID*
GetAccountConfiguration (Obtenir la configuration du compte)	`acm:GetAccountConfiguration`	`*`
GetCertificate (Obtenir un certificat)	`acm:GetCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/` *certificate_ID*
ImportCertificate (Importer un certificat)	`acm:ImportCertificate`	`arn:aws:acm:` *region*`:`*account*`:certificate/*`

Opérations d'API ACM	Autorisations requises (opérations d'API)	Ressources
		or *
ListCertificates (Liste des certificats)	acm:ListCertificates	*
ListTagsForCertificate (Liste des balises pour le certificat)	acm:ListTagsForCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
PutAccountConfiguration (Mettre la configuration du compte)	acm:PutAccountConfiguration	*
RemoveTagsFromCertificate (Supprimer les balises du certificat)	acm:RemoveTagsFromCertificate	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
RequestCertificate (Demander un certificat)	acm:RequestCertificate	arn:aws:acm: *region*:*account*:certificate/* or *
ResendValidationEmail (Renvoyer l'e-mail de validation)	acm:ResendValidationEmail	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*
UpdateCertificateOptions (Mettre à jour les options du certificat)	acm:UpdateCertificateOptions	arn:aws:acm: *region*:*account*:certificate/ *certificate_ID*

Politiques AWS gérées pour AWS Certificate Manager

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWSCertificateManagerReadOnly

Cette politique fournit un accès en lecture seule aux certificats ACM. Elle permet aux utilisateurs de décrire des certificats ACM, de les répertorier sous forme de liste et de les extraire.

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

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

Pour afficher cette politique gérée par AWS dans la console, accédez à https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly.

AWSCertificateManagerFullAccess

Cette politique fournit un accès complet à toutes les actions et ressources 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*"
```

```
    }
    ]
}
```

Pour afficher cette politique gérée par AWS dans la console, accédez à https://console.aws.amazon.com/iam/home#policies/arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess.

Mises à jour ACM des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour ACM depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la page ACM Historique du document.

Modification	Description	Date
Ajout de la prise en charge de `GetAccountConfiguration` pour la politique AWSCertificateManagerReadOnly.	La politique `AWSCertificateManagerReadOnly` inclut désormais l'autorisation d'appeler l'action d'API `GetAccountConfiguration` .	3 mars 2021
ACM commence à suivre les modifications	ACM commence à suivre les modifications pour les politiques gérées par AWS.	3 mars 2021

Utilisation de clés de condition avec ACM

AWS Certificate Manager utilise les clés de condition AWS Identity and Access Management (IAM) pour limiter l'accès aux demandes de certificats. Grâce aux clés de condition issues des politiques IAM ou des politiques de contrôle des services (SCP), vous pouvez créer des demandes de certificat conformes aux directives de votre organisation.

> **Note**
>
> Combinez les clés de condition ACM avec les clés de condition globales AWS tels que `aws:PrincipalArn` pour restreindre davantage les actions à des utilisateurs ou à des rôles spécifiques.

Conditions prises en charge pour ACM

Opérations de l'API ACM et conditions prises en charge

Clé de condition	Opérations de l'API ACM prises en charge	Type	Description
`acm:ValidationMethod`	RequestCertificate (Demander un certificat)	Chaîne (`EMAIL`, `DNS`)	Filtrer les demandes en fonction de la méthode de validation de l'ACM
`acm:DomainNames`	RequestCertificate (Demander un certificat)	ArrayOfString	Filtre basé sur les noms de domaine dans la requête ACM
`acm:KeyAlgorithm`	RequestCertificate (Demander un certificat)	Chaîne	Filtrer les demandes en fonction de l'algorithme et de la taille de la clé ACM
`acm:CertificateTransparencyLogging`	RequestCertificate (Demander un certificat)	Chaîne (`ENABLED`, `DISABLED`)	Filtrer les demandes en fonction des préférences de journalisation de la transparence des certificats ACM
`acm:CertificateAuthority`	RequestCertificate (Demander un certificat)	ARN	Filtrer les demandes en fonction des autorités de certifica

Clé de condition	Opérations de l'API ACM prises en charge	Type	Description
			tion dans la requête ACM

Exemple 1 : restreindre la méthode de validation

La stratégie suivante refuse les nouvelles demandes de certificat à l'aide de la méthode de validation des e-mails, à l'exception d'une requête effectuée à l'aide du rôle `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"]
            }
        }
    }
}
```

Exemple 2 : empêcher les domaines génériques

La stratégie suivante refuse toute nouvelle requête de certificat ACM qui utilise des domaines génériques.

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

```
        "Effect":"Deny",
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition": {
            "ForAnyValue:StringLike": {
                "acm:DomainNames": [
                    "${*}.*"
                ]
            }
        }
    }
}
```

Exemple 3 : restreindre les domaines de certificats

La stratégie suivante refuse toute nouvelle requête de certificat ACM pour les domaines qui ne se terminent pas par `*.amazonaws.com`

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

La stratégie peut également être restreinte à des sous-domaines spécifiques. Cette stratégie n'autorise que les requêtes pour lesquelles chaque domaine correspond à au moins un des noms de domaine conditionnels.

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

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

Exemple 4 : restreindre les clés d'algorithme

La stratégie suivante utilise la clé de condition `StringNotLike` pour autoriser uniquement les certificats demandés avec l'algorithme de clé ECDSA 384 bits (`EC_secp384r1`).

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

La stratégie suivante utilise la clé de condition `StringLike` et la correspondance `*` générique pour empêcher les requêtes de nouveaux certificats dans ACM avec n'importe quel algorithme clé `RSA`.

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

```
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "StringLike" : {
                "acm:KeyAlgorithm":"RSA*"
            }
        }
    }
}
```

Exemple 5 : restreindre l'autorité de certification

La stratégie suivante n'autorise que les demandes de certificats privés utilisant l'ARN de l'autorité de certification privée (PCA) fournie.

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

Cette politique utilise la condition `acm:CertificateAuthority` pour n'autoriser que les demandes de certificats publiquement fiables émis par Amazon Trust Services. Le fait de définir l'ARN de l'autorité de certification sur `false` empêche les requêtes de certificats privés de la part de PCA.

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

```
        "Action":"acm:RequestCertificate",
        "Resource":"*",
        "Condition":{
            "Null" : {
                "acm:CertificateAuthority":"false"
            }
        }
    }
}
```

Utilisation d'un rôle lié à un service (SLR) avec ACM

AWS Certificate Manager utilise un rôle lié à un service AWS Identity and Access Management (IAM) pour permettre le renouvellement automatique des certificats ACM gérés. Un rôle lié à un service (SLR) est un rôle IAM directement associé au service ACM. Les rôles SLR sont prédéfinis par ACM et comprennent toutes les autorisations dont le service a besoin pour appeler d'autres services AWS en votre nom.

Le rôle SLR simplifie la configuration d'ACM, car vous n'avez pas besoin d'ajouter manuellement les autorisations nécessaires à la signature de certificats sans assistance. ACM définit les autorisations de son rôle SLR et, sauf définition contraire, il est le seul à pouvoir endosser ce rôle. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les SLR, consultez AWS Services qui fonctionnent avec IAM et recherchez les services pour lesquels la mention Oui apparaît dans la colonne Rôle lié à un service. Choisissez une mention Oui disponible sous forme de lien pour consulter la documentation SLR du service correspondant.

Autorisations SLR pour ACM

ACM utilise un rôle SLR nommé Amazon Certificate Manager Service Role Policy.

Le AWSServiceRoleForCertificateManager SLR fait confiance aux services suivants pour assumer ce rôle :

- `acm.amazonaws.com`

La politique d'autorisations liée au rôle permet à ACM d'effectuer les actions suivantes sur les ressources spécifiées :

- Actions : `acm-pca:IssueCertificate`, `acm-pca:GetCertificate` sur "*"

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, de modifier ou de supprimer un rôle SLR. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

> **Important**
>
> ACM peut vous avertir qu'il ne peut pas déterminer si un rôle SLR existe sur votre compte. Si l'autorisation `iam:GetRole` requise a déjà été accordée au rôle SLR ACM pour votre compte, l'alerte ne se reproduira pas après la création du rôle SLR. Si elle se reproduit, vous ou votre administrateur de compte devrez peut-être accorder l'autorisation `iam:GetRole` à ACM, ou associer votre compte à la politique `AWSCertificateManagerFullAccess` gérée par ACM.

Création du rôle SLR pour ACM

Vous n'avez pas besoin de créer manuellement le rôle SLR utilisé par ACM. Lorsque vous émettez un certificat ACM à l'aide de AWS Management Console, de AWS CLI, ou de l' AWS API, ACM crée le SLR pour vous la première fois que vous choisissez une autorité de certification privée pour signer votre certificat.

Si vous recevez des messages indiquant qu'ACM ne peut pas déterminer si un reflex existe sur votre compte, cela signifie peut-être que votre compte n'a pas accordé l'autorisation de lecture requise. Autorité de certification privée AWS Cela n'empêchera pas l'installation du rôle SLR, et vous pourrez toujours émettre des certificats, mais ACM ne pourra pas renouveler automatiquement les certificats tant que vous n'aurez pas résolu le problème. Pour de plus amples informations, consultez Problèmes liés au rôle lié à un service (SLR) ACM.

> **Important**
>
> Ce rôle SLR peut apparaître dans votre compte si vous avez effectué dans un autre service une action qui utilise les fonctions prises en charge par ce rôle. De plus, si vous utilisiez le

service ACM avant le 1er janvier 2017, date à laquelle il a commencé à prendre en charge les reflex, ACM a créé le AWSServiceRoleForCertificateManager rôle dans votre compte. Pour plus d'informations, consultez A New Role Appeared in My IAM Account (Un nouveau rôle est apparu dans mon compte IAM).

Si vous supprimez ce rôle SLR et que vous devez ensuite le recréer, vous pouvez utiliser l'une des méthodes suivantes :

- Dans la console IAM, choisissez Role, Create role, Certificate Manager pour créer un nouveau rôle avec le cas CertificateManagerServiceRolePolicyd'utilisation.
- À l'aide de l'API IAM CreateServiceLinkedRoleou de la AWS CLI commande correspondante create-service-linked-role, créez un SLR avec le nom du `acm.amazonaws.com` service.

Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Modification du rôle SLR pour ACM

ACM ne vous permet pas de modifier le rôle lié au AWSServiceRoleForCertificateManager service. Après avoir créé un rôle SLR, vous ne pouvez pas modifier son nom, car différentes entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression du rôle SLR pour ACM

Il n'est généralement pas nécessaire de supprimer le AWSServiceRoleForCertificateManager reflex. Toutefois, vous pouvez supprimer le rôle manuellement à l'aide de la console IAM, de l'API AWS CLI ou de l' AWS API. Pour plus d'informations, veuillez consulter Deleting a Service-Linked Role (Suppression d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles SLR ACM

ACM prend en charge l'utilisation des reflex dans toutes les régions où ACM et Autorité de certification privée AWS ACM sont disponibles. Pour de plus amples informations, consultez Regions and EndpointsAWS (Régions et points de terminaison) .

Nom de la région	Identité de la région	Prise en charge dans ACM
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Zurich)	eu-central-2	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Paris)	eu-west-3	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui
AWS GovCloud (US-Ouest)	us-gov-west-1	Oui
AWS GovCloud (USA Est) Est	us-gov-east-1	Oui

Résolution des problèmes AWS Certificate Manager d'identité et d'accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec ACM et IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans ACM

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `acm:`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `acm:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à demander un certificat dans ACM

Si vous recevez cette erreur, c'est que votre administrateur ACM ou PKI a défini des règles qui vous empêchent de demander le certificat dans son état actuel.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM essaie d'utiliser la console pour demander un certificat à l'aide d'options configurées avec un `DENY` par l'administrateur de l'organisation.

```
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
```

Dans ce cas, la requête doit être réitérée d'une manière conforme aux stratégies définies par votre administrateur. Ou bien la politique doit être mise à jour pour permettre de demander le certificat.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à ACM.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans ACM. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources ACM

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ACM prend en charge ces fonctionnalités, consultez Comment AWS Certificate Manager fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Résilience dans AWS Certificate Manager

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Certificate Manager

En tant que service géré, AWS Certificate Manager il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure,

consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à ACM via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Octroi d'un accès programmatif à ACM

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		• Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Bonnes pratiques

Les meilleures pratiques sont des recommandations qui peuvent vous aider à utiliser AWS Certificate Manager (AWS Certificate Manager) de manière plus efficace. Les bonnes pratiques suivantes reposent sur l'expérience réelle de clients actuels d'ACM.

Rubriques

- Séparation au niveau du compte
- AWS CloudFormation
- Épinglage de certificat

- Validation de domaine
- Ajout ou suppression de noms de domaine
- Refus de la journalisation de transparence des certificats
- Allumez AWS CloudTrail

Séparation au niveau du compte

Utilisez la séparation au niveau du compte dans vos politiques pour contrôler qui peut accéder aux certificats au niveau du compte. Conservez vos certificats de production dans des comptes distincts de ceux de vos certificats de test et de développement. Si vous ne pouvez pas utiliser la séparation au niveau du compte, vous pouvez restreindre l'accès à des rôles spécifiques en interdisant toute `kms:CreateGrant` action dans le cadre de vos politiques. Cela limite les rôles d'un compte qui peuvent signer des certificats à un niveau élevé. Pour plus d'informations sur les subventions, y compris la terminologie des subventions, voir Subventions AWS KMS dans le guide du AWS Key Management Service développeur.

Si vous souhaitez un contrôle plus précis que la restriction de l'utilisation `kms:CreateGrant` par compte, vous pouvez vous limiter `kms:CreateGrant` à des certificats spécifiques à l'aide des clés de EncryptionContext condition kms :. Spécifiez `arn:aws:acm` comme clé et la valeur de l'ARN à restreindre. L'exemple de politique suivant empêche l'utilisation d'un certificat spécifique, mais en autorise d'autres.

```
{
   "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

Avec AWS CloudFormation vous pouvez créer un modèle qui décrit les AWS ressources que vous souhaitez utiliser. AWS CloudFormation fournit et configure ensuite ces ressources pour vous. AWS CloudFormation peut fournir des ressources prises en charge par ACM, telles que Elastic Load Balancing CloudFront, Amazon et Amazon API Gateway. Pour plus d'informations, consultez Services intégrés à AWS Certificate Manager.

Si vous avez l' AWS CloudFormation habitude de créer et de supprimer rapidement plusieurs environnements de test, nous vous recommandons de ne pas créer de certificat ACM distinct pour chaque environnement. En procédant ainsi, votre quota de certificats sera rapidement atteint. Pour de plus amples informations, consultez Quotas. Créez plutôt un certificat générique qui couvre tous les noms de domaine que vous utilisez pour les tests. Par exemple, si vous créez des certificats ACM de manière répétée pour des noms de domaine qui se différencient uniquement par un numéro de version, par exemple `<version>.service.example.com`, créez un seul certificat générique pour `<*>.service.example.com`. Incluez le certificat générique dans le modèle AWS CloudFormation utilisé pour créer votre environnement de test.

Épinglage de certificat

L'épinglage de certificat, parfois appelé épinglage SSL, est un processus que vous pouvez utiliser dans votre application pour valider un hôte distant en l'associant directement à son certificat X.509 ou à sa clé publique au lieu de l'associer à une hiérarchie de certificats. L'application utilise donc l'épinglage pour contourner la validation de la chaîne de certificats SSL/TLS. Le processus de validation SSL classique vérifie les signatures dans l'ensemble de la chaîne de certificats, en allant de l'autorité de certification (CA) racine aux certificats CA subordonnés, le cas échéant. Il vérifie également le certificat de l'hôte distant au bas de la hiérarchie. Sinon, votre application peut épingler le certificat à l'hôte distant et seul ce certificat et non le certificat racine ou tout autre certificat de la chaîne est donc approuvé. Vous pouvez ajouter le certificat ou la clé publique de l'hôte distant pour votre application pendant le développement. Autrement, l'application peut ajouter le certificat ou la clé lors de sa première connexion à l'hôte.

> **Warning**
>
> Nous recommandons que votre application n'épingle pas de certificat ACM. ACM effectue l'opération Renouvellement géré des certificats ACM pour renouveler automatiquement vos certificats SSL/TLS émis par Amazon avant leur date d'expiration. Pour renouveler un certificat, ACM génère une nouvelle paire de clés publiques-privées. Si votre application

épingle le certificat ACM et que celui-ci a été renouvelé avec une nouvelle clé publique, l'application risque de ne pas pouvoir se connecter à votre domaine.

Si vous décidez d'épingler un certificat, les options suivantes n'empêcheront pas votre application de se connecter à votre domaine :

- Importez votre propre certificat dans ACM, puis épinglez votre application au certificat importé. ACM n'essaie pas de renouveler automatiquement les certificats importés.
- Si vous utilisez un certificat public, épinglez votre application à tous les Amazon root certificates (certificats racines Amazon) disponibles. Si vous utilisez un certificat privé, épinglez votre application au certificat racine de votre CA.

Validation de domaine

Avant que l'autorité de certification Amazon (CA) puisse délivrer un certificat pour votre site, AWS Certificate Manager (ACM) doit vérifier que vous possédez ou contrôlez tous les domaines que vous avez spécifiés dans votre demande. Vous pouvez effectuer la vérification par e-mail ou à l'aide du DNS. Pour de plus amples informations, consultez Validation DNS et Validation par courriel.

Ajout ou suppression de noms de domaine

Vous ne pouvez pas ajouter ni supprimer de noms de domaine dans un certificat ACM existant. À la place, vous devez demander un nouveau certificat contenant la liste révisée des noms de domaine. Par exemple, si votre certificat contient cinq noms de domaine et que vous souhaitez en ajouter quatre autres, vous devez demander un nouveau certificat contenant les neuf noms de domaine. Comme pour tout nouveau certificat, vous devez valider la propriété de tous les noms de domaine figurant dans la demande, y compris les noms que vous avez validés auparavant pour le certificat d'origine.

Si vous utilisez la validation par e-mail, vous recevez 8 e-mails de validation maximum pour chaque domaine, parmi lesquels il doit être donné suite à au moins un dans les 72 heures. Par exemple, lorsque vous demandez un certificat contenant cinq noms de domaine, vous recevez 40 e-mails de validation maximum, parmi lesquels il doit être donné suite à au moins 5 dans les 72 heures. Au fur et à mesure que le nombre de noms de domaine augmente dans la demande de certificat, le travail nécessaire pour utiliser les e-mails afin de valider la propriété des domaines augmente aussi.

Si vous utilisez plutôt la validation DNS, vous devez écrire un nouvel enregistrement DNS dans la base de données pour le nom de domaine complet à valider. ACM vous envoie l'enregistrement à créer et interroge ensuite la base de données afin de déterminer si l'enregistrement a été ajouté. L'ajout de l'enregistrement indique que vous possédez ou contrôlez le domaine. Dans l'exemple précédent, si vous demandez un certificat avec cinq noms de domaine, vous devez créer cinq enregistrements DNS. Nous vous recommandons d'utiliser la validation DNS dans la mesure du possible.

Refus de la journalisation de transparence des certificats

> **Important**
>
> Quelles que soient les actions que vous utilisez pour refuser la journalisation de transparence des certificats, votre certificat peut quand même être consigné par un client ou une personne qui a accès au point de terminaison public ou privé auquel vous liez le certificat. Toutefois, le certificat ne contiendra pas d'horodatage de certificat signé (SCT). Seule l'autorité de certification émettrice peut intégrer un SCT dans un certificat.

À compter du 30 avril 2018, Google Chrome cesse de faire confiance aux certificats SSL/TLS publics qui ne sont pas enregistrés dans un journal de transparence de certificats. Par conséquent, à partir du 24 avril 2018, le CA Amazon a commencé à publier tous les certificats nouveaux et renouvelés dans au moins deux journaux publics. Une fois qu'un certificat a été consigné, il ne peut pas être supprimé. Pour de plus amples informations, consultez Journalisation de transparence des certificats.

La journalisation s'effectue automatiquement lorsque vous demandez un certificat ou lorsqu'un certificat est renouvelé, mais vous pouvez choisir de refuser cette action. Cette décision tient généralement à des préoccupations liées à la sécurité et à la confidentialité des données. Par exemple, la journalisation des noms de domaine d'hôte internes fournit à des pirates potentiels des informations sur les réseaux internes qui ne seraient autrement pas publiques. En outre, la journalisation peut causer la fuite de noms de produits et sites Web nouveaux ou non communiqués.

Pour désactiver la journalisation transparente lorsque vous demandez un certificat, utilisez le `options` paramètre de la AWS CLI commande request-certificate ou de l'opération RequestCertificateAPI. Si votre certificat a été émis avant le 24 avril 2018 et que vous souhaitez vous assurer qu'il n'est pas enregistré lors du renouvellement, vous pouvez utiliser la update-certificate-optionscommande ou l'opération UpdateCertificateOptionsAPI pour vous désinscrire.

Limites

- Vous ne pouvez pas utiliser la console pour activer ou désactiver la journalisation de transparence.
- Vous ne pouvez pas modifier le statut de journalisation lorsqu'un certificat entre dans sa période de renouvellement, généralement 60 jours avant son expiration. Aucun message d'erreur n'est généré si un changement de statut échoue.

Une fois qu'un certificat a été consigné, il ne peut pas être supprimé du journal. Refuser à ce stade n'aura aucun effet. Si vous refusez la journalisation lorsque vous demandez un certificat, puis choisissez ultérieurement de l'accepter, votre certificat ne sera consigné qu'à son renouvellement. Si vous voulez que le certificat soit consigné immédiatement, nous vous recommandons d'en émettre un nouveau.

L'exemple suivant vous montre comment utiliser la commande request-certificate pour désactiver la transparence des certificats lorsque vous demandez un nouveau certificat.

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

La commande précédente génère le nom ARN de votre nouveau certificat.

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

Si vous possédez déjà un certificat et que vous ne souhaitez pas qu'il soit enregistré lors de son renouvellement, utilisez la update-certificate-optionscommande. Cette commande ne renvoie aucune valeur.

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

Allumez AWS CloudTrail

Activez la CloudTrail journalisation avant de commencer à utiliser ACM. CloudTrail vous permet de surveiller vos AWS déploiements en récupérant l'historique des appels d' AWS API pour votre compte, y compris les appels d'API effectués via la console de AWS gestion, les AWS SDK, Amazon Web Services et les AWS Command Line Interface niveaux supérieurs d'Amazon Web Services. Vous pouvez également identifier les utilisateurs et les comptes qui ont appelé les API ACM, l'adresse IP source d'origine des appels, ainsi que le moment où les appels ont eu lieu. Vous pouvez CloudTrail intégrer des applications à l'aide de l'API, automatiser la création de traces pour votre organisation, vérifier l'état de vos pistes et contrôler la manière dont les administrateurs activent et désactivent la CloudTrail connexion. Pour plus d'informations, consultez Création d'un journal d'activité. Accédez à Utilisation CloudTrail avec AWS Certificate Manager pour consulter des exemples de journaux d'activité associés à des actions ACM.

Configuration

Avec AWS Certificate Manager (ACM), vous pouvez fournir et gérer des certificats SSL/TLS pour vos sites Web et applications AWS basés sur vous. Vous utilisez ACM pour créer ou importer un certificat, puis le gérer. Vous devez utiliser d'autres AWS services pour déployer le certificat sur votre site Web ou votre application. Pour plus d'informations sur les services intégrés à ACM, consultez Services intégrés à AWS Certificate Manager. Les sections suivantes présentent les actions à effectuer avant d'utiliser ACM.

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Enregistrement d'un nom de domaine

Le nom de domaine complet (FQDN) est le nom spécifique d'une organisation ou d'une personne sur Internet, suivi d'une extension de domaine de niveau supérieur, par exemple .com ou .org. Si vous n'avez pas encore de nom de domaine enregistré, vous pouvez en enregistrer un par l'intermédiaire d'Amazon Route 53 ou de dizaines d'autres bureaux d'enregistrement commerciaux. En général, vous accédez au site Web du registre et vous demandez un nom de domaine. Le registre interroge WHOIS afin de déterminer si le nom de domaine complet demandé est disponible. Si c'est le cas, le registre affiche habituellement la liste des noms associés qui diffèrent selon l'extension de domaine, et vous donne l'occasion d'acquérir l'un des noms disponibles. L'enregistrement dure généralement pendant une période de temps définie, par exemple un ou deux ans avant son renouvellement obligatoire.

Pour plus d'informations sur l'enregistrement des noms de domaine avec Amazon Route 53, consultez Enregistrement de noms de domaines à l'aide d'Amazon Route 53 dans le Guide du développeur Amazon Route 53.

(Facultatif) Configuration d'une adresse électronique pour votre domaine

> **Note**
>
> Les étapes suivantes ne sont requises que si vous utilisez la validation par courriel pour indiquer que vous possédez ou contrôlez le nom de domaine complet (FQDN) indiqué dans votre demande de certificat. ACM exige que vous validiez la propriété ou le contrôle avant d'émettre un certificat. Vous pouvez utiliser la validation par courriel ou la validation DNS. Pour plus d'informations sur la validation par courriel, consultez Validation par courriel.
> Si vous êtes en mesure de modifier la configuration DNS, nous vous recommandons d'utiliser la validation de domaine DNS plutôt que la validation par courriel. La validation DNS supprime le besoin de configurer des adresses électroniques pour le nom de domaine. Pour plus d'informations sur la validation DNS, consultez Validation DNS.

Base de données WHOIS

La base de données WHOIS contient les informations de contact de votre domaine. Pour valider votre identité, ACM envoie un courriel aux trois adresses suivantes de la base de données WHOIS. Vous devez vous assurer que vos informations de contact sont publiques ou que le courriel envoyé à une adresse cryptée est transféré vers votre adresse électronique réelle.

- Inscrit au domaine
- Contact technique
- Contact administratif

(Facultatif) Configuration d'un enregistrement CAA

Vous pouvez éventuellement configurer un enregistrement DNS d'autorisation d'autorité de certification (CAA) pour spécifier que AWS Certificate Manager (ACM) est autorisée à délivrer un certificat pour votre domaine ou sous-domaine. Après avoir validé votre domaine, ACM vérifie la présence d'enregistrement CAA pour s'assurer qu'il peut émettre un certificat pour vous. Vous pouvez choisir de ne pas configurer un registre CAA pour votre domaine si vous ne souhaitez pas activer la vérification de CAA.

Un enregistrement CAA contient les champs de données suivants :

flags (indicateurs)

Indique si la valeur du champ tag est prise en charge par ACM. Définissez cette valeur sur 0.

tag (balise)

Le champ tag peut comporter l'une des valeurs suivantes. Notez que le champ iodef est ignoré actuellement.

issue

Indique que l'autorité de certification (CA) ACM indiquée dans le champ value est autorisée à émettre un certificat pour votre domaine ou sous-domaine.

issuewild

Indique que l'autorité de certification (CA) ACM indiquée dans le champ value est autorisée à émettre un certificat générique pour votre domaine ou sous-domaine. Un certificat générique s'applique au domaine ou sous-domaine et à tous ses sous-domaines.

valeur

La valeur de ce champ dépend de la valeur du champ tag. Vous devez placer cette valeur entre guillemets ("").

Lors de la valeur du champ tag est issue

Le champ value contient le nom de domaine de l'autorité de certification (CA). Ce champ peut contenir le nom d'une CA autre qu'une CA Amazon. Toutefois, si aucun enregistrement CAA n'indique l'une des quatre autorités de certification Amazon suivantes, ACM ne peut pas émettre de certificat pour votre domaine ou sous-domaine :

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

Le champ de valeur peut également contenir un point-virgule (;) pour indiquer qu'aucune CA ne doit être autorisée à émettre un certificat pour votre domaine ou sous-domaine. Utilisez ce champ si vous décidez à un moment donné que vous ne souhaitez plus recevoir un certificat émis pour un domaine particulier.

Lors de la valeur de tag est issuewild

Le champ value est le même que lorsque la valeur de tag est issue, sauf que la valeur s'applique aux certificats génériques.

En présence d'un enregistrement CAA issuewild qui n'inclut pas de valeur CA ACM, aucun certificat générique ne peut être émis par ACM. Si aucun enregistrement issuewild n'est présent, mais qu'il existe un enregistrement CAA issue pour ACM, des certificats génériques peuvent être émis par ACM.

Example Exemples d'enregistrements CAA

Dans les exemples suivants, votre nom de domaine est indiqué en premier, suivi du type d'enregistrement (CAA). Le champ flags a toujours la valeur 0. Le champ tags peut avoir pour valeur issue ou issuewild. Si le champ a pour valeur issue et que vous tapez le nom de domaine d'un serveur d'autorité de certification dans le champ value, l'enregistrement CAA indique que le serveur spécifié est autorisé à émettre le certificat demandé. Si vous tapez un point-virgule (« ; ») dans le champ value, l'enregistrement CAA indique qu'aucune autorité de certification n'est autorisée à émettre un certificat. La configuration des enregistrements CAA varie en fonction du fournisseur 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      ";"
```

Pour plus d'informations sur l'ajout ou la modification d'enregistrements DNS, consultez votre fournisseur DNS. Route 53 prend en charge les enregistrements CAA. Si Route 53 est votre fournisseur DNS, consultez Format CAA pour plus d'informations sur la création d'un enregistrement.

Émission et gestion de certificats

Les certificats ACM peuvent être utilisés pour établir des communications sécurisées sur Internet ou au sein d'un réseau interne. Vous pouvez demander un certificat approuvé publiquement à ACM (« certificat ACM ») ou importer un certificat approuvé publiquement émis par un tiers. Les certificats auto-signés sont également pris en charge. Pour provisionner la PKI interne de votre organisation, vous pouvez émettre des certificats ACM signés par une autorité de certification privée créée et gérée par Autorité de certification privée AWS. L'autorité de certification peut résider dans votre compte ou être partagée avec vous par un autre compte.

> **Note**
>
> Les certificats ACM publics peuvent être installés sur des instances Amazon EC2 connectées à une enclave Nitro, mais pas à d'autres instances Amazon EC2. Pour plus d'informations sur la configuration d'un serveur web autonome sur une instance Amazon EC2 non connectée à une enclave Nitro, consultez Tutoriel : Installation d'un serveur web LAMP sur Amazon Linux 2 ou Tutoriel : Installation d'un serveur web LAMP avec une AMI Amazon Linux.

> **Note**
>
> Dans la mesure où les certificats signés par une autorité de certification privée ne sont pas approuvés par défaut, les administrateurs doivent les installer dans les magasins d'approbation clients.

Pour commencer à émettre des certificats, connectez-vous à la console AWS de gestion et ouvrez la console ACM à l'adresse https://console.aws.amazon.com/acm/home. Si la page d'introduction s'affiche, sélectionnez Get Started (Démarrer). Dans le cas contraire, choisissez Certificate Manager ou Private CAs (Autorités de certification privées) dans le volet de navigation de gauche.

Rubriques

- Demande de certificat public
- Demande de certificat privé PKI
- Validation de la propriété du domaine
- Établissement de la liste des certificats gérés par ACM

- Description des certificats ACM
- Suppression de certificats gérés par ACM
- Installation de certificats ACM

Demande de certificat public

Les sections suivantes expliquent comment utiliser la console ACM ou AWS CLI demander un certificat ACM public. Après la demande d'un certificat public, suivez l'une des procédures décrites dans Validation de la propriété du domaine.

Les certificats ACM publics respectent tous les deux la norme X.509 et sont soumis aux restrictions suivantes :

- Noms :Vous devez utiliser des noms de sujet conformes au DNS. Pour plus d'informations, consultez Noms de domaine.
- Algorithme : pour le chiffrement, l'algorithme de clés privées du certificat doit être soit un RSA 2 048 bits, soit un ECDSA 256 bits, soit un ECDSA 384 bits.
- Expiration : chaque certificat est valide pendant une durée de13 mois (395 jours).
- Renouvellement : ACM tente de renouveler automatiquement un certificat privé après une période de 11 mois.

Si vous rencontrez des problèmes lors d'une demande de certificat, veuillez consultez Résolution des problèmes liés aux demandes de certificat.

Pour demander un certificat pour une PKI privée en utilisant Autorité de certification privée AWS, voirDemande de certificat privé PKI.

> **Note**
>
> Les administrateurs peuvent utiliser les stratégies de clés conditionnelles ACM pour contrôler la manière dont les utilisateurs finaux émettent de nouveaux certificats. Ces clés conditionnelles permettent d'imposer des restrictions sur les domaines, les méthodes de validation et d'autres attributs liés à une demande de certificat.

> **Note**
>
> À moins que vous choisissiez de vous désengager, les certificats ACM approuvés publiquement sont automatiquement enregistrés dans au moins deux bases de données de transparence. Actuellement, vous ne pouvez pas utiliser la console pour vous désengager. Vous devez utiliser l'API AWS CLI ou l'API ACM. Pour plus d'informations, consultez Refus de la journalisation de transparence des certificats. Pour obtenir des informations générales sur les journaux de transparence, consultez Journalisation de transparence des certificats.

Rubriques

Demande de certificat public à l'aide de la console

Pour demander un certificat public ACM (console)

1. Connectez-vous à la console de AWS gestion et ouvrez la console ACM à l'adresse https://console.aws.amazon.com/acm/home.

   Choisissez Request a certificate (Demander un certificat).
2. Dans la page Ajouter des noms de domaine, saisissez votre nom de domaine.

   Vous pouvez utiliser un nom de domaine complet (FQDN) comme **`www.example.com`** ou un nom de domaine strict ou apex tel que **`example.com`**. Vous pouvez également utiliser un astérisque (**`*`**) comme caractère générique à la position la plus à gauche pour protéger plusieurs noms de site dans le même domaine. Par exemple, **`*.example.com`** protège **`corp.example.com`** et **`images.example.com`**. Le nom générique apparaît dans le champ Objet et dans l'extension Autre nom de l'objet du certificat ACM.

   Lorsque vous demandez un certificat générique, l'astérisque (**`*`**) doit se trouver tout à gauche du nom de domaine et ne peut protéger qu'un seul niveau de sous-domaine. Par exemple, **`*.example.com`** il peut protéger **`login.example.com`**, et **`test.example.com`**, mais ne peut pas protéger **`test.login.example.com`**. Notez aussi que **`*.example.com`** protège uniquement les sous-domaines de **`example.com`**, il ne protège pas le domaine strict ou apex (**`example.com`**). Pour protéger les deux, consultez l'étape suivante.

> **Note**
>
> Conformément à la norme RFC 5280, la longueur du nom de domaine (techniquement, le nom commun) que vous entrez à cette étape ne peut pas dépasser 64 octets (caractères), points compris. La longueur de chacun des autres noms d'objet que vous fournissez ensuite, comme à l'étape suivante, peut atteindre 253 octets.

Pour ajouter un autre nom, choisissez Ajouter un autre nom à ce certificat et tapez le nom dans la zone de texte. Ceci est très utile pour protéger un nom de domaine strict ou apex (comme **`example.com`**) et ses sous-domaines (comme **`*.example.com`**).

3. Sur la section Validation method (Méthode de validation), choisissez DNS validation – recommended (Validation DNS – recommandé) ou Email validation (Validation par e-mail), selon vos besoins.

> **Note**
>
> Si vous êtes en mesure de modifier la configuration DNS, nous vous recommandons d'utiliser la validation de domaine DNS plutôt que la validation par e-mail. La validation du DNS présente plusieurs avantages par rapport à la validation par e-mail. veuillez consulter Validation DNS.

Avant qu'ACM émette un certificat, il valide le fait que vous possédiez ou contrôliez les noms de domaine de votre demande de certificat. Vous pouvez utiliser la validation par e-mail ou la validation DNS.

Si vous choisissez la validation par e-mail, ACM envoie un e-mail de validation aux trois adresses de contact enregistrées dans la base de données WHOIS et jusqu'à cinq adresses d'administration système courantes de chaque nom de domaine. Vous ou un représentant autorisé devez répondre à l'un de ces e-mails. Pour de plus amples informations, consultez Validation par courriel.

Si vous utilisez la validation DNS, il vous suffit d'ajouter un enregistrement CNAME fourni par ACM dans votre configuration DNS. Pour plus d'informations sur la validation DNS, consultez Validation DNS.

4. Dans la section Key algorithm (Algorithme de clés), choisissez l'un des trois algorithmes disponibles :

   - RSA 2048 (par défaut)
   - ECDSA P 256
   - ECDSA P 384

   Pour plus d'informations vous aidant à choisir un algorithme, consultez Algorithme de clés le billet de AWS blog Comment évaluer et utiliser les certificats ECDSA dans. AWS Certificate Manager

5. Sur la page Balises vous pouvez éventuellement baliser votre certificat. Les balises sont des paires clé-valeur qui servent de métadonnées pour identifier et organiser AWS les ressources. Pour obtenir la liste des paramètres de balise ACM et des instructions sur l'ajout de balises aux certificats après leur création, consultez Balisage des certificats AWS Certificate Manager.

   Lorsque vous avez terminé d'ajouter des balises, choisissez Demande.

6. Une fois la demande traitée, la console vous renvoie à votre liste de certificats, où les informations sur le nouveau certificat sont affichées.

   Un certificat prend le statut En attente de validation sur demande, sauf s'il échoue pour l'une des raisons indiquées dans la rubrique de dépannage Échec de la demande de certificat. ACM tente à plusieurs reprises de valider un certificat pendant 72 heures, puis s'arrête. Si un certificat affiche le statut Échec ou Expiration de la validation, supprimez la demande, corrigez le problème avec Validation DNS ou Validation par e-mail et réessayez. Si la validation aboutit, le certificat prend le statut Émis.

   > **Note**
   >
   > Selon la façon dont vous avez commandé la liste, un certificat que vous recherchez peut ne pas être immédiatement visible. Vous pouvez cliquer sur le triangle noir à droite pour modifier l'ordre. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite.

Demande de certificat public via l'interface CLI

Utilisez la commande request-certificate pour demander un nouveau certificat ACM public via l'interface de ligne de commande. Les valeurs facultatives pour la méthode de validation sont DNS et EMAIL. Les valeurs facultatives de l'algorithme de clés sont RSA_2048 (valeur par défaut si le paramètre n'est pas explicitement fourni), EC_prime256v1 et EC_secp384r1.

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

Cette commande génère le nom Amazon Resource Name (ARN) de votre nouveau certificat public.

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

Demande de certificat privé PKI

Si vous avez accès à une autorité de certification privée existante créée par Autorité de certification privée AWS, ACM peut demander un certificat adapté à une utilisation dans votre PKI privée. L'autorité de certification peut résider dans votre compte ou être partagée avec vous par un autre compte. Pour plus d'informations sur la création d'une Autorité de certification privée, consultez Création d'une autorité de certification privée.

Les certificats signés par une autorité de certification privée ne sont pas approuvés par défaut et ACM ne prend en charge aucune forme de validation pour ces certificats. Par conséquent, un administrateur doit prendre des mesures pour les installer dans les magasins de confiance destinés aux clients de votre organisation.

Les certificats ACM privés respectent tous les deux la norme X.509 et sont soumis aux restrictions suivantes :

- Noms :Vous devez utiliser des noms de sujet conformes au DNS. Pour plus d'informations, consultez Noms de domaine.

- Algorithme : pour le chiffrement, l'algorithme de clés privées du certificat doit être soit un RSA 2 048 bits, soit un ECDSA 256 bits, soit un ECDSA 384 bits.

> **Note**
>
> La famille d'algorithmes de signature spécifiée (RSA ou ECDSA) doit correspondre à la famille d'algorithmes de la clé secrète de l'autorité de certification.

- Expiration : chaque certificat est valide pendant une durée de13 mois (395 jours). La date d'expiration d'une certification privée doit être postérieure à la date de fin de la certification demandée, autrement la demande échoue.
- Renouvellement : ACM tente de renouveler automatiquement un certificat privé après une période de 11 mois.

L'autorité de certification privée utilisée pour signer les certificats de l'entité finale est soumise à ses propres restrictions :

- Le statut de l'autorité de certification doit être « Actif ».
- L'algorithme de la clé privée de celle-ci doit être RSA 2048 ou RSA 4096.

> **Note**
>
> Contrairement aux certificats approuvés publiquement, les certificats signés par une Autorité de certification privée ne nécessitent aucune validation.

Rubriques

Configuration de l'accès à une autorité de certification privée

Vous pouvez les utiliser Autorité de certification privée AWS pour signer vos certificats ACM dans l'un des deux cas suivants :

- Compte unique : l'autorité de certification signataire et le certificat ACM émis résident dans le même AWS compte.

  Pour que l'émission et les renouvellements liés à compte unique soient activés, l'administrateur de Autorité de certification privée AWS doit autoriser le principal du service ACM a créer, récupérer et répertorier les certificats. Cela se fait à l'aide de l'action Autorité de certification privée AWS API CreatePermissionou de la AWS CLI commande create-permission. Le propriétaire du compte attribue ces autorisations à un utilisateur IAM, un groupe d'utilisateurs IAM ou un rôle IAM responsable de l'émission des certificats.

- Comptes multiples : l'autorité de certification signataire et le certificat ACM émis résident dans des AWS comptes différents, et l'accès à l'autorité de certification a été accordé au compte sur lequel réside le certificat.

  Pour activer l'émission et les renouvellements entre comptes, l' Autorité de certification privée AWS administrateur doit associer une politique basée sur les ressources à l'autorité de certification à l'aide de l'action Autorité de certification privée AWS API PutPolicyou de la commande put-policy. AWS CLI La stratégie précise les principaux des autres comptes qui ont un accès limité à l'autorité de certification. Pour plus d'informations, consultez Utilisation d'une stratégie basée sur les ressources avec ACM Private CA.

  Le scénario Comptes multiples exige également qu'ACM mette en place un rôle lié à un service (SLR) pour interagir en tant que principal avec la stratégie PCA. ACM crée automatiquement le rôle SLR lors de l'émission du premier certificat.

  ACM peut vous avertir qu'il ne peut pas déterminer si un rôle SLR existe sur votre compte. Si l'autorisation `iam:GetRole` requise a déjà été accordée au rôle SLR ACM pour votre compte, l'alerte ne se reproduira pas après la création du rôle SLR. Si elle se reproduit, vous ou votre administrateur de compte devrez peut-être accorder l'autorisation `iam:GetRole` à ACM, ou associer votre compte à la stratégie `AWSCertificateManagerFullAccess` gérée par ACM.

  Pour plus d'informations, consultez Utilisation d'un rôle lié à un service avec ACM.

> **Important**
>
> Votre certificat ACM doit être activement associé à un AWS service pris en charge avant de pouvoir être automatiquement renouvelé. Pour en savoir plus sur les ressources prises en charge par ACM, consultez Services intégrés à AWS Certificate Manager.

Demande de certificat privé à l'aide de la console ACM

1. Connectez-vous à la console AWS de gestion et ouvrez la console ACM à l'adresse https://console.aws.amazon.com/acm/home.

   Choisissez Request a certificate (Demander un certificat).
2. Sur la page Demander un certificat choisissez Request a private certificate (Demander un certificat privé) et Next (Suivant) pour continuer.
3. Dans la section Informations de l'autorité de certification, cliquez sur le menu Certificate authority (Autorité de certification) et choisissez l'une des autorités de certification privées disponibles. Si l'autorité de certification est partagée à partir d'un autre compte, l'ARN est précédé des informations de propriété.

   Les informations relatives à l'autorité de certification s'affichent pour vous permettre de vérifier que vous avez choisi la bonne :

   - Propriétaire
   - Type
   - Nom commun
   - Organisation
   - Unité d'organisation
   - Nom du pays
   - État ou province
   - Nom de la localité
4. Dans la page Ajouter des noms de domaine, saisissez votre nom de domaine. Vous pouvez utiliser un nom de domaine complet (FQDN) comme **`www.example.com`** ou un nom de domaine strict ou apex tel que **`example.com`**. Vous pouvez également utiliser un astérisque (**`*`**) comme caractère générique à la position la plus à gauche pour protéger plusieurs noms de site dans le même domaine. Par exemple, **`*.example.com`** protège **`corp.example.com`** et **`images.example.com`**. Le nom générique apparaît dans le champ Objet et dans l'extension Autre nom de l'objet du certificat ACM.

   > **Note**
   >
   > Lorsque vous demandez un certificat générique, l'astérisque (**`*`**) doit se trouver tout à gauche du nom de domaine et ne peut protéger qu'un seul niveau de sous-

domaine. Par exemple, **`*.example.com`** il peut protéger **`login.example.com`**, et **`test.example.com`**, mais ne peut pas protéger **`test.login.example.com`**. Notez aussi que **`*.example.com`** protège uniquement les sous-domaines de **`example.com`**, il ne protège pas le domaine strict ou apex (**`example.com`**). Pour protéger les deux, consultez l'étape suivante

Choisissez éventuellement Ajouter un autre nom à ce certificat et tapez le nom dans la zone de texte. Ceci est très utile pour authentifier un nom de domaine strict ou apex (comme **`example.com`**) et ses sous-domaines (comme **`*.example.com`**).

5. Dans la section Key algorithm (Algorithme de clés), choisissez l'un des trois algorithmes disponibles :

   - RSA 2048 (par défaut)
   - ECDSA P 256
   - ECDSA P 384

   Pour obtenir des informations qui vous aideront à choisir un algorithme, consultez Algorithme de clés.
6. Sur la page Ajouter des balises vous pouvez éventuellement baliser votre certificat. Les balises sont des paires clé-valeur qui servent de métadonnées pour identifier et organiser AWS les ressources. Pour obtenir la liste des paramètres de balise ACM et des instructions sur l'ajout de balises aux certificats après leur création, consultez Balisage des certificats AWS Certificate Manager.
7. Dans la section Permissions de renouvellement de certificats, accusez réception de l'avis concernant les autorisations de renouvellement de certificat. Ces autorisations permettent le renouvellement automatique des certificats PKI privés que vous signez avec l'autorité de certification sélectionnée. Pour plus d'informations, consultez Utilisation d'un rôle lié à un service avec ACM.
8. Après avoir fourni toutes les informations requises, choisissez Request (Demander). La console vous renvoie à la liste des certificats, où vous pouvez afficher votre nouveau certificat.

> **Note**
>
> Selon la façon dont vous avez commandé la liste, un certificat que vous recherchez peut ne pas être immédiatement visible. Vous pouvez cliquer sur le triangle noir à droite pour

modifier l'ordre. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite.

Demande de certificat PKI via l'interface de ligne de commande (CLI)

Utilisez la commande request-certificate pour demander un certificat privé dans ACM.

> **Note**
>
> Lorsque vous demandez un certificat PKI privé signé par une autorité de certification AWS Private CA, la famille d'algorithmes de signature spécifiée (RSA ou ECDSA) doit correspondre à la famille d'algorithmes de la clé secrète de l'autorité de certification.

```
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
```

Cette commande génère le nom Amazon Resource Name (ARN) de votre nouveau certificat privé.

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

Dans la plupart des cas, ACM attache automatiquement un rôle lié à un service (SLR) à votre compte la première fois que vous utilisez une autorité de certification partagée. Le rôle SLR permet le renouvellement automatique des certificats d'entité finale que vous émettez. Pour déterminer si le rôle SLR est présent, vous pouvez interroger IAM à l'aide de la commande suivante :

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

Si le rôle SLR est présent, la sortie de commande est semblable à la suivante :

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

En l'absence de rôle SLR, consultez Utilisation d'un rôle lié à un service avec ACM.

Validation de la propriété du domaine

Avant que l'autorité de certification Amazon ne puisse émettre un certificat pour votre site, AWS Certificate Manager (ACM) doit vérifier que vous possédez ou contrôlez tous les noms de domaine spécifiés dans votre demande. Afin de prouver que vous en êtes le propriétaire, vous pouvez choisir la validation DNS ou la validation par e-mail au moment où vous effectuez la demande de certificat.

> **Note**
>
> La validation s'applique uniquement aux certificats approuvés publiquement émis par ACM. ACM ne valide pas la propriété du domaine pour les certificats importés ou pour les certificats signés par une autorité de certification privée. ACM ne peut pas valider les ressources

dans une zone privée hébergée Amazon VPC ou tout autre domaine privé. Pour plus d'informations, consultez Résolution des problèmes liés à la validation des certificats.

En général, nous recommandons d'utiliser la validation DNS plutôt que la validation par e-mail pour les raisons suivantes :

- Si vous utilisez Amazon Route 53 pour gérer vos enregistrements DNS publics, vous pouvez mettre à jour vos enregistrements directement via ACM.
- ACM renouvelle automatiquement les certificats qui ont fait l'objet d'une validation DNS tant que le certificat est utilisé et que l'enregistrement DNS est en place.
- Pour renouveler les certificats validés par courriel, une action est requise de la part du propriétaire du domaine. ACM commence à envoyer des avis de renouvellement 45 jours avant l'expiration. Ces notifications sont envoyées aux adresses de boîte aux lettres WHOIS du domaine et jusqu'à cinq adresses d'administrateur courantes. Les notifications contiennent un lien sur lequel le propriétaire du domaine peut cliquer pour un renouvellement facile. Une fois tous les domaines répertoriés validés, ACM émet un certificat renouvelé avec le même ARN.

Si vous ne disposez pas de l'autorisation nécessaire pour modifier la base de données DNS de votre domaine, utilisez plutôt la validation par e-mail.

> **Note**
>
> Une fois que vous avez créé un certificat avec une validation par e-mail, vous ne pouvez pas passer à sa validation avec DNS.

Rubriques

Validation DNS

Le système de noms de domaine (DNS) est un service d'annuaire dédié aux ressources connectées à un réseau. Votre fournisseur DNS gère une base de données contenant les enregistrements qui définissent votre domaine. Lorsque vous choisissez la validation DNS, ACM vous fournit un

ou plusieurs enregistrements CNAME qui doivent être ajoutés à cette base de données. Ces enregistrements contiennent une paire clé-valeur unique qui prouve que vous contrôlez le domaine.

> **Note**
>
> Une fois que vous avez créé un certificat avec une validation par e-mail, vous ne pouvez pas passer à sa validation avec DNS.

Par exemple, si vous demandez un certificat pour le domaine `example.com` avec `www.example.com` comme nom supplémentaire, ACM crée deux enregistrements CNAME pour vous. Chacun des enregistrements créés spécifiquement pour votre domaine et votre compte contient un nom et une valeur. La valeur est un alias qui pointe vers un AWS domaine qu'ACM utilise pour renouveler automatiquement votre certificat. Les enregistrements CNAME ne doivent être ajoutés qu'une seule fois à votre base de données DNS. ACM renouvelle automatiquement votre certificat tant qu'il est utilisé et que votre enregistrement CNAME reste en place.

> **Important**
>
> Si vous n'utilisez pas Amazon Route 53 pour gérer vos enregistrements DNS publics, contactez votre fournisseur DNS pour savoir comment ajouter des enregistrements. Si vous n'êtes pas autorisé à modifier la base de données DNS de votre domaine, utilisez plutôt la validation par e-mail.

Sans avoir à répéter la validation, vous pouvez demander des certificats ACM supplémentaires pour votre nom de domaine complet (FQDN) tant que l'enregistrement CNAME reste en place. En d'autres termes, vous pouvez créer des certificats de remplacement portant le même nom de domaine, ou des certificats couvrant différents sous-domaines. Comme le jeton de validation CNAME fonctionne pour toutes les AWS régions, vous pouvez recréer le même certificat dans plusieurs régions. Vous pouvez également remplacer un certificat supprimé.

Vous pouvez arrêter le renouvellement automatique en supprimant le certificat du service AWS auquel il est associé ou en supprimant l'enregistrement CNAME. Si Route 53 n'est pas votre fournisseur DNS, contactez votre fournisseur pour savoir comment supprimer un enregistrement. Si Route 53 est votre fournisseur, consultez Suppression de jeux d'enregistrements de ressources dans le Guide du développeur Route 53. Pour plus d'informations sur le renouvellement de certificats gérés, consultez Renouvellement géré des certificats ACM.

> **Note**
>
> La résolution CNAME échoue si plus de cinq CNAME sont enchaînés dans votre configuration DNS. Si vous avez besoin d'un enchaînement plus long, nous vous recommandons d'utiliser la validation par e-mail.

Fonctionnement des enregistrements CNAME pour ACM

> **Note**
>
> Cette section s'adresse aux clients qui n'utilisent pas Route 53 comme fournisseur DNS.

Si vous n'utilisez pas Route 53 comme fournisseur DNS, vous devez entrer manuellement les enregistrements CNAME fournis par ACM dans la base de données de votre fournisseur, généralement via un site web. Les enregistrements CNAME sont utilisés à différentes fins, notamment comme mécanismes de redirection et comme conteneurs pour les métadonnées spécifiques au fournisseur. Pour ACM, ces enregistrements permettent la validation initiale de la propriété du domaine et le renouvellement automatisé continu des certificats.

Le tableau suivant présente des exemples d'enregistrements CNAME pour six noms de domaine. La paire Nom de l'enregistrement-Valeur de l'enregistrement de chaque enregistrement sert à authentifier la propriété du nom de domaine.

Dans le tableau, notez que les deux premières paires Nom de l'enregistrement-Valeur de l'enregistrement sont identiques. Ceci illustre le fait que pour un domaine générique, tel que `*.example.com`, les chaînes créées par ACM sont les mêmes que celles créées pour son domaine de base, `example.com`. Sinon, la paire Nom de l'enregistrement-Valeur de l'enregistrementdiffère pour chaque nom de domaine.

Exemples d'enregistrements CNAME

Nom de domaine	Nom de l'enregistrement	Valeur de l'enregistrement	Comment
*.example.com	*_x1*.example.com.	*_x2*.acm-validations.aws.	Identical (éléments identiques)

Nom de domaine	Nom de l'enregistrement	Valeur de l'enregistrement	Comment
example.com	_*x1*.example.com.	_*x2*.acm-validations.aws.	
www.example.com	_*x3*.www.example.com.	_*x4*.acm-validations.aws.	Unique
host.example.com	_*x5*.host.example.com.	_*x6*.acm-validations.aws.	Unique
subdomain.example.com	_*x7*.subdomain.example.com.	_*x8*.acm-validations.aws.	Unique
host.subdomain.example.com	_*x9*.host.subdomain.example.com.	_*x10*.acm-validations.aws.	Unique

Les valeurs *xN* qui suivent le trait de soulignement (_) sont de longues chaînes générées par ACM. Par exemple,

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

est représentatif d'un résultat généré pour le Nom de l'enregistrement. La Valeur de l'enregistrement associée pourrait être

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

pour le même enregistrement DNS.

> **Note**
>
> Si votre fournisseur DNS ne prend pas en charge les valeurs CNAME comportant un trait de soulignement de début, consultez Résolution des problèmes liés à la validation DNS.

Lorsque vous effectuez une demande de certificat avec validation DNS, ACM fournit des informations CNAME au format suivant :

Nom de domaine	Nom de l'enregistrement	Type d'enregistrement	Valeur de l'enregistrement
example.com	_a79865eb4cd1a6ab990a45779b4e0b96.example.com.	CNAME	_424c7224e9b0146f9a8808af955727d0.acm-validations.aws.

Le Nom de domaine est le nom de domaine complet associé au certificat. Le Nom de l'enregistrement identifie l'enregistrement de manière unique, en servant de clé dans la paire clé-valeur. La Valeur d'enregistrement sert de valeur dans la paire clé-valeur.

Ces trois valeurs (Domain Name (Nom de domaine), Record Name (Nom d'enregistrement), and Record Value (Valeur d'enregistrement)) doivent être entrées dans les champs appropriés de l'interface web de votre fournisseur DNS pour ajouter des enregistrements DNS. Les fournisseurs ne traitent pas nom de l'enregistrement (ou « nom ») de la même manière. Dans certains cas, vous devez fournir la chaîne entière comme illustré ci-dessus. D'autres fournisseurs ajoutent automatiquement le nom de domaine à la chaîne que vous entrez, ce qui signifie (dans cet exemple) que vous ne devez entrer que

```
_a79865eb4cd1a6ab990a45779b4e0b96
```

dans le champ de nom. Si vous vous trompez et que vous saisissez un nom d'enregistrement qui contient un nom de domaine (tel que *.example.com*), vous risquez de vous retrouver avec ce qui suit :

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

Dans ce cas, la validation échouera. Par conséquent, vous devez essayer de déterminer à l'avance quel type de données votre fournisseur attend.

Configuration de la validation DNS

Cette section décrit comment configurer un certificat public pour utiliser la validation DNS.

Pour configurer la validation DNS sur la console

> **Note**
>
> Cette procédure suppose que vous avez déjà créé au moins un certificat et que vous travaillez dans la AWS région où vous l'avez créé. Si vous essayez d'ouvrir la console et que l'écran de première utilisation s'affiche à la place, ou si vous réussissez à ouvrir la console et que votre certificat ne figure pas dans la liste, vérifiez que vous avez spécifié la bonne région.

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/.
2. Dans la liste des certificats, choisissez l'ID de certificat d'un certificat avec statut Validation en attente que vous souhaitez configurer. Cette opération ouvre une page d'informations pour le certificat.
3. Dans la section Domaines, effectuez l'une des deux procédures suivantes :

   a. (Facultatif) Validez à l'aide de Route 53.

   Un bouton Créer des enregistrements dans Route 53 actif apparaît si les conditions suivantes sont réunies :

   - Vous utilisez Route 53 comme fournisseur DNS.
   - Vous disposez de l'autorisation nécessaire pour écrire dans la zone hébergée par Route 53.
   - Votre nom de domaine complet (FQDN) n'a pas encore été validé.

   > **Note**
   >
   > Si vous utilisez Route 53 mais que le bouton Créer des enregistrements dans Route 53 est absent ou désactivé, consultez La console ACM n'affiche pas le bouton « Créer des enregistrements dans Route 53 ».

   Choisissez le bouton Créer des enregistrements dans Route 53, puis Create (Créer). La page Status du certificat doit s'ouvrir avec un rapport de bannière d'état Enregistrements DNS créés avec succès.

Votre nouveau certificat doit rester affiché avec le statut Validation en attente pendant au moins 30 minutes.

> **Tip**
>
> Actuellement, vous ne pouvez pas demander par programmation la création automatique par ACM de votre enregistrement dans Route 53. Vous pouvez toutefois effectuer un appel AWS CLI d'API à Route 53 pour créer l'enregistrement dans la base de données DNS Route 53. Pour plus d'informations sur les jeux d'enregistrements Route 53, consultez Utilisation de jeux d'enregistrements de ressources.

b. (Facultatif) Si vous n'utilisez pas Route 53 comme fournisseur DNS, vous devez récupérer les informations CNAME et les ajouter à votre base de données DNS. Sur la page de détails du nouveau certificat, effectuez cette opération de deux manières :

- Copiez les composants CNAME affichés dans la section Domaines. Ces informations doivent être ajoutées manuellement à votre base de données DNS.
- Sinon, choisissez Export to CSV (Exporter vers CSV). Les informations contenues dans le fichier doivent être ajoutées manuellement à votre base de données DNS.

> **Important**
>
> Pour éviter les problèmes de validation, vérifiez Fonctionnement des enregistrements CNAME pour ACM avant d'ajouter des informations à la base de données de votre fournisseur DNS. Si vous rencontrez des problèmes, consultez Résolution des problèmes liés à la validation DNS.

Si ACM n'est pas en mesure de valider le nom de domaine dans les 72 heures qui suivent la génération d'une valeur CNAME, le statut du certificat est remplacé par Validation expirée. La raison la plus probable de ce résultat est que vous n'avez pas réussi à mettre à jour votre configuration DNS avec la valeur générée par ACM. Pour remédier à ce problème, vous devez demander un nouveau certificat après avoir examiné les instructions relatives au CNAME.

Validation par courriel

Avant que l'autorité de certification Amazon (CA) puisse délivrer un certificat pour votre site, AWS Certificate Manager (ACM) doit vérifier que vous possédez ou contrôlez tous les domaines que vous avez spécifiés dans votre demande. Vous pouvez effectuer la vérification par e-mail ou à l'aide du DNS. Cette rubrique traite de la validation par e-mail. Pour plus d'informations sur la validation DNS, consultez Validation DNS.

Prenez en compte les considérations suivantes concernant la validation par e-mail.

- Pour pouvoir utiliser la validation par e-mail, vous devez disposer d'une adresse électronique valide enregistrée dans votre domaine. Les procédures à suivre pour configurer une adresse électronique ne sont pas présentées dans ce guide.
- La validation s'applique uniquement aux certificats approuvés publiquement émis par ACM. ACM ne valide pas la propriété du domaine pour les certificats importés ou pour les certificats signés par une autorité de certification privée. ACM ne peut pas valider les ressources dans une zone privée hébergée Amazon VPC ou tout autre domaine privé. Pour plus d'informations, consultez Résolution des problèmes liés à la validation des certificats.
- Une fois que vous avez créé un certificat avec une validation par e-mail, vous ne pouvez pas passer à sa validation avec DNS.

Les certificats ACM sont valides pendant 13 mois (395 jours). Pour renouveler les certificats validés par e-mail, une action est requise de la part du propriétaire du domaine. ACM commence à envoyer des avis de renouvellement 45 jours avant l'expiration, en utilisant les adresses de boîte aux lettres WHOIS du domaine et cinq adresses d'administrateur communes. Les notifications contiennent un lien sur lequel le propriétaire du domaine peut cliquer pour un renouvellement facile. Une fois tous les domaines répertoriés validés, ACM émet un certificat renouvelé avec le même ARN.

Si vous rencontrez des problèmes lors de l'utilisation de la validation par e-mail, veuillez consulter Résolution des problèmes liés à la validation par courriel.

ACM envoie des e-mails au superdomaine de votre choix. Tout sous-domaine inférieur à l'adresse minimale du site Web est valide et sera utilisé comme domaine pour l'adresse e-mail en tant que suffixe après « @ » (par exemple, vous pouvez recevoir un e-mail à admin@example.com si vous spécifiez exemple.com comme domaine de validation pour sous-domain.exemple.com).

Ces messages électroniques sont envoyés aux trois adresses de contact suivantes dans WHOIS :

- Inscrit au domaine
- Contact technique
- Contact administratif

> **Note**
>
> Nous vous recommandons fortement de configurer et de surveiller les cinq adresses système communes à votre certificat. La récupération des informations de contact à partir du WHOIS n'est pas fiable. Le taux de réussite des recherches dans le WHOIS est faible (moins de 5 %), en partie en raison du respect des lois internationales sur la protection de la vie privée.

> **Important**
>
> À compter de juin 2024, ACM ne prend plus en charge la validation des nouveaux e-mails via les adresses de contact WHOIS. Pour les certificats existants, à compter d'octobre 2024, ACM n'enverra pas de notifications de renouvellement aux adresses de contact WHOIS du domaine. ACM continuera d'envoyer des e-mails de validation aux cinq adresses système communes pour le domaine demandé. Pour plus de détails, voir AWS Certificate Manager va arrêter la recherche dans le WHOIS pour les certificats validés par e-mail

Lorsque vous demandez un certificat, ACM envoie un e-mail au nom de domaine que vous spécifiez dans le `DomainName` paramètre ou dans le `ValidationDomain` paramètre facultatif. Pour plus d'informations, consultez ???.

- administrator@*votre_nom_domaine*
- hostmaster@*votre_nom_domaine*
- postmaster@*votre_nom_domaine*
- webmaster@*votre_nom_domaine*
- admin@*votre_nom_domaine*

Pour plus d'informations sur la manière dont ACM détermine les adresses électronique de vos domaines, consultez (Facultatif) Configuration d'une adresse électronique pour votre domaine.

Exception à ce processus

Si vous demandez un certificat ACM pour un nom de domaine qui commence par **www** ou par un astérisque générique (*), ACM supprime les caractères **www** ou l'astérisque du début et envoie un e-mail aux adresses administratives. Ces adresses sont formées en ajoutant admin@, administrator@, hostmaster@, postmaster@ et webmaster@ à la partie restante du nom de domaine. Par exemple, si vous demandez un certificat ACM pour www.example.com, l'e-mail n'est pas envoyé à admin@www.example.com mais à admin@example.com. De même, si vous demandez un certificat ACM pour *.test.example.com, l'e-mail est envoyé à admin@test.example.com. Les adresses administratives courantes restantes sont formées de la même manière.

> **Note**
>
> Veillez à ce que l'e-mail soit envoyé aux adresses administratives d'un domaine apex, par exemple `example.com` et non aux adresses administratives pour un sous-domaine, par exemple `test.example.com`. Pour ce faire, spécifiez l'`ValidationDomain`option dans l'RequestCertificateAPI ou dans la commande request-certificate AWS CLI . Cette fonction n'est pas prise en charge actuellement lorsque vous utilisez la console pour demander un certificat.
>
> Même lorsque tous les messages sont envoyés à une seule adresse électronique, vous devez répondre à un message par domaine ou sous-domaine afin de le valider et de générer le certificat.

Expiration et renouvellement de certificat

Les certificats ACM sont valides pendant 13 mois (395 jours). Pour renouveler les certificats validés par e-mail, une action est requise de la part du propriétaire du domaine. ACM commence à envoyer des avis de renouvellement 45 jours avant l'expiration, en utilisant les adresses de boîte aux lettres WHOIS du domaine et cinq adresses d'administrateur communes. Les notifications contiennent un lien sur lequel le propriétaire du domaine peut cliquer pour un renouvellement facile. Une fois tous les domaines répertoriés validés, ACM émet un certificat renouvelé avec le même ARN.

Consultez Validation par courriel, ci-dessus, pour plus d'informations.

(Facultatif) Renvoi d'un e-mail de validation

Chaque e-mail de validation contient un jeton que vous pouvez utiliser pour approuver une demande de certificat. Cependant, étant donné que l'e-mail de validation nécessaire pour le processus d'approbation peut être bloqué par des filtres anti-spam ou perdu en transit, le jeton de validation

expire automatiquement au bout de 72 heures. Si vous ne recevez pas l'e-mail d'origine ou que le jeton a expiré, vous pouvez demander que l'e-mail soit renvoyé.

En cas de problèmes persistants liés à la validation des e-mails, veuillez consulter la section Résolution des problèmes liés à la validation par courriel dans le Résolution des problèmes.

> **Note**
>
> Les informations suivantes s'appliquent uniquement aux certificats fournis par ACM et uniquement aux certificats qui utilisent la validation par e-mail. L'e-mail de validation n'est pas obligatoire pour les certificats que vous avez importés dans ACM. Pour de plus amples informations sur la validation de domaine DNS, veuillez consulter Validation DNS.

Pour renvoyer un e-mail de validation à l'aide de la console

1. Connectez-vous à la console de AWS gestion et ouvrez la console ACM à l'adresse https://console.aws.amazon.com/acm/home.
2. Dans la liste des certificats, choisissez l'ID de certificat d'un certificat que vous souhaitez valider. Cette action ouvre une page d'informations.

   > **Note**
   >
   > Selon la façon dont vous avez commandé la liste, un certificat que vous recherchez peut ne pas être immédiatement visible. Vous pouvez cliquer sur le triangle noir à droite pour modifier l'ordre. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite.

3. Dans la section Domaines, choisissez Resend validation email (Renvoyer un e-mail de validation), sélectionnez chacun des domaines nécessitant une validation, puis choisissez Resend (Renvoyer). La bannière Renvoi des e-mails de validation réussi doit apparaître.

Pour renvoyer un e-mail de validation à l'aide de AWS CLI

Vous pouvez utiliser la resend-validation-emailcommande pour renvoyer un e-mail.

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

> **Note**
>
> La resend-validation-emailcommande s'applique uniquement aux certificats ACM pour lesquels vous utilisez la validation par e-mail. La validation n'est pas obligatoire pour les certificats que vous avez importés dans ACM ou pour les certificats privés que vous gérez avec ACM.

Établissement de la liste des certificats gérés par ACM

Vous pouvez utiliser la console ACM ou AWS CLI répertorier les certificats gérés par ACM. La console peut répertorier jusqu'à 500 certificats sur une page et la CLI jusqu'à 1 000.

Pour dresser la liste des certificats à l'aide de la console

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/.
2. Consultez les informations de la liste des certificats. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite. Chaque certificat occupe une ligne avec les colonnes suivantes affichées par défaut pour chacun :

- Nom de domaine : nom de domaine complet du certificat (FQDN).
- Type : le type de certificat. Les valeurs possibles sont : Émis par Amazon | Privé | Importé
- Statut : statut du certificat. Les valeurs possibles sont : Validation en attente | Émis | Inactif | Expiré | Révoqué | Échec | Validation expirée
- En cours d'utilisation ? — Si le certificat ACM est activement associé à un AWS service tel que Elastic Load Balancing ou CloudFront. La valeur peut être Non ou Oui.
- Éligibilité au renouvellement : indique le renouvellement automatique du certificat par ACM lorsqu'il se rapproche de sa date d'expiration. Les valeurs possibles sont les suivantes : Eligible | Inéligible. Pour les règles d'éligibilité, consulter Renouvellement géré des certificats ACM.

En cliquant sur l'icône des paramètres dans le coin supérieur droit de la console, vous pouvez personnaliser le nombre de certificats affichés sur une page, spécifier le comportement du contenu

des cellules et afficher des champs d'informations supplémentaires. Disponibilité des champs facultatifs suivants :

- Noms de domaine supplémentaires — Un ou plusieurs noms de domaine (noms alternatifs du sujet) inclus dans le certificat.
- Demandé à : l'heure à laquelle ACM a demandé le certificat.
- Délivré à : L'heure de délivraison du certificat. Ces informations sont disponibles uniquement pour les certificats émis par Amazon, et non pas pour les importations.
- Pas avant : l'heure avant laquelle le certificat n'est pas valide.
- Pas après : l'heure après laquelle le certificat n'est pas valide.
- Révoqué à — Pour les certificats révoqués, date de la révocation.
- Balise de nom : la valeur d'une balise sur ce certificat appelée Nom, s'il existe une telle balise.
- État du renouvellement — État de la demande de renouvellement d'un certificat. Ce champ s'affiche et n'a de valeur que lorsque le renouvellement a été demandé. Les valeurs possibles sont les suivantes : En attente de renouvellement automatique | En attente de validation | Succès | Échec.

> **Note**
>
> Il peut s'écouler jusqu'à plusieurs heures avant que les modifications au statut du certificat ne soient disponibles. En cas de problème, une demande de certificat est périmée après 72 heures et le processus d'émission ou de renouvellement doit être repris depuis le début.

La préférence Page size (Taille de la page) spécifie le nombre de certificats renvoyés sur chaque page de console.

Pour de plus amples informations sur les détails des certificats disponibles, veuillez consulter Description des certificats ACM.

Pour répertorier vos certificats à l'aide du AWS CLI

Utilisez la commande list-certificates pour dresser la liste des certificats gérés par ACM, comme illustré dans l'exemple suivant :

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

La commande renvoie des informations semblables à ce qui suit :

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

Par défaut, seuls les certificats pour lesquels la valeur de keyTypes est `RSA_1024` ou `RSA_2048` et pour lesquels au moins un domaine est spécifié sont renvoyés. Pour afficher d'autres certificats que vous contrôlez, tels que des certificats sans domaine ou des certificats utilisant une taille de bits ou un algorithme différent, utilisez le paramètre `--includes` comme indiqué dans l'exemple suivant. Le paramètre vous permet de spécifier un membre de la structure de filtres.

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

Description des certificats ACM

Vous pouvez utiliser la console ACM ou le AWS CLI pour répertorier les métadonnées détaillées relatives à vos certificats.

Pour afficher les informations des certificats dans la console

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/ pour afficher vos certificats. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite.
2. Pour afficher les métadonnées détaillées d'un certificat répertorié, choisissez l'ID de certificat. Une page s'ouvre, affichant les informations suivantes :

   - Statut du certificat
     - Identifiant : identifiant unique hexadécimal de 32 octets du certificat
     - ARN : Amazon Resource Name (ARN) sous la forme `arn:aws:acm:`*`Region`*`:`*`444455556666`*`:certificate/`*`certificate_ID`*
     - Type : identifie la catégorie de gestion d'un certificat ACM. Les valeurs possibles sont : Émis par Amazon | Privé | Importé. Pour plus d'informations, veuillez consulter Demande de certificat public, Demande de certificat privé PKI ou Importation de certificats dans AWS Certificate Manager.
     - Statut : statut du certificat. Les valeurs possibles sont : Validation en attente | Émis | Inactif | Expiré | Révoqué | Échec | Validation expirée
     - Statut détaillé : date et heure auxquelles le certificat a été demandé ou importé
   - Domaines
     - Domaine : nom de domaine complet (FQDN) du certificat.
     - Statut : statut de validation du domaine. Les valeurs possibles sont : Validation en attente | Révoqué | Échec | Validation expirée | Succès
   - Détails
     - En cours d'utilisation ? : indique si le certificat est associé à un AWS service intégré Les valeurs possibles sont : Oui | Non
     - Nom de domaine : le premier nom de domaine complet du certificat.
     - Nombre de noms supplémentaires : nombre de noms de domaine pour lesquels le certificat est valide
     - Numéro de série : numéro de série hexadécimal de 16 octets du certificat

- Informations sur la clé publique : algorithme cryptographique utilisé pour générer la paire de clés
- Algorithme de signature : algorithme cryptographique utilisé pour signer le certificat.
- Peut être utilisé avec : une liste deservices intégrés ACM qui prennent en charge un certificat présentant ces paramètres
- Demandé à : date et heure de la demande d'émission
- Émis à : le cas échéant, la date et l'heure d'émission
- Importé à : le cas échéant, la date et l'heure de l'importation
- Pas avant : début de la période de validité du certificat
- Pas après : date et heure d'expiration du certificat
- Admissibilité du renouvellement - Les valeurs possibles sont : Eligible | Inéligible. Pour les règles d'éligibilité, voir Renouvellement géré des certificats ACM.
- État du renouvellement — État de la demande de renouvellement d'un certificat. Ce champ s'affiche et n'a de valeur que lorsque le renouvellement a été demandé. Les valeurs possibles sont les suivantes : En attente de renouvellement automatique | En attente de validation | Succès | Échec.

  > **Note**
  >
  > Il peut s'écouler jusqu'à plusieurs heures avant que les modifications au statut du certificat ne soient disponibles. En cas de problème, une demande de certificat est périmée après 72 heures et le processus d'émission ou de renouvellement doit être repris depuis le début.

- CA : ARN de la CA de signature

- Balises
  - Clé
  - Valeur
- État de validation : le cas échéant, les valeurs possibles sont :
  - En attente : la validation a été demandée et n'est pas terminée.
  - La validation a expiré : une demande de validation a expiré, mais vous pouvez la relancer.
  - Aucun : le certificat est destiné à une infrastructure PKI privée ou est auto-signé, et ne nécessite pas de validation.

Pour consulter les détails du certificat à l'aide du AWS CLI

Utilisez le describe-certificate dans le AWS CLI pour afficher les détails du certificat, comme indiqué dans la commande suivante :

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

La commande renvoie des informations semblables à ce qui suit :

```
{
    "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"
    }
}
```

Suppression de certificats gérés par ACM

Vous pouvez utiliser la console ACM ou le AWS CLI pour supprimer un certificat.

Important

- Vous ne pouvez pas supprimer un certificat ACM qui est en cours d'utilisation dans un autre service AWS . Pour supprimer un certificat en cours d'utilisation, vous devez commencer par supprimer l'association de ce certificat. Pour ce faire, utilisez la console ou de l'interface CLI pour le service associé.
- La suppression d'un certificat émis par une autorité de certification privée n'a aucun effet sur l'autorité de certification. Vous continuerez à être facturé pour l'autorité de certification jusqu'à ce que celle-ci soit supprimée. Pour de plus amples informations, veuillez consulter Suppression de votre autorité de certification privée dans le Guide de l'utilisateur AWS Private Certificate Authority .

Pour supprimer un certificat à l'aide de la console

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/.
2. Dans la liste des certificats, cochez la case correspondant au certificat ACM, puis choisissez Delete (Supprimer)

Note

Selon la façon dont vous avez commandé la liste, un certificat que vous recherchez peut ne pas être immédiatement visible. Vous pouvez cliquer sur le triangle noir à droite pour modifier l'ordre. Vous pouvez également parcourir plusieurs pages de certificats à l'aide des numéros de page situés en haut à droite.

Pour supprimer un certificat à l'aide du AWS CLI

Utilisez la commande delete-certificate pour supprimer un certificat, comme illustré dans la commande suivante :

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

Installation de certificats ACM

Vous ne pouvez pas utiliser ACM pour installer un certificat public directement sur le site Web ou l'application que vous AWS utilisez. Vous devez utiliser l'un des services intégrés à ACM. Pour plus d'informations, consultez Services intégrés à AWS Certificate Manager.

Les certificats ACM signés par une autorité de certification Autorité de certification privée AWS et destinés à votre PKI privée peuvent être exportés et installés manuellement sur n'importe quel système auquel vous disposez d'un accès administratif. Ces certificats ne sont pas approuvés sur l'Internet public.

Renouvellement géré des certificats ACM

ACM fournit un renouvellement géré des certificats SSL/TLS émis par Amazon. Concrètement, ACM renouvelle automatiquement vos certificats (si vous utilisez la validation DNS), ou vous envoie des notifications par courriel lorsque la date d'expiration approche. Ces services s'appliquent aux certificats ACM publics et privés.

Un certificat peut faire l'objet d'un renouvellement automatique sous réserve des considérations suivantes :

- ÉLIGIBLE s'il est associé à un autre AWS service, tel que Elastic Load Balancing ou CloudFront.
- ÉLIGIBLE s'il est exporté depuis l'émission ou le dernier renouvellement.
- ÉLIGIBLE s'il s'agit d'un certificat privé émis en appelant l'RequestCertificateAPI ACM puis exporté ou associé à un autre AWS service.
- ÉLIGIBLE s'il s'agit d'un certificat privé émis via la Console de gestion et qu'il est ensuite exporté ou associé à un autre service AWS .
- NON ÉLIGIBLE s'il s'agit d'un certificat privé émis en appelant l' Autorité de certification privée AWS IssueCertificateAPI.
- NON ÉLIGIBLE s'il est importé.
- NON ÉLIGIBLE s'il a déjà expiré.

En outre, les exigences Punycode suivantes relatives aux noms de domaine internationalisés doivent être remplies :

1. Les noms de domaine commençant par le modèle « <character><character>-- » doivent correspondre à « xn-- ».
2. Les noms de domaine commençant par « xn-- » doivent également être des noms de domaine internationalisés valides.

Exemples de Punycode

Nom de domaine	Remplit #1	Remplit #2	Autoris	Remarque
example.com	N/A	s/o	✓	Ne commence pas par « <character><character>-- »
a--example.com	N/A	s/o	✓	Ne commence pas par « <character><character>-- »
abc--example.com	N/A	s/o	✓	Ne commence pas par « <character><character>-- »
xn--xyz.com	Oui	Oui	✓	Nom de domaine internationalisé valide (se résout sur 简.com)
xn--example.com	Oui	Non	✗	Nom de domaine internationalisé non valide
ab--example.com	Non	Non	✗	Doit commencer par « xn-- »

Lorsqu'ACM renouvelle un certificat, le nom Amazon Resource Name (ARN) de celui-ci ne change pas. En outre, les certificats ACM sont des ressources régionales. Si vous possédez des certificats pour le même nom de domaine dans plusieurs AWS régions, chacun de ces certificats doit être renouvelé indépendamment.

Rubriques

- Renouvellement de certificats publiquement approuvés
- Renouvellement des certificats dans une infrastructure PKI privée
- Vérifier le statut de renouvellement d'un certificat

Renouvellement de certificats publiquement approuvés

Lorsque vous émettez un certificat géré et approuvé par le AWS Certificate Manager public, vous devez prouver que vous êtes le propriétaire du domaine. Cela se fait avec Validation DNS ou

validation par courriel. Lorsqu'un certificat est renouvelé, ACM utilise la même méthode que celle que vous avez choisie précédemment pour valider à nouveau votre propriété. Les rubriques suivantes décrivent comment fonctionne le processus de renouvellement dans chaque cas.

Rubriques

- Renouvellement des domaines validés par DNS
- Renouvellement des domaines validés par email

Renouvellement des domaines validés par DNS

Le renouvellement géré est entièrement automatisé pour les certificats ACM qui ont initialement été émis à l'aide de la validation DNS.

Soixante jours avant l'expiration, ACM vérifie les critères de renouvellement suivants :

- Le certificat est actuellement utilisé par un AWS service.
- Tous les enregistrements requis CNAME DNS fournis par ACM (un pour chaque nom alternatif de sujet unique) sont présents et accessibles via le DNS public.

Si tous ces critères sont remplis, ACM considère que les noms de domaine sont validés et renouvelle le certificat.

ACM envoie AWS Health des événements et des EventBridge événements Amazon lorsqu'elle ne peut pas valider automatiquement un domaine lors du renouvellement (par exemple, en raison de la présence d'un enregistrement CAA). Ces événements sont envoyés 45 jours, 30 jours, 15 jours, sept jours, trois jours et un jour avant leur expiration. Pour plus d'informations, consultez EventBridge Support Amazon pour ACM.

Renouvellement des domaines validés par email

Les certificats ACM sont valides pendant 13 mois (395 jours). Pour renouveler les certificats validés par e-mail, une action est requise de la part du propriétaire du domaine. ACM commence à envoyer des avis de renouvellement 45 jours avant l'expiration, en utilisant les adresses de boîte aux lettres WHOIS du domaine et cinq adresses d'administrateur communes. Les notifications contiennent un lien sur lequel le propriétaire du domaine peut cliquer pour un renouvellement facile. Une fois tous les domaines répertoriés validés, ACM émet un certificat renouvelé avec le même ARN.

Pour plus d'informations sur la validation des courriels, consultez Validation par courriel.

Pour savoir comment répondre par programmation à un message électronique de validation, consultez Automatisation de la validation par courriel .

Demandez un message électronique de validation de domaine

Une fois les adresses e-mail de contact configurées pour votre domaine (consultez (Facultatif) Configuration d'une adresse électronique pour votre domaine), vous pouvez utiliser la console AWS Certificate Manager ou l'API ACM pour demander à ce qu'ACM vous envoie un e-mail de validation de domaine pour votre renouvellement de certificat. Pour ce faire, procédez comme suit :

- Vous avez utilisé la validation par courriel lors de votre demande initiale de certificat ACM.
- Le statut de renouvellement de votre certificat est Pending Validation (validation en attente). Pour plus d'informations sur l'identification du statut de renouvellement d'un certificat, consultez Vérifier le statut de renouvellement d'un certificat.
- Vous n'avez pas reçu ou avez perdu le message électronique original de validation de domaine envoyé par ACM pour le renouvellement du certificat.

Pour demander à ACM de vous renvoyer le message électronique de validation de domaine (console)

1. Ouvrez la AWS Certificate Manager console à l'adresse https://console.aws.amazon.com/acm/home.
2. Cliquez sur l'onglet ID de certificat du certificat qui nécessite une validation.
3. Choisissez Resend validation email (renvoyer un courriel de validation).

Pour demander à ACM de vous renvoyer le courriel de validation de domaine (API ACM)

Utilisez l'ResendValidationEmailopération dans l'API ACM. Pour ce faire, transmettez l'ARN du certificat, du domaine exigeant la validation manuelle et du domaine dans lequel vous souhaitez recevoir les courriels de validation de domaine. L'exemple suivant montre comment procéder avec AWS CLI. Cet exemple contient des sauts de ligne pour faciliter la lecture.

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

Renouvellement des certificats dans une infrastructure PKI privée

Les certificats ACM signés par une autorité de certification privée Autorité de certification privée AWS sont éligibles au renouvellement géré. Contrairement aux certificats ACM approuvés publiquement, les certificats d'une infrastructure PKI privée ne nécessitent aucune validation. La confiance est établie lorsqu'un administrateur installe le certificat de l'autorité de certification racine appropriée dans les magasins d'approbation clients.

> **Note**
>
> Seuls les certificats obtenus à l'aide de la console ACM ou à RequestCertificatel'aide de l'API ACM sont éligibles au renouvellement géré. Les certificats émis directement à Autorité de certification privée AWS l'aide de l'IssueCertificateaction de l' Autorité de certification privée AWS API ne sont pas gérés par ACM.

Soixante jours avant la date d'expiration d'un certificat géré, ACM tente de le renouveler automatiquement. Cela s'applique également aux certificats exportés et installés manuellement (par exemple, dans un centre de données sur site). Les clients peuvent également forcer le renouvellement à tout moment à l'RenewCertificateaide de l'API ACM. Pour obtenir un exemple d'implémentation Java du renouvellement forcé, consultez Renouvellement d'un certificat.

Après le renouvellement, le déploiement d'un certificat s'effectue de l'une des manières suivantes :

- Si le certificat est associé à un service intégré ACM, le nouveau certificat remplace l'ancien sans action supplémentaire du client.
- Si le certificat n'est pas associé à un service intégré ACM, une action du client est requise pour exporter et installer le certificat renouvelé. Vous pouvez effectuer ces actions manuellement ou avec l'aide d'Amazon AWS Health EventBridge, en procédant AWS Lambdacomme suit. Pour de plus amples informations, consultez Automatisation de l'exportation des certificats renouvelés

Automatisation de l'exportation des certificats renouvelés

La procédure suivante fournit un exemple de solution pour automatiser l'exportation de vos certificats PKI privés lorsque ACM les renouvelle. Cet exemple n'exporte qu'un certificat et sa clé privée hors d'ACM ; après l'exportation, le certificat doit encore être installé sur son périphérique cible.

Automatiser l'exportation de certificats à l'aide de la console

1. En suivant les procédures décrites dans le guide du développeur AWS Lambda, créez et configurez une fonction Lambda qui appelle l'API d'exportation ACM.

   a. Création d'une fonction Lambda.

   b. Création d'un rôle d'exécution Lambda pour votre fonction et ajoutez-y la politique d'approbation suivante. La politique autorise le code de votre fonction à récupérer le certificat et la clé privée renouvelés en appelant l'ExportCertificateaction de l'API ACM.

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

2. Créez une règle dans Amazon EventBridge pour suivre les événements de santé d'ACM et appelez votre fonction Lambda lorsqu'elle en détecte un. ACM écrit sur un AWS Health événement chaque fois qu'il tente de renouveler un certificat. Pour plus d'informations sur ces avis, consultez Vérifier le statut à l'aide du tableau de bord Personal Health Dashboard (PHD).

   Configurez la règle en ajoutant le modèle d'événement suivant.

```
{
   "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. Finalisez le processus de renouvellement en installant manuellement le certificat sur le système cible.

Test du renouvellement géré des certificats PKI privés

Vous pouvez utiliser l'API ACM ou AWS CLI tester manuellement la configuration de votre flux de renouvellement géré par ACM. De cette façon, vous pouvez confirmer que vos certificats seront renouvelés automatiquement par ACM avant expiration.

> **Note**
>
> Vous pouvez uniquement tester le renouvellement des certificats émis et exportés par Autorité de certification privée AWS.

Lorsque vous utilisez les actions d'API ou les commandes CLI décrites ci-dessous, ACM tente de renouveler le certificat. Si le renouvellement aboutit, ACM met à jour les métadonnées du certificat affichées dans la Console de gestion ou dans la sortie de l'API. Si le certificat est associé à un service intégré ACM, le nouveau certificat est déployé et un événement de renouvellement est généré dans Amazon CloudWatch Events. Si le renouvellement échoue, ACM renvoie une erreur et suggère une action corrective. (Vous pouvez afficher cette information à l'aide de la commande describe-certificate). Si le certificat n'est pas déployé via un service intégré, vous devez malgré tout l'exporter et l'installer manuellement sur votre ressource.

> **Important**
>
> Pour renouveler vos Autorité de certification privée AWS certificats auprès d'ACM, vous devez d'abord accorder au service ACM les autorisations principales pour le faire. Pour

plus d'informations, consultez Assigning Certificate Renewal Permissions to ACM(Octroi d'autorisations de renouvellement de certificats à ACM).

Pour tester manuellement le renouvellement de certificats (AWS CLI)

1. Utilisez la commande renew-certificate pour renouveler un certificat privé exporté.

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

2. Utilisez ensuite la commande describe-certificate pour confirmer que les informations du certificat ont été mises à jour.

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

Pour tester manuellement le renouvellement de certificat (API ACM)

- Envoyez une RenewCertificatedemande en spécifiant l'ARN du certificat privé à renouveler. Utilisez ensuite cette DescribeCertificateopération pour confirmer que les informations de renouvellement du certificat ont été mises à jour.

Vérifier le statut de renouvellement d'un certificat

Lorsque vous avez tenté de renouveler un certificat, ACM fournit un champ d'informations sur Renewal status (le statut du renouvellement) dans les détails du certificat. Vous pouvez utiliser la AWS Certificate Manager console, l'API ACM AWS CLI, ou le AWS Health Dashboard pour vérifier l'état de renouvellement d'un certificat ACM. Si vous utilisez la console ou l'API ACM, le statut du renouvellement peut avoir l'une des quatre valeurs de statut possibles répertoriées ci-dessous. AWS CLI Des valeurs similaires sont affichées si vous utilisez le AWS Health Dashboard.

Renouvellement automatique en attente

ACM essaie de valider automatiquement les noms de domaine contenus dans le certificat. Pour de plus amples informations, consultez Renouvellement des domaines validés par DNS. Aucune action supplémentaire n'est requise.

Validation en attente

ACM n'a pas pu valider automatiquement un ou plusieurs noms de domaine contenus dans le certificat. Vous devez agir pour valider ces noms de domaine ou le certificat ne sera pas renouvelé. Si vous avez initialement utilisé la validation par courriel pour le certificat, recherchez un courriel envoyé par ACM, puis suivez le lien contenu dans ce courriel pour procéder à la validation. Si vous avez utilisé la validation DNS, vérifiez que votre enregistrement DNS existe et que votre certificat est toujours en cours d'utilisation.

Réussite

Tous les noms de domaine contenus dans le certificat sont validés, et ACM a renouvelé le certificat. Aucune action supplémentaire n'est requise.

Échec

Un ou plusieurs noms de domaine n'ont pas été validés avant l'expiration du certificat, et ACM n'a pas renouvelé le certificat. Vous pouvez Request a new certificate (demander un nouveau certificat).

Un certificat est éligible au renouvellement s'il est associé à un autre AWS service, tel qu'Elastic Load Balancing CloudFront, ou s'il a été exporté depuis sa délivrance ou son dernier renouvellement.

> **Note**
>
> Il peut s'écouler jusqu'à plusieurs heures avant que les modifications du statut de renouvellement ne soient disponibles. En cas de problème, une demande de renouvellement expire au bout de 72 heures et le processus de renouvellement doit recommencer depuis le début. Pour bénéficier d'une aide à la résolution des problèmes, consultez Résolution des problèmes liés aux demandes de certificat.

Rubriques

Vérification du statut (console)

La procédure suivante explique comment utiliser la console ACM pour vérifier le statut du renouvellement d'un certificat ACM.

1. Ouvrez la AWS Certificate Manager console à l'adresse https://console.aws.amazon.com/acm/home.
2. Développez un certificat pour afficher ses détails.
3. Recherchez Statut du renouvellement dans la section Détails. Si vous ne voyez pas le statut, cela signifie qu'ACM n'a pas commencé le processus de renouvellement géré pour ce certificat.

Vérification du statut (API)

Pour un exemple Java qui montre comment utiliser l'DescribeCertificateaction pour vérifier l'état, consultezDescription d'un certificat.

Vérification du statut (CLI)

L'exemple suivant montre comment vérifier le statut de renouvellement de votre certificat ACM à l'aide de l'AWS Command Line Interface (AWS CLI).

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

Dans la réponse, notez la valeur dans le champ `RenewalStatus`. Si vous ne voyez pas le champ `RenewalStatus`, cela signifie qu'ACM n'a pas commencé le processus de renouvellement géré pour votre certificat.

Vérifier le statut à l'aide du tableau de bord Personal Health Dashboard (PHD)

ACM tente de renouveler automatiquement votre certificat ACM 60 jours avant son expiration. Si ACM ne peut pas renouveler automatiquement votre certificat, elle vous envoie des notifications relatives AWS Health Dashboard au renouvellement du certificat à des intervalles de 45 jours, 30 jours, 15 jours, 7 jours, 3 jours et 1 jour après son expiration pour vous informer que vous devez prendre des mesures. Cela AWS Health Dashboard fait partie du AWS Health service. Il ne nécessite

aucune configuration et peut être affiché par n'importe quel utilisateur authentifié dans votre compte. Pour plus d'informations, consultez le AWS Health guide de l'utilisateur.

> **Note**
>
> ACM envoie des avis d'événement de renouvellement successifs pour chacun des événements du calendrier de votre tableau de bord PHD. Chaque avis écrase le précédent jusqu'à ce que le renouvellement aboutisse.

Pour utiliser le AWS Health Dashboard:

1. Connectez-vous à l' AWS Health Dashboard adresse https://phd.aws.amazon.com/phd/home#/.
2. Choisissez Event Log (Journal des événements).
3. Pour Filtrer par balises ou attributs, choisissez Service.
4. Choisissez Certificate Manager (gestionnaire de certificat).
5. Choisissez Appliquer.
6. Pour Event category (Catégorie d'événements), choisissez Scheduled Change (Modification planifiée).
7. Choisissez Appliquer.

Automatisation de la validation par courriel

Les certificats ACM qui ont été validés par e'mail nécessitent normalement une intervention manuelle de la part du propriétaire du domaine. Les organisations qui traitent d'un grand nombre de certificats validés par courriel peuvent préférer créer un analyseur capable d'automatiser les réponses requises. Pour les clients qui utilisent la validation par courriel, les informations de cette section décrivent les modèles utilisés pour les messages électroniques de validation de domaine et le flux de travail nécessaire afin de mener à bien le processus de validation.

Modèles d'email de validation

Les messages d'email de validation se présentent sous l'un des deux formats suivants, selon qu'un nouveau certificat est demandé ou qu'un certificat existant est en cours de renouvellement. Le contenu des chaînes en surbrillance doit être remplacé par des valeurs spécifiques au domaine en cours de validation.

Validation d'un nouveau certificat

Texte du modèle de courriel :

```
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
```

Validation d'un certificat en vue de son renouvellement

Texte du modèle de courriel :

```
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
```

Une fois que vous aurez reçu un nouveau message de validation AWS, nous vous recommandons de l'utiliser comme modèle le plus up-to-date fiable pour votre analyseur syntaxique. Les clients disposant d'analyseurs de messages conçus avant novembre 2020 doivent tenir compte du fait que les modifications suivantes ont pu être apportées au modèle :

- La ligne d'objet du message électronique indique maintenant « `Certificate request for` *`domain name`* » au lieu de « `"Certificate approval for` *`domain name`* ».
- Le `AWS account ID` est maintenant présenté sans tirets ni traits d'union.
- Le `Certificate Identifier` présente maintenant l'ARN complet du certificat au lieu d'un formulaire raccourci, par exemple, *`arn:aws:acm:us-east-1:000000000000:certificate/3b4d78e1-0882-4f51-954a-298ee44ff369`* plutôt que *`3b4d78e1-0882-4f51-954a-298ee44ff369`*.
- L'URL d'approbation du certificat contient maintenant `acm-certificates.amazon.com` au lieu de `certificates.amazon.com`.
- Le formulaire d'approbation qui s'ouvre lorsque l'on clique sur l'URL d'approbation du certificat contient désormais le bouton d'approbation. Le nom du bouton d'approbation div est maintenant `approve-button` au lieu de `approval_button`.
- Le même format de courriel est utilisé pour les messages de validation des certificats nouvellement demandés et des certificats de renouvellement.

Flux de travail de validation

Cette section fournit des informations sur le flux de travail de renouvellement des certificats validés par courriel.

- Lorsque la console ACM traite une demande de certificat multidomaine, elle envoie des e-mails de validation au TODO. Avant qu'ACM puisse émettre le certificat, le propriétaire des domaines

doit valider un message électronique pour chaque domaine. Pour plus d'informations, consultez Utilisation d'un courriel pour valider la propriété du domaine.

- La validation par courriel des demandes de certificats multidomaines à l'aide de l'API ACM ou de l'interface CLI entraîne l'envoi par défaut d'un message électronique au domaine apex et à tous les sous-domaines. Avant qu'ACM puisse émettre le certificat, le propriétaire des domaines doit valider un message électronique pour chacun de ces domaines.

  > **Note**
  >
  > Avant novembre 2020, les clients pouvaient se contenter de ne valider que le domaine apex puisqu'ACM émettait un certificat qui couvrait également tous les sous-domaines. Les clients disposant d'analyseurs de messages conçus avant cette date doivent tenir compte des modifications apportées au flux de travail de validation par courriel.

- Avec l'API ACM ou l'interface CLI, vous pouvez forcer tous les messages électroniques de validation pour une demande de certificat multidomaine à envoyer au domaine apex. Dans l'API, utilisez le `DomainValidationOptions` paramètre de l'RequestCertificateaction pour spécifier une valeur pour`ValidationDomain`, qui est membre du DomainValidationOptiontype. Dans l'interface CLI, utilisez le paramètre --domain-validation-options de la commande request-certificate afin de spécifier une valeur pour `ValidationDomain`.

Importation de certificats dans AWS Certificate Manager

En plus de demander des certificats SSL/TLS fournis par AWS Certificate Manager (ACM), vous pouvez importer des certificats que vous avez obtenus en dehors de. AWS Cela peut être nécessaire lorsque vous disposez déjà d'un certificat délivré par un émetteur tiers ou que les certificats émis par ACM ne répondent pas aux besoins spécifiques de l'application.

Vous pouvez utiliser un certificat importé avec n'importe quel AWS service intégré à ACM. Les certificats que vous importez fonctionnent de la même manière que ceux fournis par ACM, à une exception importante près : ACM ne fournit pas de renouvellement géré pour les certificats importés.

Pour renouveler un certificat importé, vous pouvez vous procurer un nouveau certificat auprès de l'émetteur, puis le réimporter manuellement dans ACM. Cette action préserve l'association du certificat et son nom Amazon Resource Name (ARN). Sinon, vous pouvez importer un certificat complètement nouveau. Plusieurs certificats avec le même nom de domaine peuvent être importés, mais ils doivent être importés un par un.

> **Important**
>
> Vous êtes chargé de surveiller la date d'expiration de vos certificats importés et de les renouveler avant leur expiration. Vous pouvez simplifier cette tâche en utilisant Amazon CloudWatch Events pour envoyer des notifications lorsque vos certificats importés approchent de l'expiration. Pour plus d'informations, consultez Utilisation d'Amazon EventBridge.

Tous les certificats présents dans ACM sont des ressources régionales, y compris les certificats que vous importez. Pour utiliser le même certificat avec les équilibreurs de charge Elastic Load Balancing dans différentes AWS régions, vous devez importer le certificat dans chaque région où vous souhaitez l'utiliser. Pour utiliser un certificat auprès d'Amazon CloudFront, vous devez l'importer dans la région USA Est (Virginie du Nord). Pour plus d'informations, consultez Régions prises en charge.

Pour plus d'informations sur la procédure à suivre pour importer des certificats dans ACM, consultez les rubriques suivantes. Si vous rencontrez des problèmes lors de l'importation d'un certificat, consultez Problèmes liés à l'importation de certificat.

Rubriques

Conditions préalables à l'importation de certificats

Pour importer un certificat SSL/TLS auto-signé dans ACM, vous devez fournir le certificat et sa clé privée. Pour importer un certificat signé par une autorité de certification (CA) non-AWS , vous devez également inclure les clés privées et publiques du certificat. Votre certificat doit satisfaire à tous les critères décrits dans cette rubrique.

Pour tous les certificats importés, vous devez indiquer un algorithme de chiffrement et une taille de clé. ACM prend en charge les algorithmes suivants (nom de l'API entre parenthèses) :

- 1 024 bits RSA (`RSA_1024`)
- 2 048 bits RSA (`RSA_2048`)
- 3 072 bits RSA (`RSA_3072`)
- 4 096 bits RSA (`RSA_4096`)
- 256 bits ECDSA (`EC_prime256v1`)
- 384 bits ECDSA (`EC_secp384r1`)
- 521 bits ECDSA (`EC_secp521r1`)

Notez également les exigences supplémentaires suivantes :

- Les services intégrés d'ACM ne permettent d'associer à leurs ressources que les algorithmes et les tailles de clés qu'ils prennent en charge. Par exemple, il CloudFront ne prend en charge que les clés RSA 1024 bits, RSA 2048 bits, RSA 3072 bits et Elliptic Prime Curve 256 bits, tandis qu'Application Load Balancer prend en charge tous les algorithmes disponibles auprès d'ACM. Pour plus d'informations, consultez la documentation relative au service que vous utilisez.
- Le certificat doit être un certificat SSL/TLS SSL/TLS X.509 version 3. Il doit contenir une clé publique, le nom de domaine complet (FQDN) ou l'adresse IP de votre site web, ainsi que des informations sur l'émetteur.

- Un certificat peut être auto-signé par votre propre clé privée ou par la clé privée d'une autorité de certification (CA) émettrice. Vous devez fournir une clé privée qui a un taille inférieure à 5 Ko (5 120 octets) et elle doit être non chiffrée.
- Si le certificat est signé par une autorité de certification (CA) et que vous choisissez de fournir la chaîne de certificats, la chaîne doit être codée en PEM.
- Le certificat doit être valide au moment de son importation. Vous ne pouvez pas importer de certificat avant le début de sa période de validité et après la fin de celle-ci. Le champ de certificat `NotBefore` contient la date de début de validité et le champ `NotAfter` contient la date de fin de validité.
- Tous les matériaux de certificat requis (certificat, clé privée et chaîne de certificats) doivent être codés en PEM. Le téléchargement de matériaux encodés en DER entraîne une erreur. Pour plus d'informations et d'exemples, consultez Format de certificat et de clé pour l'importation.
- Lorsque vous renouvelez (réimportez) un certificat, vous ne pouvez pas ajouter d'extension `KeyUsage` ou `ExtendedKeyUsage` si l'extension n'était pas présente dans le certificat précédemment importé.
- AWS CloudFormation ne prend pas en charge l'importation de certificats dans ACM.

Format de certificat et de clé pour l'importation

ACM vous oblige à importer séparément le certificat, la chaîne de certificats et la clé privée (le cas échéant), et à encoder chaque composant au format PEM. PEM signifie Privacy Enhanced Mail. Le format PEM est souvent utilisé pour représenter des certificats, des demandes de certificats, des chaînes de certificats et des clés. Les fichiers PEM portent généralement l'extension `.pem`, mais ce n'est pas obligatoire.

> **Note**
>
> AWS ne fournit aucun utilitaire permettant de manipuler des fichiers PEM ou d'autres formats de certificats. Les exemples suivants s'appuient sur un éditeur de texte générique pour les opérations simples. Si vous devez effectuer des tâches plus complexes (telles que la conversion de formats de fichiers ou l'extraction de clés), vous pouvez facilement vous procurer des outils gratuits et open source tels qu'OpenSSL.

Les exemples suivants illustrent le format des fichiers à importer. Si les composants vous parviennent dans un seul fichier, utilisez un éditeur de texte (avec précaution) pour les séparer en trois fichiers.

Notez que si vous modifiez l'un des caractères d'un fichier PEM de façon incorrecte ou si vous ajoutez un ou plusieurs espaces à la fin d'une ligne, le certificat, la chaîne de certificats ou la clé privée est non valide.

Example 1. Certificat codé en PEM

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

Example 2. Chaîne de certificats codée en PEM

Une chaîne de certificats contient un ou plusieurs certificats. Vous pouvez utiliser un éditeur de texte, la commande `copy` sous Windows ou la commande Linux `cat` pour concaténer vos fichiers de certificats dans une chaîne. Les certificats doivent être concaténés dans l'ordre de façon à ce que chacun d'entre eux certifie directement celui qui le précède. Si vous importez un certificat privé, copiez le certificat racine en dernier. L'exemple suivant contient trois certificats, mais votre chaîne de certificats peut en contenir plus ou moins.

> **Important**
>
> Ne copiez pas votre certificat dans la chaîne de certificats.

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

Example 3. Clés privées codées PEM

Les certificats X.509 version 3 utilisent des algorithmes de clé publique. Lorsque vous créez un certificat X.509 ou une demande de certificat, vous spécifiez l'algorithme et la taille de clé en bits qui doivent être utilisés pour créer la paire de clés privée-publique. La clé publique est placée dans le

certificat ou la demande. Vous devez conserver secrète la clé privée qui lui est associée. Précisez la clé privée lorsque vous importez le certificat. La clé doit être non chiffrée. L'exemple ci-dessous illustre une clé privée RSA.

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

L'exemple suivant illustre une clé privée à courbes elliptiques codée en PEM. En fonction de la façon dont vous créez la clé, le bloc de paramètres peut ne pas être inclus. Si le bloc de paramètres est inclus, ACM le supprime avant d'utiliser la clé pendant le processus d'importation.

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

Importation d'un certificat

Vous pouvez importer un certificat obtenu en externe (c'est-à-dire un certificat fourni par un fournisseur de services de confiance tiers) dans ACM à l'aide de l'API AWS Management Console, de ou de l'API ACM. AWS CLI Les rubriques suivantes expliquent comment utiliser le AWS Management Console et le AWS CLI. Les procédures d'obtention d'un certificat auprès d'un AWS non-émetteur n'entrent pas dans le champ d'application de ce guide.

> **Important**
>
> L'algorithme de signature que vous avez choisi doit respecter les Conditions préalables à l'importation de certificats.

Rubriques

- Importer (console)
- Importer (AWS CLI)

Importer (console)

L'exemple suivant montre comment importer un certificat à l'aide du AWS Management Console.

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/home. S'il s'agit de la première fois que vous utilisez ACM, recherchez l'en-tête AWS Certificate Manager et cliquez sur le bouton Get Started (Démarrer) en dessous.
2. Choisissez Import a certificate. (Importer un certificat)
3. Procédez comme suit :

   a. Pour Corps du certificate, collez le certificat codé en PEM à importer. Il doit commencer par `-----BEGIN CERTIFICATE-----` et se terminer par `-----END CERTIFICATE-----`.

   b. Dans le champ Clé privée du certificat, collez la clé privée codée en PEM et non chiffrée du certificat. Elle doit commencer par `-----BEGIN PRIVATE KEY-----` et se terminer par `-----END PRIVATE KEY-----`.

   c. (Facultatif) Pour Chaîne de certificate, collez la chaîne de certificats codée en PEM.
4. (Facultatif) Pour ajouter des balises à votre certificat importé, choisissez Tags. Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Vous pouvez utiliser des balises pour organiser vos ressources ou suivre vos AWS coûts.
5. Choisissez Import (Importer).

Importer (AWS CLI)

L'exemple suivant montre comment importer un certificat à l'aide de AWS Command Line Interface (AWS CLI). Dans cet exemple il est supposé que :

- Le certificat codé en PEM est stocké dans un fichier nommé `Certificate.pem`.
- La chaîne de certificats codée en PEM est stockée dans un fichier nommé `CertificateChain.pem`.
- La clé privée non chiffrée, codée en PEM est stockée dans un fichier nommé `PrivateKey.pem`.

Pour utiliser l'exemple, remplacez les noms de fichier par les vôtres et saisissez la commande sur une seule ligne continue. L'exemple suivant inclut des sauts de ligne et des espaces supplémentaires pour en faciliter la lecture.

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

Si la commande `import-certificate` aboutit, elle renvoie le nom Amazon Resource Name (ARN) du certificat importé.

Réimportation d'un certificat

Si vous avez importé un certificat et que vous l'avez associé à d'autres AWS services, vous pouvez le réimporter avant son expiration tout en préservant les associations de AWS services du certificat d'origine. Pour plus d'informations sur AWS les services intégrés à ACM, consultezServices intégrés à AWS Certificate Manager.

Les conditions suivantes s'appliquent lorsque vous réimportez un certificat :

- Vous pouvez ajouter ou supprimer des noms de domaine.
- Vous ne pouvez pas supprimer tous les noms de domaine à partir d'un certificat.
- Si les extensions Key Usage sont présentes dans le certificat importé à l'origine, vous pouvez ajouter de nouvelles valeurs d'extension, mais vous ne pouvez pas supprimer de valeurs existantes.
- Si les extensions Extended Key Usage sont présentes dans le certificat importé à l'origine, vous pouvez ajouter de nouvelles valeurs d'extension, mais vous ne pouvez pas supprimer de valeurs existantes.
- Le type et la taille de clé ne peuvent pas être modifiés.
- Vous ne pouvez pas appliquer de balises de ressource lors de la réimportation d'un certificat.

Rubriques

Réimporter (console)

L'exemple suivant montre comment réimporter un certificat à l'aide du AWS Management Console.

1. Ouvrez la console ACM à partir de l'adresse https://console.aws.amazon.com/acm/home.

2. Sélectionnez ou développez le certificat à réimporter.
3. Ouvrez le volet des détails du certificat et cliquez sur le bouton Reimport certificate (Réimporter le certificat). Si vous avez sélectionné le certificat en cochant la case en regard de son nom, choisissez Reimport certificate (Réimporter le certificat) dans le menu Actions.
4. Pour Corps du certificat, collez le certificat d'entité finale codé en PEM.
5. Pour Clé privée du certificat, collez la clé privée codée en PEM non chiffrée associée à la clé publique du certificat.
6. (Facultatif) Pour Chaîne de certificats, collez la chaîne de certificats codée en PEM. La chaîne de certificats comprend un ou plusieurs certificats pour toutes les Autorités de certification émettrices intermédiaires et le certificat racine. Si le certificat à importer est auto-attribué, aucune chaîne de certificats n'est nécessaire.
7. Choisissez Review and import (Vérifier et importer).
8. Vérifiez les informations concernant votre certificat. Si elles ne contiennent aucune erreur, choisissez Reimport (Réimporter).

Réimporter (AWS CLI)

L'exemple suivant montre comment réimporter un certificat à l'aide de AWS Command Line Interface (AWS CLI). Dans cet exemple il est supposé que :

- Le certificat codé en PEM est stocké dans un fichier nommé `Certificate.pem`.
- La chaîne de certificats codée en PEM est stockée dans un fichier nommé `CertificateChain.pem`.
- (Certificats privés uniquement) La clé privée non chiffrée codée en PEM est stockée dans un fichier nommé `PrivateKey.pem`.
- Vous avez l'ARN du certificat que vous souhaitez réimporter.

Pour utiliser l'exemple suivant, remplacez les noms de fichier et l'ARN par les vôtres et saisissez la commande sur une seule ligne continue. L'exemple suivant inclut des sauts de ligne et des espaces supplémentaires pour en faciliter la lecture.

> **Note**
>
> Pour réimporter un certificat, vous devez spécifier son ARN.

```
$ 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
```

Si la commande `import-certificate` aboutit, elle renvoie le nom Amazon Resource Name (ARN) du certificat.

Exportation d'un certificat privé

Vous pouvez exporter un certificat émis par Autorité de certification privée AWS pour l'utiliser n'importe où dans votre environnement PKI privé. Le fichier exporté contient le certificat, la chaîne de certificats et la clé privée chiffrée. Ce fichier doit être stocké de manière sécurisée. Pour plus d'informations Autorité de certification privée AWS, consultez le Guide de AWS Private Certificate Authority l'utilisateur.

> **Note**
>
> Vous ne pouvez pas exporter un certificat approuvé publiquement ou sa clé privée, qu'il soit émis par ACM ou importé.

Rubriques

Exportation d'un certificat privé (console)

1. Connectez-vous à la console AWS de gestion et ouvrez la console ACM à l'adresse https://console.aws.amazon.com/acm/home.
2. Choisissez Certificate Manager
3. Cliquez sur le lien du certificat que vous voulez exporter.
4. Cliquez sur Exporter.
5. Entrez et confirmez une phrase secrète pour la clé privée.

   > **Note**
   >
   > Votre phrase secrète peut contenir n'importe quel caractère ASCII, à l'exception des caractères suivants : #, $ ou %.

6. Choisissez Générer l'encodage PEM.
7. Vous pouvez copier le certificat, la chaîne de certificats et la clé chiffrée dans la mémoire ou choisir Exporter dans un fichier pour chaque élément.

8. Sélectionnez Done (Exécuté).

Exportation d'un certificat privé (CLI)

Utilisez la commande export-certificate pour exporter un certificat privé et une clé privée. Vous devez attribuer une phrase secrète lorsque vous exécutez la commande. Pour plus de sécurité, vous pouvez utiliser un éditeur de fichiers pour stocker votre phrase secrète dans un fichier, puis fournir la phrase secrète à la livraison du fichier. Cela évite le stockage de votre code secret dans l'historique des commandes et empêche les autres personnes de voir le code secret lorsque vous le saisissez.

> **Note**
>
> Le fichier contenant la phrase secrète ne doit pas se terminer par une marque de fin de ligne. Vous pouvez vérifier votre fichier de mots de passe comme suit :
>
> ```
> $ file -k passphrase.txt
> passphrase.txt: ASCII text, with no line terminators
> ```

L'exemple suivant achemine la sortie de la commande vers `jq` pour appliquer le format 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)\"'
```

Cela produit un certificat codé en base64, au format PEM et contenant également la chaîne de certificats et la clé privée chiffrée, comme dans l'exemple abrégé suivant.

```
-----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-----
```

Pour la sortie de tous les éléments dans un fichier, ajoutez la redirection > à l'exemple précédent, ce qui donne le résultat suivant.

```
$ 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
```

Balisage des certificats AWS Certificate Manager

Une balise est une étiquette que vous pouvez attribuer à un certificat ACM. Chaque balise se compose d'une clé et d'une valeur. Vous pouvez utiliser la console AWS Certificate Manager, AWS Command Line Interface (AWS CLI) ou l'API ACM pour ajouter, afficher ou supprimer des balises pour les certificats ACM. Vous pouvez choisir les balises à afficher dans la console ACM.

Vous pouvez créer des balises personnalisées qui répondent à vos besoins. Par exemple, vous pouvez baliser plusieurs certificats ACM avec une balise `Environment = Prod` ou `Environment = Beta` pour identifier l'environnement auquel est destiné chaque certificat ACM. La liste suivante contient quelques exemples supplémentaires d'autres balises personnalisées :

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

D'autres ressources AWS prennent également en charge le balisage. Vous pouvez donc attribuer la même balise à différentes ressources pour indiquer si ces ressources sont liées. Par exemple, vous pouvez attribuer une balise telle que `Website = example.com` au certificat ACM, à l'équilibreur de charge et à d'autres ressources utilisées pour votre site web example.com.

Rubriques

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises des certificats ACM :

- Le nombre maximal de balises par certificat ACM est de 50.
- La longueur maximale d'une clé de balise est de 127 caractères.
- La longueur maximale d'une valeur de balise est de 255 caractères.
- Les clés et valeurs de balise sont sensibles à la casse.

- Le préfixe `aws:` est réservé à AWS. Vous ne pouvez pas ajouter, modifier ou supprimer des balises dont la clé commence par `aws:`. Les balises avec le préfixe `aws:` ne sont pas comptabilisées en fonction de la limite de balises par ressource.
- Si vous prévoyez d'utiliser votre schéma de balisage sur plusieurs services et ressources, n'oubliez pas que d'autres services peuvent avoir d'autres restrictions concernant les caractères autorisés. Reportez-vous à la documentation correspondant à ce service.
- Les balises ACM ne peuvent pas être utilisées dans les outils Resource Groups et Éditeur de balise de la AWS Management Console.

Pour plus d'informations sur les conventions de balisage AWS, consultez Balisage des ressources AWS.

Gestion des balises

Vous pouvez ajouter, modifier et supprimer des balises à l'aide d'AWS Management Console, de l'AWS Command Line Interface ou de l'API AWS Certificate Manager.

Gestion des balises (console)

Vous pouvez utiliser AWS Management Console pour ajouter, supprimer ou modifier des balises. Vous pouvez également afficher des balises dans les colonnes.

Ajout d'une balise

Utilisez la procédure suivante pour ajouter des balises à l'aide de la console ACM.

Pour ajouter une balise à un certificat (console)

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Certificate Manager sur la page https://console.aws.amazon.com/acm/home.
2. Choisissez la flèche en regard du certificat que vous voulez baliser.
3. Dans le volet des détails, faites défiler jusqu'à Tags.
4. Choisissez Edit et Add Tag.
5. Saisissez une clé et une valeur pour la balise.
6. Choisissez Enregistrer.

Suppression d'une balise

Utilisez la procédure suivante pour supprimer des balises à l'aide de la console ACM.

Pour supprimer une balise (console)

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Certificate Manager sur la page https://console.aws.amazon.com/acm/home.
2. Choisissez la flèche en regard du certificat contenant une balise que vous voulez supprimer.
3. Dans le volet des détails, faites défiler jusqu'à Tags.
4. Choisissez Edit (Modifier).
5. Choisissez le signe X en regard de la balise que vous voulez supprimer.
6. Choisissez Enregistrer.

Modification d'une balise

Utilisez la procédure suivante pour modifier des balises à l'aide de la console ACM.

Pour modifier une balise (console)

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Certificate Manager sur la page https://console.aws.amazon.com/acm/home.
2. Choisissez la flèche en regard du certificat que vous voulez modifier.
3. Dans le volet des détails, faites défiler jusqu'à Tags.
4. Choisissez Edit (Modifier).
5. Modifiez la clé ou la valeur de la balise.
6. Choisissez Enregistrer.

Affichage des balises en colonnes

Utilisez la procédure suivante pour afficher les balises en colonnes dans la console ACM.

Pour afficher les balises en colonnes (console)

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Certificate Manager sur la page https://console.aws.amazon.com/acm/home.

2. Choisissez les balises que vous voulez afficher sous forme de colonnes en choisissant l'icône en forme d'engrenage

   dans le coin supérieur droit de la console.
3. Activez la case à cocher en regard de la balise que vous voulez afficher dans une colonne.

Gestion des balises (interface CLI)

Consultez les rubriques suivantes pour apprendre à ajouter, répertorier et supprimer des balises à l'aide de l'AWS CLI.

- add-tags-to-certificate
- list-tags-for-certificate
- remove-tags-from-certificate

Gestion des balises (API ACM)

Consultez les rubriques suivantes pour apprendre à ajouter, répertorier et supprimer des balises à l'aide de l'API.

- AddTagsToCertificate (Ajouter des balises au certificat)
- ListTagsForCertificate (Liste des balises pour le certificat)
- RemoveTagsFromCertificate (Supprimer les balises du certificat)

Surveillance et journalisation AWS Certificate Manager

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Certificate Manager et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant.

Les rubriques suivantes décrivent les outils de AWS surveillance du cloud disponibles pour une utilisation avec ACM.

Rubriques

Utilisation d'Amazon EventBridge

Vous pouvez utiliser Amazon EventBridge (anciennement CloudWatch Events) pour automatiser vos AWS services et répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements liés AWS aux services, y compris ACM, sont transmis à Amazon EventBridge en temps quasi réel. Vous pouvez utiliser des événements pour déclencher des cibles, notamment des AWS Lambda fonctions, des AWS Batch tâches, des rubriques Amazon SNS, etc. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ?

Rubriques

EventBridge Support Amazon pour ACM

Cette rubrique répertorie et décrit les événements liés à l'ACM pris en charge par Amazon EventBridge.

Certificat ACM qui s'approche d'un événement d'expiration

ACM renvoie des événements quotidiens d'expiration pour tous les certificats actifs (publics, privés et importés) à partir de 45 jours avant l'expiration. Ce timing peut être modifié à l'aide PutAccountConfigurationde l'API ACM.

ACM renouvelle automatiquement les certificats éligibles qu'elle a émis, mais les certificats importés doivent être réémis et réimportés avant leur expiration pour éviter les pannes. Pour plus d'informations, consultez Réimporter un certificat. Vous pouvez utiliser les événements d'expiration pour configurer l'automatisation afin de réimporter des certificats dans ACM. Pour un exemple d'utilisation de l'automatisation AWS Lambda, voirDéclencher des actions avec Amazon EventBridge dans ACM.

La structure des événements certificat ACM qui s'approche de l'expiration est la suivante.

```
{
  "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"
  }
}
```

Événement certificat ACM expiré

> **Note**
>
> Les événements d'expiration des certificats ne sont pas disponibles pour les certificats importés.

Les clients peuvent écouter cet événement qui les avertit sur l'expiration d'un certificat public ou privé émis par ACM sur leur compte.

La structure des événements certificat ACM expiré est la suivante.

```
{
    "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
    }
 }
```

Événement certificat ACM disponible

Les clients peuvent écouter cet événement pour être avertis lorsqu'un certificat public ou privé géré est prêt pour l'utilisation. L'événement est publié lors de l'émission, du renouvellement et de l'importation. Lorsqu'un certificat privé est disponible, l'action du client est toujours requise pour le déployer sur les hôtes.

La structure des événements certificat ACM disponible est la suivante.

```
{
    "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
     }
}
```

Événement action de renouvellement du certificat ACM requis

> **Note**
>
> Action de renouvellement de certificat Les événements requis ne sont pas disponibles pour les certificats importés.

Les clients peuvent écouter cet événement pour être avertis lorsqu'une action doit être entreprise avant le renouvellement d'un certificat. Par exemple, si un client ajoute des enregistrements CAA qui empêchent le renouvellement d'un certificat par ACM, ce dernier publie cet événement en cas d'échec du renouvellement automatique 45 jours avant l'expiration. Si aucune action du client n'est entreprise, ACM effectue de nouvelles tentatives de renouvellement dans les 30 jours, 15 jours, 3 jours et 1 jour, ou jusqu'à ce que le client agisse, que le certificat expire ou qu'il ne soit plus valable pour le renouvellement. Un événement est publié pour chacune de ces tentatives de renouvellement.

La structure des événements action de renouvellement du certificat ACM requise est la suivante.

```
{
   "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 événements liés à la santé

AWS des événements de santé sont générés pour les certificats ACM éligibles au renouvellement. Pour plus d'informations sur l'éligibilité au renouvellement, consultez Renouvellement géré des certificats ACM.

Les événements Health sont générés dans deux scénarios :

- En cas de renouvellement réussi d'un certificat public ou privé.
- Quand un client doit prendre des actions pour qu'un renouvellement se produise. Il peut s'agir de cliquer sur un lien dans un message électronique (pour les certificats validés par e-mail) ou de résoudre une erreur. Un des codes d'événement suivants est inclus avec chaque événement. Les codes sont exposés sous forme de variables que vous pouvez utiliser pour le filtrage.
  - `AWS_ACM_RENEWAL_STATE_CHANGE` (le certificat a été renouvelé, a expiré ou est sur le point d'expirer)
  - `CAA_CHECK_FAILURE` (échec de la vérification CAA)
  - `AWS_ACM_RENEWAL_FAILURE` (pour les certificats signés par une autorité de certification privée)

La structure des événements d'état est la suivante. Dans cet exemple, un événement `AWS_ACM_RENEWAL_STATE_CHANGE` a été généré.

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

Déclencher des actions avec Amazon EventBridge dans ACM

Vous pouvez créer des EventBridge règles Amazon basées sur ces événements et utiliser la EventBridge console Amazon pour configurer les actions qui ont lieu lorsque les événements sont détectés. Cette section fournit des exemples de procédures pour configurer les EventBridge règles Amazon et les actions qui en résultent.

Rubriques

- Répondre à un événement avec Amazon SNS
- Répondre à un événement avec une fonction Lambda

Répondre à un événement avec Amazon SNS

Cette section explique comment configurer Amazon SNS pour envoyer une notification écrite lorsqu'ACM génère un événement d'état.

Suivez la procédure ci-dessous pour configurer une réponse.

Pour créer une EventBridge règle Amazon et déclencher une action

1. Créez une EventBridge règle Amazon. Pour plus d'informations, consultez la section Création de EventBridge règles Amazon qui réagissent aux événements.

   a. Dans la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/, accédez à la page Événements > Règles et choisissez Create rule.

   b. Sur la page Créer une règle, sélectionnez Modèle d'événement.

   c. Dans le champ Nom du service, choisissez État à partir du menu.

   d. Dans le champ Type d'événement, choisissez Événements d'état spécifiques.

   e. Sélectionnez Service(s) spécifique(s) et choisissez ACM à partir du menu.

   f. Sélectionnez Catégorie(s) de type d'événement spécifique(s) et choisissezaccountNotification.

   g. Choisissez N'importe quel code de type d'événement.

   h. Choisissez N'importe quel type de ressource.

   i. Dans l'éditeur Aperçu du modèle d'événement, collez le modèle JSON émis par l'événement. Cet exemple utilise le modèle de la section AWS événements liés à la santé.

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

2. Configurez une action.

   Dans la section Cibles, vous pouvez effectuer un choix parmi de nombreux services susceptibles d'utiliser immédiatement votre événement, comme Amazon Simple Notification Service (SNS), ou vous pouvez choisir Fonction Lambda pour transmettre l'événement à un code exécutable personnalisé. Pour obtenir un exemple d'implémentation de AWS Lambda , consultez Répondre à un événement avec une fonction Lambda.

Répondre à un événement avec une fonction Lambda

Cette procédure explique comment AWS Lambda écouter sur Amazon EventBridge, créer des notifications avec Amazon Simple Notification Service (SNS) et publier des résultats sur Amazon AWS Security Hub, offrant ainsi une visibilité aux administrateurs et aux équipes de sécurité.

Pour configurer une fonction Lambda et un rôle IAM

1. Configurez d'abord un rôle AWS Identity and Access Management (IAM) et définissez les autorisations requises par la fonction Lambda. Cette bonne pratique en matière de sécurité vous offre une certaine souplesse pour désigner la personne autorisée à appeler la fonction, et pour limiter les autorisations accordées à cette personne. Il n'est pas recommandé d'exécuter la plupart AWS des opérations directement sous un compte utilisateur et surtout pas sous un compte administrateur.

   Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Utilisez l'éditeur de stratégie JSON pour créer la stratégie définie dans le modèle ci-dessous. Indiquez votre région et les détails de votre AWS compte. Pour plus d'informations, consultez Création de stratégies sous l'onglet 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. Créez un rôle IAM et attachez la nouvelle stratégie à celui-ci. Pour plus d'informations sur la création d'un rôle IAM et l'attachement d'une politique, consultez la section Création d'un rôle pour un AWS service (console).
4. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
5. Créez la fonction Lambda. Pour plus d'informations, consultez Créer une fonction Lambda à l'aide de la console. Procédez comme suit :

   a. Sur la page Créer une fonction, choisissez l'option Créer de bout en bout afin de créer la fonction.

   b. Spécifiez un nom tel que « handle-expiring-certificates » dans le champ Nom de la fonction.

   c. Dans la liste Environnement d'exécution, choisissez Python 3.8.

   d. Développez Modifier le rôle d'exécution par défaut et choisissez Utiliser un rôle existant.

   e. Dans la liste Rôle existant, choisissez le rôle que vous avez précédemment créé.

   f. Choisissez Créer une fonction.

   g. Sous Code de fonction, insérez le code suivant :

```
# 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. Sous Variables d'environnement, choisissez Modifier et ajoutez éventuellement les variables suivantes.

- (Facultatif) EXPIRY_DAYS

  Indique le délai, en jours, avant l'envoi de l'avis d'expiration du certificat. La fonction est définie par défaut sur 45 jours, mais vous pouvez spécifier des valeurs personnalisées.

- (Facultatif) SNS_TOPIC_ARN

  Indique un ARN pour un service Amazon SNS. Entrez l'ARN complet au format arn:aws:sns:*<région>*:*<numéro-de-compte>*:*<nom-de-la-rubrique>*.

- (Facultatif) SECURITY_HUB_REGION

  Spécifie un AWS Security Hub dans une autre région. Si cela n'est pas indiqué, la région de la fonction Lambda en cours d'exécution est utilisée. Si la fonction est exécutée dans plusieurs régions, il est préférable que tous les messages de certificat soient acheminés vers le Security Hub d'une même région.

i. Sous Paramètres de base, définissez Expiration sur 30 secondes.

j. En haut de la page, choisissez Déployer.

Effectuez les tâches de la procédure suivante pour commencer à utiliser cette solution.

Pour automatiser l'envoi d'un avis d'expiration par e-mail

Dans cet exemple, nous fournissons un e-mail unique pour chaque certificat expirant au moment où l'événement est déclenché via Amazon EventBridge. Par défaut, ACM déclenche un événement par jour au cours des 45 jours qui précèdent l'expiration d'un certificat. (Cette période peut être personnalisée à l'aide du PutAccountConfigurationfonctionnement de l'API ACM.) Chacun de ces événements déclenche la cascade d'actions automatisées suivante :

```
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. Créez la fonction Lambda et configurez les autorisations. (Déjà terminé – voir Pour configurer une fonction Lambda et un rôle IAM).
2. Créez une rubrique SNS standard à utiliser par la fonction Lambda pour envoyer des notifications. Pour plus d'informations, consultez Création d'une rubrique Amazon SNS.
3. Abonnez toutes les parties intéressées à la nouvelle rubrique SNS. Pour plus d'informations, consultez Abonnement à une rubrique Amazon SNS.
4. Créez une EventBridge règle Amazon pour déclencher la fonction Lambda. Pour plus d'informations, consultez la section Création de EventBridge règles Amazon qui réagissent aux événements.

   Dans la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/, accédez à la page Événements > Règles et choisissez Create rule. Complétez les champs Nom du service, Type d'événement et Fonction Lambda. Dans l'éditeur Aperçu du modèle d'événement, collez le code suivant :

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

   Un événement tel que Lambda reçoit apparaît sous Afficher les exemples d'événements :

   ```
   {
     "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"
  }
}
```

Pour nettoyer

Une fois que vous n'avez plus besoin de l'exemple de configuration, ou de toute autre configuration, il est préférable d'en supprimer toute trace pour éviter les problèmes de sécurité et les frais imprévus :

- Politique IAM et rôle
- Fonction Lambda
- CloudWatch Règle des événements
- CloudWatch Logs associés à Lambda
- Rubrique SNS

Utilisation CloudTrail avec AWS Certificate Manager

AWS Certificate Manager est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans ACM. CloudTrail est activé par défaut sur votre AWS compte. CloudTrail capture les appels d'API pour ACM sous forme d'événements, y compris les appels depuis la console ACM et les appels de code vers les opérations de l'API ACM. Si vous configurez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour ACM. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à ACM, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements. Lorsqu'une activité événementielle prise en charge se produit dans ACM, cette activité est enregistrée dans un

CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS .

En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence.

Pour plus d'informations CloudTrail, consultez la documentation suivante :

- AWS CloudTrail Guide de l'utilisateur.
- Présentation de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Rubriques

- Actions de l'API ACM prises en charge dans la journalisation CloudTrail
- Journalisation des appels d'API pour les services intégrés

Actions de l'API ACM prises en charge dans la journalisation CloudTrail

ACM prend en charge l'enregistrement des actions suivantes sous forme d'événements dans des fichiers CloudTrail journaux :

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été faite avec des informations d'identification utilisateur Utilisateur racine d'un compte AWS ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez l'élément CloudTrailUserIdentity.

Les sections suivantes fournissent des exemples de journaux pour les opérations d'API prises en charge.

- Ajout de balises à un certificat (AddTagsToCertificate)
- Suppression d'un certificat (DeleteCertificate)
- Description d'un certificat (DescribeCertificate)
- Exportation d'un certificat (ExportCertificate)
- Importation d'un certificat (ImportCertificate)
- Établissement d'une liste de certificats (ListCertificates)
- Établissement d'une liste de balises pour un certificat (ListTagsForCertificate)
- Suppression de balises dans un certificat (RemoveTagsFromCertificate)
- Demande de certificat (RequestCertificate)
- Renvoi d'un e-mail de validation (ResendValidationEmail)
- Récupération d'un certificat (GetCertificate)

Ajout de balises à un certificat (AddTagsToCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
    }
 ]
}
```

Suppression d'un certificat (DeleteCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
      }
   ]
}
```

Description d'un certificat (DescribeCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'DescribeCertificateAPI.

> **Note**
>
> Le CloudTrail journal de l'`DescribeCertificate`opération n'affiche aucune information sur le certificat ACM que vous spécifiez. Vous pouvez consulter les informations relatives au certificat à l'aide de la console, de ou de l'DescribeCertificateAPI. AWS Command Line Interface

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

Exportation d'un certificat (ExportCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
```

```
         }
      }
   ]
}
```

Importation d'un certificat (ImportCertificate)

L'exemple suivant montre l'entrée du CloudTrail journal qui enregistre un appel à l'opération d'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"
```

```
}
```

Établissement d'une liste de certificats (ListCertificates)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'ListCertificatesAPI.

> **Note**
>
> Le CloudTrail journal de l'`ListCertificates`opération n'affiche pas vos certificats ACM. Vous pouvez consulter la liste des certificats à l'aide de la console, de ou de l'ListCertificatesAPI. AWS Command Line Interface


```
{
   "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"
```

```
      }
   ]
}
```

Établissement d'une liste de balises pour un certificat (ListTagsForCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'ListTagsForCertificateAPI.

> **Note**
>
> Le CloudTrail journal de l'`ListTagsForCertificate`opération n'affiche pas vos tags. Vous pouvez consulter la liste des balises à l'aide de la console, de ou de l'ListTagsForCertificateAPI. AWS Command Line Interface

```
{
   "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"
```

```
      }
   ]
}
```

Suppression de balises dans un certificat (RemoveTagsFromCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
      }
   ]
```

```
}
```

Demande de certificat (RequestCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
      }
   ]
}
```

Renvoi d'un e-mail de validation (ResendValidationEmail)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
      }
   ]
}
```

Récupération d'un certificat (GetCertificate)

L' CloudTrail exemple suivant montre les résultats d'un appel à l'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"
      }
   ]
}
```


Journalisation des appels d'API pour les services intégrés

Vous pouvez l'utiliser CloudTrail pour auditer les appels d'API effectués par les services intégrés à ACM. Pour plus d'informations sur l'utilisation CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur. Les exemples suivants illustrent les types de journaux qui peuvent être générés en fonction des ressources AWS sur lesquelles vous approvisionnez le certificat ACM.

Rubriques

- Création d'un équilibreur de charge

Création d'un équilibreur de charge

Vous pouvez l'utiliser CloudTrail pour auditer les appels d'API effectués par les services intégrés à ACM. Pour plus d'informations sur l'utilisation CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur. Les exemples suivants montrent les types de journaux qui peuvent être générés en fonction des AWS ressources sur lesquelles vous fournissez le certificat ACM.

Rubriques

- Création d'un équilibreur de charge
- Enregistrement d'une instance Amazon EC2 auprès d'un équilibreur de charge
- Déchiffrement d'une clé privée
- Déchiffrement d'une clé privée

Création d'un équilibreur de charge

L'exemple suivant illustre un appel à la fonction `CreateLoadBalancer` effectué par une utilisatrice IAM nommée Alice. Le nom de l'équilibreur de charge est `TestLinuxDefault`, et l'écouteur est créé à l'aide d'un certificat 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"
}
```

Enregistrement d'une instance Amazon EC2 auprès d'un équilibreur de charge

Lorsque vous approvisionnez votre site web ou votre application sur une instance Amazon Elastic Compute Cloud (Amazon EC2), vous devez informer l'équilibreur de charge de l'existence de cette instance. Pour ce faire, vous pouvez utiliser la console Elastic Load Balancing ou le AWS Command Line Interface. L'exemple suivant montre un appel à un équilibreur `RegisterInstancesWithLoadBalancer` de charge nommé LinuxTest sur le AWS compte 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"
}
```

Déchiffrement d'une clé privée

L'exemple suivant illustre un appel à `Encrypt` qui chiffre la clé privée associée à un certificat ACM. Le chiffrement est effectué dans 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"
      }
   ]
}
```

Déchiffrement d'une clé privée

L'exemple suivant illustre un appel à `Decrypt` qui déchiffre la clé privée associée à un certificat ACM. Le déchiffrement est effectué à l'intérieur AWS, et la clé déchiffrée ne sort jamais. 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 Métriques prises en charge

Amazon CloudWatch est un service de surveillance des AWS ressources. Vous pouvez l'utiliser CloudWatch pour collecter et suivre les métriques, définir des alarmes et réagir automatiquement aux modifications de vos AWS ressources. ACM publie des métriques une fois par jour pour chaque certificat d'un compte jusqu'à son expiration.

L'espace de noms `AWS/CertificateManager` inclut la métrique suivante.

Métrique	Description	Unité	Dimensions
`DaysToExpiry`	Nombre de jours avant l'expiration	Entier	CertificateArn

Métrique	Description	Unité	Dimensions
	d'un certificat. ACM cesse de publier cette métrique après l'expiration d'un certificat.		• Valeur : ARN du certificat

Pour plus d'informations sur CloudWatch les métriques, consultez les rubriques suivantes :

- Utilisation d'Amazon CloudWatch Metrics
- Création d' CloudWatchalarmes Amazon

Utilisation de l'API (exemples Java)

Vous pouvez utiliser l'API AWS Certificate Manager pour interagir par programmation avec le service en envoyant des demandes HTTP. Pour plus d'informations, consultez la AWS Certificate Manager API Reference (Référence d'API).

En plus de l'API web (ou de l'API HTTP), vous pouvez utiliser les kits SDK AWS et les outils de ligne de commande pour interagir avec ACM et d'autres services. Pour plus d'informations, veuillez consulter Outils pour Amazon Web Services.

Les rubriques suivantes vous montrent comment utiliser l'un des kits SDK AWS, le kitAWS SDK for Java, pour effectuer les opérations disponibles dans l'API AWS Certificate Manager.

Rubriques

Ajout de balises à un certificat

L'exemple suivant montre comment utiliser la fonction 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);
     }
}
```

Suppression d'un certificat

L'exemple suivant montre comment utiliser la fonction DeleteCertificate. En cas de réussite, la fonction renvoie un ensemble vide {}.

```
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);

   }
}
```

Description d'un certificat

L'exemple suivant montre comment utiliser la fonction 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);

   }
}
```

En cas de réussite, l'exemple précédent affiche des informations similaires à ce qui suit.

```
{
    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,
    }
}
```

Exportation d'un certificat

L'exemple suivant montre comment utiliser la fonction ExportCertificate. La fonction exporte un certificat privé. émis par une autorité de certification (CA) privée au format PKCS #8. (Il n'est pas possible d'exporter des certificats publics, qu'ils soient émis ou importés.) Elle exporte également la chaîne de certificats et la clé privée. Dans l'exemple, la phrase passe de la clé est stockée dans un fichier local.

```
package com.amazonaws.samples;

import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
import com.amazonaws.services.certificatemanager.AWSCertificateManager;


import com.amazonaws.services.certificatemanager.model.ExportCertificateRequest;
import com.amazonaws.services.certificatemanager.model.ExportCertificateResult;

import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.InvalidTagException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;

import java.io.FileNotFoundException;
import java.io.IOException;
import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
```

```
import java.nio.channels.FileChannel;

public class ExportCertificate {

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

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

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

      // Initialize a file descriptor for the passphrase file.
      RandomAccessFile file_passphrase = null;

      // Initialize a buffer for the passphrase.
      ByteBuffer buf_passphrase = null;

      // Create a file stream for reading the private key passphrase.
      try {
         file_passphrase = new RandomAccessFile("C:\\Temp\\password.txt", "r");
      }
      catch (IllegalArgumentException ex) {
         throw ex;
      }
      catch (SecurityException ex) {
         throw ex;
      }
      catch (FileNotFoundException ex) {
         throw ex;
      }
```

```
      // Create a channel to map the file.
      FileChannel channel_passphrase = file_passphrase.getChannel();

      // Map the file to the buffer.
      try {
         buf_passphrase = channel_passphrase.map(FileChannel.MapMode.READ_ONLY, 0,
channel_passphrase.size());

         // Clean up after the file is mapped.
         channel_passphrase.close();
         file_passphrase.close();
      }
      catch (IOException ex)
      {
         throw ex;
      }

      // Create a request object.
      ExportCertificateRequest req = new ExportCertificateRequest();

      // Set the certificate ARN.
      req.withCertificateArn("arn:aws:acm:region:account:"
            +"certificate/M12345678-1234-1234-1234-123456789012");

      // Set the passphrase.
      req.withPassphrase(buf_passphrase);

      // Export the certificate.
      ExportCertificateResult result = null;

      try {
         result = client.exportCertificate(req);
      }
      catch(InvalidArnException ex)
      {
         throw ex;
      }
      catch (InvalidTagException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
```

```
        }

        // Clear the buffer.
        buf_passphrase.clear();

        // Display the certificate and certificate chain.
        String certificate = result.getCertificate();
        System.out.println(certificate);

        String certificate_chain = result.getCertificateChain();
        System.out.println(certificate_chain);

        // This example retrieves but does not display the private key.
        String private_key = result.getPrivateKey();
    }
}
```

Récupération d'un certificat et d'une chaîne de certificats

L'exemple suivant montre comment utiliser la fonction 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'exemple précédent crée une sortie similaire à ce qui suit :

```
{Certificate: -----BEGIN CERTIFICATE-----
    base64-encoded certificate
-----END CERTIFICATE-----,
CertificateChain: -----BEGIN CERTIFICATE-----
    base64-encoded certificate chain
-----END CERTIFICATE-----
}
```

Importation d'un certificat

L'exemple suivant montre comment utiliser la fonction 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);
    }
}
```

Établissement de la liste des certificats

L'exemple suivant montre comment utiliser la fonction 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'exemple précédent crée une sortie similaire à ce qui suit :

```
{
    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
    }]
}
```

Renouvellement d'un certificat

L'exemple suivant illustre comment utiliser la fonction RenewCertificate. La fonction renouvelle un certificat privé émis par une autorité de certification (CA) privée et exporté avec la fonction ExportCertificate. À l'heure actuelle, seuls les certificats privé exportés peuvent être renouvelés avec cette fonction. Pour renouveler vos certificats avec Autorité de certification privée AWS, vous devez d'abord accorder les autorisations appropriées au principal du service ACM. Pour plus d'informations, consultez Octroi d'autorisations de renouvellement de certificats à ACM.

```
package com.amazonaws.samples;

import com.amazonaws.AmazonClientException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.regions.Regions;

import com.amazonaws.services.certificatemanager.AWSCertificateManagerClientBuilder;
```

```
import com.amazonaws.services.certificatemanager.AWSCertificateManager;

import com.amazonaws.services.certificatemanager.model.RenewCertificateRequest;
import com.amazonaws.services.certificatemanager.model.RenewCertificateResult;


import com.amazonaws.services.certificatemanager.model.InvalidArnException;
import com.amazonaws.services.certificatemanager.model.ResourceNotFoundException;
import com.amazonaws.services.certificatemanager.model.ValidationException;

import java.io.FileNotFoundException;
import java.io.IOException;
import java.io.RandomAccessFile;
import java.nio.ByteBuffer;
import java.nio.channels.FileChannel;

public class RenewCertificate {

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

      // Retrieve your credentials from the C:\Users\name\.aws\credentials file in
 Windows
      // or the ~/.aws/credentials in Linux.
      AWSCredentials credentials = null;
      try {
          credentials = new ProfileCredentialsProvider().getCredentials();
      }
      catch (Exception ex) {
          throw new AmazonClientException("Cannot load your credentials from file.",
 ex);
      }

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


      // Create a request object and specify the ARN of the certificate to renew.
      RenewCertificateRequest req = new RenewCertificateRequest();
      req.withCertificateArn("arn:aws:acm:region:account:"
            +"certificate/M12345678-1234-1234-1234-123456789012");
```

```
      // Renew the certificate.
      RenewCertificateResult result = null;
      try {
         result = client.renewCertificate(req);
      }
      catch(InvalidArnException ex)
      {
         throw ex;
      }
      catch (ResourceNotFoundException ex)
      {
         throw ex;
      }
      catch (ValidationException ex)
      {
         throw ex;
      }

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

Établissement de la liste des balises de certificat

L'exemple suivant montre comment utiliser la fonction 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'exemple précédent crée une sortie similaire à ce qui suit :

```
{Tags: [{Key: Purpose,Value: Test}, {Key: Short_Name,Value: My_Cert}]}
```

Suppression de balises dans un certificat

L'exemple suivant montre comment utiliser la fonction 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);
   }
}
```

Demande de certificat

L'exemple suivant illustre comment utiliser la fonction DeleteCertificate.

```
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'exemple précédent crée une sortie similaire à ce qui suit :

```
{CertificateArn:
 arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012}
```

Renvoi d'un e-mail de validation

L'exemple suivant montre comment utiliser la fonction 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'exemple précédent renvoie votre e-mail de validation et affiche un ensemble vide.

Résolution des problèmes

Si vous rencontrez des problèmes lors de l'utilisation d' AWS Certificate Manager, consultez les rubriques suivantes.

> **Note**
>
> Si votre problème n'est pas traité dans cette section, nous vous recommandons de consulter le Centre de connaissances AWS.

Rubriques

Résolution des problèmes liés aux demandes de certificat

Consultez les rubriques suivantes si vous rencontrez des problèmes lors d'une demande de certificat ACM.

Rubriques

Dépassement du délai d'attente de la demande de certificat

Les demandes de certificats ACM expirent si elles ne sont pas validées dans les 72 heures. Pour corriger cette condition, ouvrez la console, recherchez l'enregistrement du certificat, cochez la case correspondante, choisissez Actions, puis sélectionnez Supprimer. Puis choisissez Actions et Demander un certificat pour recommencer. Pour plus d'informations, consultez Validation DNS ou

Validation par courriel. Nous vous recommandons d'utiliser la validation DNS dans la mesure du possible.

Échec de la demande de certificat

Si votre demande échoue, ACM et vous-même recevez l'un des messages d'erreur ci-dessous. Suivez les étapes suggérées pour résoudre le problème. Vous ne pouvez pas soumettre à nouveau une demande de certificat ayant échoué. Une fois que vous avez résolu le problème, vous devez envoyer une nouvelle demande.

Rubriques

Message d'erreur : Aucun contact disponible

Vous avez choisi la validation par courriel dans le cadre d'une demande de certificat, mais ACM n'a pas trouvé d'adresse électronique à utiliser pour valider un ou plusieurs noms de domaine contenus dans la demande. Pour résoudre ce problème, vous pouvez procéder de l'une des manières suivantes :

- Vérifiez que vous avez une adresse électronique de travail enregistrée dans WHOIS et que cette adresse apparaît lorsque vous effectuez une recherche WHOIS standard sur les noms de domaine figurant dans la demande de certificat. En général, vous utilisez pour cela votre registre de domaine.
- Vérifiez que votre domaine est configuré pour recevoir des courriels. Le serveur de noms de votre domaine doit disposer d'un enregistrement MX pour que les serveurs de messagerie d'ACM sachent où envoyer le courriel de validation de domaine.

L'une des tâches précédentes suffit pour résoudre ce problème. Il est inutile d'effectuer les deux. Une fois que vous avez résolu le problème, demandez un nouveau certificat.

Pour plus d'informations sur la façon de vous assurer que vous recevez les courriel de validation de domaine d'ACM, consultez (Facultatif) Configuration d'une adresse électronique pour votre

domaine ou Non-réception du courriel de validation. Si vous suivez ces étapes et que vous continuez à obtenir le message Aucun contact disponible, signalez le problème à AWS pour que nous puissions l'examiner.

Message d'erreur : Vérification supplémentaire nécessaire

ACM requiert davantage d'informations pour traiter cette demande de certificat. Cela se produit en tant que mesure de protection contre la fraude si votre domaine se classe dans les 1 000 meilleurs sites web d'Alexa. Pour fournir ces informations, utilisez le Centre de support pour contacter AWS Support. Si vous n'avez pas de plan de support, publiez un nouveau fil de discussion dans le forum de discussion ACM.

> **Note**
>
> Vous ne pouvez pas demander de certificat pour des noms de domaine qui sont la propriété d'Amazon, par exemple ceux qui se terminent par amazonaws.com, cloudfront.net ou elasticbeanstalk.com.

Message d'erreur : Domaine public non valide

Un ou plusieurs noms de domaine figurant dans la demande de certificat ne sont pas valides. En général, cela provient du fait qu'un nom de domaine figurant dans la demande ne correspond pas à un domaine de niveau supérieur valide. Essayez de renouveler votre demande de certificat, en corrigeant les fautes d'orthographe ou de frappe qui existaient dans la demande qui a échoué et assurez-vous que tous les noms de domaine figurant dans la demande correspondent à des domaines de niveau supérieur valides. Par exemple, vous ne pouvez pas demander de certificat ACM pour example.invalidpublicdomain, car « invalidpublicdomain » n'est pas un domaine de niveau supérieur valide. Si vous continuez à recevoir ce motif d'échec, contactez le Centre de Support. Si vous n'avez pas de plan de support, publiez un nouveau fil de discussion dans le forum de discussion ACM.

Message d'erreur : Autre

En règle générale, cet échec se produit lorsqu'un ou plusieurs noms de domaine figurant dans la demande de certificat contient une coquille. Essayez de renouveler votre demande de certificat en corrigeant les fautes d'orthographe ou de frappe qui existaient dans la demande qui a échoué. Si vous continuez à recevoir ce motif d'échec, utilisez le Centre de Support pour contacter AWS

Support. Si vous n'avez pas de plan de support, publiez un nouveau fil de discussion dans le forum de discussion ACM.

Résolution des problèmes liés à la validation des certificats

Si le statut de la demande de certificat ACM est Validation en attente, la demande est en attente d'une action de votre part. Si vous avez choisi la validation par courriel lorsque vous avez fait la demande, vous ou un représentant autorisé devez répondre aux courriels de validation. Ces messages ont été envoyés aux adresses des contacts WHOIS enregistrés et aux autres adresses électroniques courantes du domaine demandé. Pour de plus amples informations, consultez Validation par courriel. Si vous avez choisi la validation DNS, vous devez écrire l'enregistrement CNAME créé pour vous par ACM dans votre base de données DNS. Pour de plus amples informations, consultez Validation DNS.

> **Important**
>
> Vous devez valider que vous possédez ou contrôlez chaque nom de domaine que vous avez inclus dans votre demande de certificat. Si vous avez choisi la validation par courriel, vous recevrez des courriels de validation pour chaque domaine. Si ce n'est pas le cas, consultez Non-réception du courriel de validation. Si vous choisissez la validation DNS, vous devez créer un enregistrement CNAME pour chaque domaine.

> **Note**
>
> Les certificats ACM publics peuvent être installés sur des instances Amazon EC2 connectées à une enclave Nitro, mais pas à d'autres instances Amazon EC2. Pour plus d'informations sur la configuration d'un serveur web autonome sur une instance Amazon EC2 non connectée à une enclave Nitro, consultez Tutoriel : Installation d'un serveur web LAMP sur Amazon Linux 2 ou Tutoriel : Installation d'un serveur web LAMP avec une AMI Amazon Linux.

Nous vous recommandons d'utiliser la validation DNS plutôt que la validation par courriel.

Consultez les rubriques suivantes si vous rencontrez des problèmes de validation.

Rubriques

Résolution des problèmes liés à la validation DNS

Consultez les conseils suivants si vous rencontrez des problèmes pour valider un certificat avec DNS.

La première étape du dépannage DNS consiste à vérifier l'état actuel de votre domaine à l'aide d'outils tels que les suivants :

- dig – Linux, Windows
- nslookup – Linux, Windows
- whois – Linux, Windows

Rubriques

Traits de soulignement interdits par le fournisseur DNS

Si votre fournisseur DNS interdit les traits de soulignement de début dans les valeurs CNAME, vous pouvez supprimer le trait de soulignement de la valeur fournie par ACM et valider votre domaine sans lui. Par exemple, la valeur CNAME `_x2.acm-validations.aws` peut être modifiée en `x2.acm-validations.aws` à des fins de validation. Toutefois, le paramètre de nom CNAME doit toujours commencer par un trait de soulignement de début.

Vous pouvez utiliser une des valeurs figurant dans la partie droite du tableau ci-dessous pour valider un domaine.

Nom	Type	Valeur
_<random value>.example.com.	CNAME	_<random value>.acm-validations.aws.
_<random value>.example.com.	CNAME	<random value>.acm-validations.aws.

Point final par défaut ajouté par le fournisseur DNS

Certains fournisseurs DNS ajoutent par défaut un point final à la valeur CNAME que vous fournissez. Par conséquent, si vous ajoutez vous-même un point, une erreur se produit. Par exemple, « `<random_value>.acm-validations.aws.` » est rejeté alors que « `<random_value>.acm-validations.aws` » est accepté.

Validation DNS en GoDaddy cas d'échec

La validation DNS des domaines enregistrés auprès de Godaddy et d'autres registres peut échouer si vous ne modifiez pas les valeurs CNAME fournies par ACM. Prenant example.com comme nom de domaine, l'enregistrement CNAME émis a la forme suivante :

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

Vous pouvez créer un enregistrement CNAME compatible avec GoDaddy en tronquant le domaine apex (y compris le point) à la fin du champ NAME, comme suit :

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

La console ACM n'affiche pas le bouton « Créer des enregistrements dans Route 53 »

Si vous sélectionnez Amazon Route 53 comme fournisseur DNS, vous AWS Certificate Manager pouvez interagir directement avec celui-ci pour valider la propriété de votre domaine. Dans certains cas, le bouton Créer des enregistrements dans Route 53 de la console peut ne pas être disponible lorsque vous l'attendez. Si cela se produit, passez en revue les causes possibles suivantes.

- Vous n'utilisez pas Route 53 comme fournisseur DNS.

- Vous êtes connecté à ACM et Route 53 via différents comptes.
- Vous ne disposez pas des autorisations IAM requises pour créer des enregistrements dans une zone hébergée par Route 53.
- Vous ou quelqu'un d'autre a déjà validé le domaine.
- Le domaine n'est pas accessible publiquement.

Échec de la validation Route 53 sur les domaines privés (non approuvés).

Lors de la validation DNS, ACM recherche un CNAME dans une zone hébergée publiquement. Lorsqu'il n'en trouve pas, il expire au bout de 72 heures avec le statut Validation expirée. Vous ne pouvez pas l'utiliser pour héberger des enregistrements DNS pour des domaines privés, y compris des ressources dans une zone hébergée privée Amazon VPC, des domaines non approuvés dans votre PKI privée et des certificats auto-signés.

AWS fournit un support pour les domaines publics non fiables via le Autorité de certification privée AWSservice.

La validation est réussie mais l'émission ou le renouvellement échoue

Si l'émission du certificat échoue avec la mention « Validation en attente » même si le DNS est correct, vérifiez que l'émission n'est pas bloquée par un enregistrement d'autorisation de l'autorité de certification (CAA). Pour plus d'informations, consultez (Facultatif) Configuration d'un enregistrement CAA.

Échec de la validation auprès d'un serveur DNS sur un VPN

Si vous localisez un serveur DNS sur un VPN et qu'ACM ne parvient pas à valider un certificat auprès de ce dernier, déterminez si le serveur est publiquement accessible. L'émission de certificats publics à l'aide de la validation DNS ACM nécessite que les enregistrements de domaine puissent être résolus sur l'Internet public.

Résolution des problèmes liés à la validation par courriel

Consultez les conseils suivants si vous rencontrez des problèmes pour valider le domaine d'un certificat par courriel.

Rubriques

- Non-réception du courriel de validation

- Courriel envoyé au sous-domaine
- Informations de contact masquées
- Renouvellement de certificats
- Limitation WHOIS
- Horodatage initial persistant pour la validation par courriel
- Résolution des problèmes liés au domaine de premier niveau .IO
- Je n'arrive pas à passer à la validation DNS

Non-réception du courriel de validation

Lorsque vous demandez un certificat à ACM et que vous choisissez la validation par courriel, le courriel de validation de domaine est envoyé aux trois adresses de contact indiquées dans la base de données WHOIS et à cinq adresses administratives courantes. Pour de plus amples informations, consultez Validation par courriel. Si vous rencontrez des problèmes de réception du courriel de validation, consultez les suggestions qui suivent.

Où chercher le courriel

Le courriel de validation est envoyé aux adresses de contact répertoriées dans WHOIS et aux adresses administratives courantes du domaine. Aucun e-mail n'est envoyé au propriétaire du AWS compte, sauf si celui-ci est également répertorié comme contact de domaine dans le WHOIS. Consultez la liste des adresses e-mail affichées dans la console ACM (ou renvoyées par l'interface CLI ou l'API) pour déterminer où vous devez rechercher le courriel de validation. Pour consulter la liste, cliquez sur l'icône en regard du nom de domaine dans la case Validation non terminée.

Le courriel est marqué comme courrier indésirable

Recherchez le courriel de validation dans votre dossier Courrier indésirable.

GMail trie automatiquement vos courriels

Si vous utilisez Gmail, le courriel de validation a peut-être été automatiquement trié dans les onglets Mises à jour ou Promotions.

Le registre de domaine n'affiche pas d'informations sur le contact ou la protection de la confidentialité est activée

Dans certains cas, le titulaire du nom de domaine ainsi que les contacts techniques et administratifs dans le WHOIS ne sont pas accessibles au public et ne peuvent AWS donc pas

joindre ces contacts. Vous pouvez choisir de configurer votre registre pour qu'il répertorie votre adresse électronique dans WHOIS, mais les registres ne prennent pas tous cette option en charge. Vous pouvez être contraint d'apporter la modification directement dans le registre de votre domaine. Dans d'autres cas, les informations de contact du domaine peuvent utiliser une adresse de confidentialité, telle que celles fournies via WhoisGuard ou PrivacyGuard.

Pour les domaines achetés auprès de Route 53, la protection de la confidentialité est activée par défaut et votre adresse e-mail est mappée à une adresse électronique `whoisprivacyservice.org`, `contact.gandi.net`, ou `identity-protect.org` l'adresse email. Vérifiez que votre adresse électronique d'inscrit figurant dans le fichier avec votre registre de domaine est à jour afin que le courriel envoyé à ces adresses électroniques masquées puisse être envoyé à une adresse électronique que vous contrôlez.

> **Note**
>
> La protection de la confidentialité de certains domaines achetés auprès de Route 53 est activée, même si vous choisissez de rendre vos informations de contact publiques. Par exemple, la protection de la confidentialité du domaine de premier niveau .ca ne peut pas être désactivée par programmation par Route 53. Vous devez contacter le AWS Centre de support pour lui demander de désactiver la protection de la confidentialité.

Si les coordonnées du contact courriel pour votre domaine ne sont pas disponibles via WHOIS ou que le courriel envoyé aux coordonnées du contact n'atteint pas le propriétaire du domaine ou un représentant autorisé, nous vous recommandons de configurer votre domaine ou sous-domaine pour recevoir le courriel envoyé à une ou plusieurs adresses administratives courantes comprenant le préfixe admin@, administrator@, hostmaster@, webmaster@ et postmaster@ au nom du domaine demandé. Pour plus d'informations sur la configuration d'un courriel pour votre domaine, consultez la documentation de votre fournisseur de services de messagerie et suivez les instructions indiquées à l'adresse (Facultatif) Configuration d'une adresse électronique pour votre domaine. Si vous utilisez Amazon WorkMail, consultez la section Travailler avec les utilisateurs dans le manuel Amazon WorkMail Administrator Guide.

Après voir mis à disposition au moins une des huit adresses électronique auxquelles AWS envoie un courriel de validation et avoir confirmé que vous pouvez recevoir un courriel pour cette adresse, vous êtes prêt à demander un certificat via ACM. Une fois que vous avez créé une demande de certificat, vérifiez que l'adresse électronique prévue s'affiche dans la liste des adresses électroniques dans AWS Management Console. Pendant que le certificat a l'état

Validation en attente, vous pouvez développer la liste pour l'afficher en cliquant sur l'icône en regard du nom de domaine dans la case Validation non terminée. Vous pouvez aussi afficher la liste à l'Étape 3 : Validation de l'Assistant ACM Demander un certificat. Les adresses électroniques répertoriées sont celles auxquelles le courriel a été envoyé.

Enregistrements MX manquants ou configurés de façon incorrecte

Un enregistrement MX est un enregistrement de ressource situé dans la base de données du système de noms de domaine (DNS), qui spécifie un ou plusieurs serveurs de messagerie qui acceptent les courriels pour votre domaine. Si votre enregistrement MX est manquant ou mal configuré, aucun courriel ne peut être envoyé à l'une des cinq adresses d'administration système courantes indiquées à la section Validation par courriel. Corrigez ce problème d'enregistrement MX manquant ou mal configuré et essayez de renvoyer le courriel ou de redemander votre certificat.

> **Note**
>
> Actuellement, nous vous recommandons de patienter au moins une heure avant d'essayer de renvoyer le courriel ou de demander votre certificat.

> **Note**
>
> Pour éviter d'exiger un enregistrement MX, vous pouvez utiliser l'`ValidationDomain`option de l'RequestCertificateAPI ou la AWS CLI commande request-certificate pour spécifier le nom de domaine auquel ACM envoie des e-mails de validation. Si vous utilisez l'API ou le AWS CLI, AWS n'effectue pas de recherche MX.

Contacter le Centre de support

Si, après avoir consulté les conseils précédents, vous ne recevez toujours pas le courriel de validation de domaine, accédez au Centre de support AWS Support et créez un cas. Si vous n'avez pas de contrat d'assistance, envoyez un message au Forum de discussion ACM.

Courriel envoyé au sous-domaine

Si vous utilisez la console et que vous effectuez une demande de certificat pour un nom de sous-domaine, par exemple `sub.test.example.com`, ACM vérifie s'il existe un enregistrement

MX pour `sub.test.example.com`. Sinon, le domaine parent `test.example.com` est ensuite vérifié et ainsi de suite, jusqu'au domaine de base `example.com`. Si un enregistrement MX est trouvé, la recherche s'arrête et un courriel de validation est envoyé aux adresses administratives courantes pour le sous-domaine. Ainsi, par exemple, si un enregistrement MX est trouvé pour `test.example.com`, un courriel est envoyé à admin@test.example.com, administrator@test.example.com et aux autres adresses administratives indiquées dans Validation par courriel. Si aucun enregistrement MX n'est trouvé dans tous les sous-domaines, un courriel est envoyé au sous-domaine pour lequel vous avez initialement demandé le certificat. Pour une discussion approfondie sur la configuration de votre courriel et sur le fonctionnement d'ACM avec DNS et la base de données WHOIS, consultez (Facultatif) Configuration d'une adresse électronique pour votre domaine.

Au lieu d'utiliser la console, vous pouvez utiliser l'`ValidationDomain`option de l'RequestCertificateAPI ou la AWS CLI commande request-certificate pour spécifier le nom de domaine auquel ACM envoie des e-mails de validation. Si vous utilisez l'API ou le AWS CLI, AWS n'effectue pas de recherche MX.

Informations de contact masquées

Un problème fréquent survient lorsque vous tentez de créer un nouveau certificat. Certains registres vous permettent de masquer vos informations de contact dans votre liste WHOIS. D'autres vous permettent de remplacer vos adresses de messagerie réelles par une adresse privée (ou proxy). Cela vous empêche de recevoir un courriel de validation à vos adresses de contact enregistrées.

Pour recevoir le courriel, vérifiez que vos informations de contact sont publiques dans WHOIS ou si votre liste WHOIS affiche une adresse électronique confidentielle, assurez-vous que le courriel envoyé à cette adresse est transmis à votre adresse électronique réelle. Une fois la configuration de votre base de données WHOIS terminée, et tant que votre demande de certificat n'a pas expiré, vous pouvez choisir de renvoyer le courriel de validation. ACM effectue une nouvelle recherche WHOIS/MX et envoie un courriel de validation à votre adresse de contact désormais publique.

Renouvellement de certificats

Si vous avez rendu vos informations WHOIS publiques lors de la demande d'un nouveau certificat et que vous avez ensuite masqué ces informations, ACM ne retrouvera pas les adresses de contact enregistrées lorsque vous tenterez de renouveler votre certificat. ACM envoie un courriel de validation à ces adresses de contact et à cinq adresses administratives courantes formées à partir de votre enregistrement MX. Pour résoudre ce problème, rendez à nouveau vos informations WHOIS

publiques et renvoyez les courriels de validation. ACM effectue une nouvelle recherche WHOIS/MX et envoie un courriel de validation à vos adresses de contact désormais publiques.

Limitation WHOIS

Parfois, ACM ne parvient pas à contacter le serveur WHOIS, même après l'envoi de plusieurs demandes de courriel de validation. Ce problème est externe à AWS. Cela signifie que AWS ne contrôle pas les serveurs WHOIS et ne peut pas empêcher la limitation du serveur WHOIS. Si vous rencontrez ce problème, créez une demande auprès du AWS Support Centre qui vous aidera à le contourner.

Horodatage initial persistant pour la validation par courriel

L'horodatage de la première demande de validation par courriel d'un certificat persiste lors des demandes ultérieures de renouvellement de la validation. Ceci n'est pas une preuve d'une erreur dans les opérations ACM.

Résolution des problèmes liés au domaine de premier niveau .IO

Le domaine de premier niveau .IO est attribué au Territoire britannique de l'océan Indien. Actuellement, le registre des domaines n'affiche pas vos informations publiques provenant de la base de données WHOIS. Ceci demeure vrai, que vous disposiez d'un service de protection de la vie privée activé ou désactivé. Les bureaux d'enregistrement peuvent afficher ces informations dans leurs propres sorties WHOIS si la protection de la confidentialité est désactivée, mais cette pratique varie d'un bureau d'enregistrement à l'autre. ACM ne peut pas envoyer d'e-mail de validation aux trois adresses de contact enregistrées suivantes si elles ne sont pas disponibles auprès du bureau d'enregistrement dans WHOIS.

- Inscrit au domaine
- Contact technique
- Contact administratif

ACM envoie cependant un courriel de validation aux cinq adresses d'administration système courantes suivantes, où *votre_domaine* correspond au nom de domaine que vous avez saisi lors de la demande initiale de certificat tandis que `.io` correspond au domaine de premier niveau.

- administrator@*votre_domaine*.io
- hostmaster@*votre_domaine*.io

- postmaster@*votre_domaine*.io
- webmaster@*votre_domaine*.io
- admin@*votre_domaine*.io

Pour recevoir un courriel de validation pour un domaine .IO, vérifiez que l'un de vos cinq comptes de messagerie ci-dessus est activé. Sinon, vous ne recevrez pas d courriel de validation et aucun certificat ACM ne vous sera délivré.

> **Note**
>
> Nous vous recommandons d'utiliser la validation DNS plutôt que la validation par courriel. Pour plus d'informations, consultez Validation DNS.

Je n'arrive pas à passer à la validation DNS

Une fois que vous avez créé un certificat avec une validation par e-mail, vous ne pouvez pas passer à sa validation avec DNS.

Résolution des problèmes liés au renouvellement géré des certificats

ACM essaie de renouveler automatiquement vos certificats ACM avant qu'ils expirent, afin qu'aucune action ne soit requise de votre part. Si vous rencontrez des problèmes liés au Renouvellement géré des certificats ACM, consultez les rubriques suivantes.

Préparation de la validation automatique de domaine

Pour qu'ACM puisse renouveler automatiquement vos certificats, les conditions suivantes doivent être remplies :

- Votre certificat doit être associé à un AWS service intégré à ACM. Pour en savoir plus sur les ressources prises en charge par ACM, consultez Services intégrés à AWS Certificate Manager.
- Pour les certificats validés par courriel, ACM doit pouvoir vous joindre à une adresse électronique d'administrateur pour chaque domaine répertorié dans votre certificat. Les adresses électroniques qui seront essayées sont répertoriées dans Validation par courriel.

- Pour les certificats validés par le DNS, assurez-vous que votre configuration DNS contient les registres CNAME corrects, comme décrit dans Validation DNS.

Traitement des échecs de renouvellement géré des certificats

Lorsque le certificat arrive à expiration (60 jours pour le DNS, 45 jours pour EMAIL et 60 jours pour le mode privé), ACM tente de le renouveler s'il répond aux critères d'éligibilité. Vous devrez peut-être prendre des mesures pour que le renouvellement réussisse. Pour plus d'informations, consultez Renouvellement géré des certificats ACM.

Renouvellement géré des certificats pour les certificats validés par courriel

Les certificats ACM sont valides pendant 13 mois (395 jours). Pour renouveler les certificats validés par e-mail, une action est requise de la part du propriétaire du domaine. ACM commence à envoyer des avis de renouvellement 45 jours avant l'expiration, en utilisant les adresses de boîte aux lettres WHOIS du domaine et cinq adresses d'administrateur communes. Les notifications contiennent un lien sur lequel le propriétaire du domaine peut cliquer pour un renouvellement facile. Une fois tous les domaines répertoriés validés, ACM émet un certificat renouvelé avec le même ARN.

Consultez Valider par courriel pour obtenir des instructions sur l'identification des domaines qui sont à l'état `PENDING_VALIDATION` et répétez le processus de validation pour ces domaines.

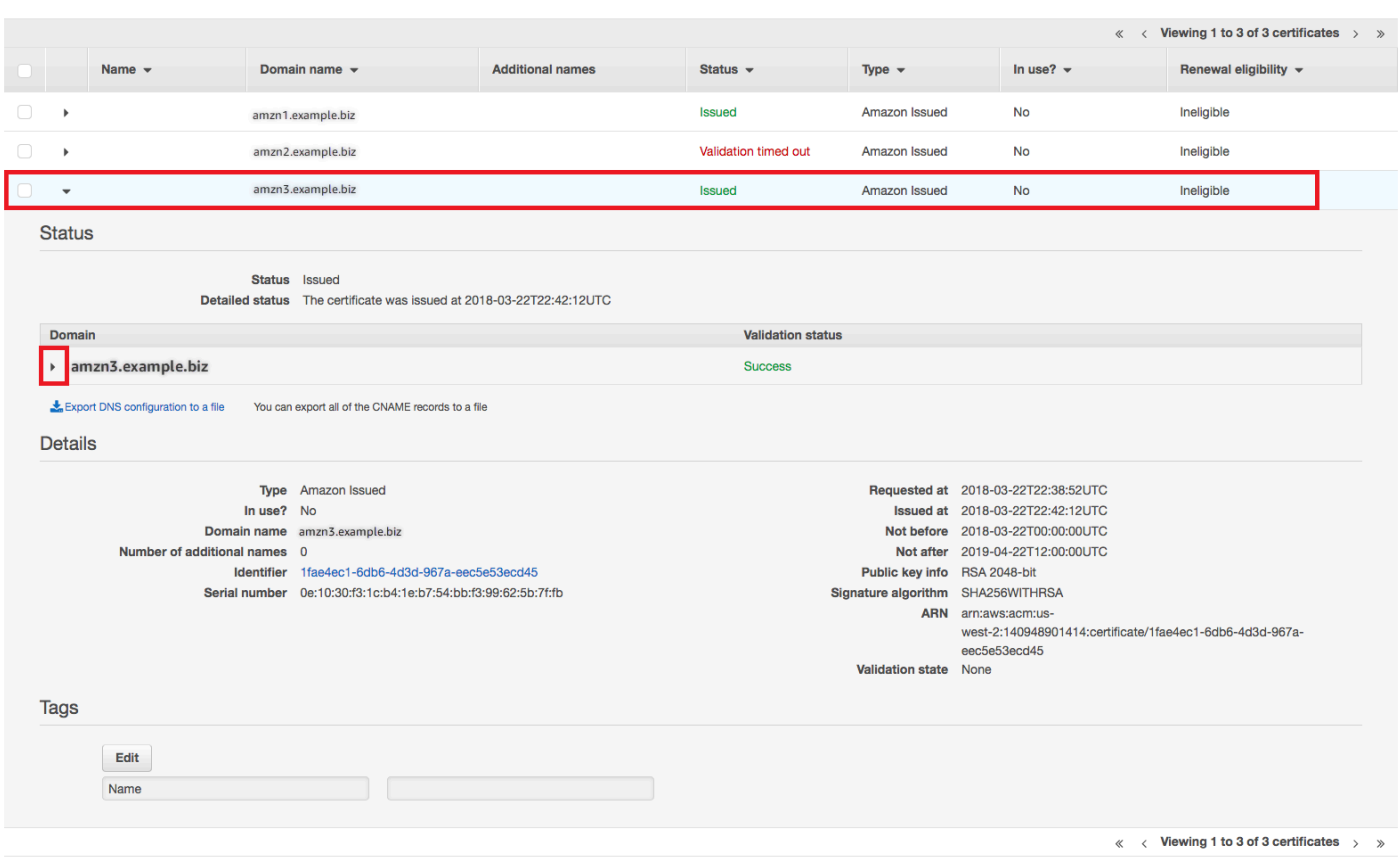
Renouvellement géré des certificats pour les certificats validés par DNS

ACM ne tente pas de validation TLS pour les certificats validés par DNS. Si ACM ne parvient pas à renouveler un certificat qui a fait l'objet d'une validation DNS, cela est probablement dû à des enregistrements CNAME manquants ou inexacts dans votre configuration DNS. Dans ce cas, ACM vous informe que le certificat n'a pas pu être renouvelé automatiquement.

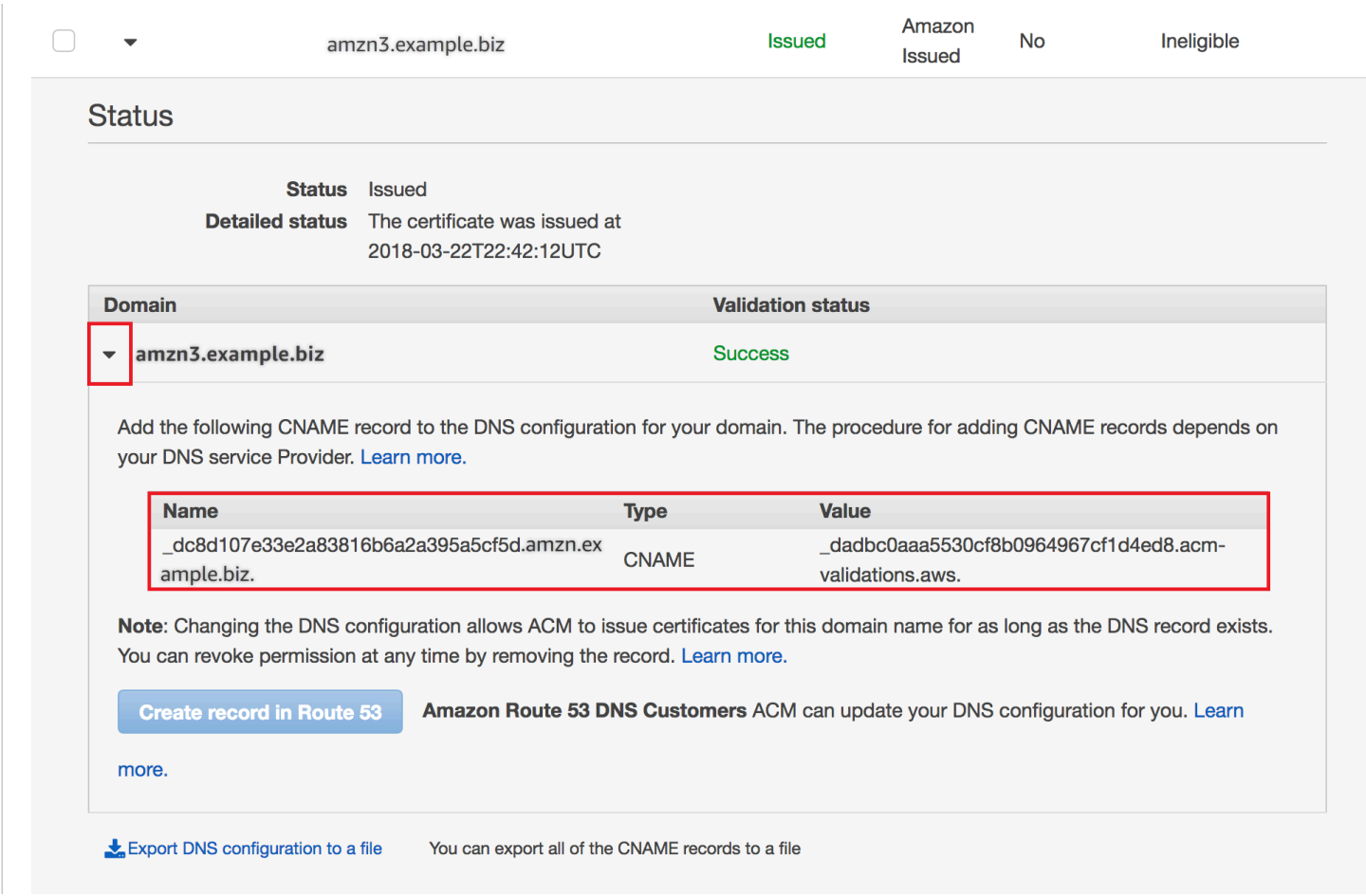
> **Important**
>
> Vous devez insérer les enregistrements CNAME corrects dans votre base de données DNS. Consultez votre bureau d'enregistrement de domaine pour savoir comment procéder.

Vous trouverez les enregistrements CNAME pour vos domaines en développant votre certificat et ses entrées de domaine dans la console ACM. Consultez les figures ci-dessous pour plus d'informations. Vous pouvez également récupérer des enregistrements CNAME à l'aide de

l'DescribeCertificateopération de l'API ACM ou de la commande describe-certificate de la CLI ACM. Pour plus d'informations, consultez Validation DNS.



Choisissez le certificat cible à partir de la console.



Développez la fenêtre de certificat pour trouver les informations CNAME du certificat.

Si le problème persiste, contactez le Centre de support.

Présentation des délais de renouvellement

Renouvellement géré des certificats ACM est un processus asynchrone. Cela signifie que les étapes ne se succèdent pas immédiatement. Une fois tous les noms de domaine d'un certificat ACM validés, un certain temps peut s'écouler avant qu'ACM n'obtienne le nouveau certificat. Un délai supplémentaire peut se produire entre le moment où ACM obtient le certificat renouvelé et le moment où ce certificat est déployé sur les ressources AWS qui l'utilisent. Par conséquent, l'affichage des modifications apportées à l'état du certificat dans la console peut prendre jusqu'à plusieurs heures.

Résolution d'autres problèmes

Cette section contient des conseils relatifs à des problèmes non liés à la délivrance ou à la validation des certificats ACM.

Rubriques

Problèmes d'autorisation de l'autorité de certification (CAA)

Vous pouvez utiliser des enregistrements DNS CAA afin de spécifier que l'autorité de certification Amazon peut émettre des certificats ACM pour votre domaine ou sous-domaine. Si vous recevez une erreur lors de l'émission du certificat indiquant La validation a échoué pour un ou plusieurs domaines en raison d'une erreur d'autorisation de l'autorité de certification (CAA), vérifiez vos enregistrements DNS de CAA. Si vous recevez cette erreur alors que votre demande de certificat a été validée, vous devez mettre à jour vos enregistrements CAA et demander un nouveau certificat. Le champ de value (valeur) de votre enregistrement CAA doit comporter l'un des noms de domaine suivants :

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

Pour plus d'informations sur la création d'un enregistrement CAA, consultez (Facultatif) Configuration d'un enregistrement CAA.

> **Note**
>
> Vous pouvez choisir de ne pas configurer un registre CAA pour votre domaine si vous ne souhaitez pas activer la vérification de CAA.

Problèmes liés à l'importation de certificat

Vous pouvez importer des certificats tiers dans ACM et les associer à des services intégrés. Si vous rencontrez des problèmes, passez en revue les rubriques consacrées aux prérequis et aux formats de certificats. Notez en particulier les éléments suivants :

- Vous pouvez importer uniquement les certificats SSL/TLS X.509 version 3.
- Votre certificat peut être auto-signé ou signé par une autorité de certification (CA).
- Si votre certificat est signé par une autorité de certification, vous devez inclure une chaîne de certificats intermédiaire qui fournit un chemin d'accès à la racine de l'autorité.
- Si votre certificat est auto-signé, vous devez inclure la clé privée en texte brut.
- Chaque certificat de la chaîne doit directement certifier celui qui le précède.
- N'incluez pas votre certificat d'entité finale dans la chaîne de certificats intermédiaire.
- Votre certificat, la chaîne de certificats et la clé privée (le cas échéant) doivent être codés PEM. En général, le codage PEM se compose de blocs de texte ASCII codé en Base64 qui commencent et se terminent par des lignes d'en-tête et de pied de page en texte brut. Vous ne devez pas ajouter de lignes ou d'espaces ni apporter d'autres modifications à un fichier PEM lors de sa copie ou de son téléchargement. Vous pouvez vérifier les chaînes de certificats à l'aide de l'utilitaire de vérification OpenSSL.
- Votre clé privée (le cas échéant) ne doit pas être chiffrée. (Astuce : si elle comporte une phrase secrète, celle-ci est chiffrée).
- Les services intégrés à ACM doivent utiliser des algorithmes et des tailles de clé pris en charge par ACM. Consultez le guide de l' AWS Certificate Manager utilisateur et la documentation de chaque service pour vous assurer que votre certificat fonctionnera.
- La prise en charge des certificats par les services intégrés peut varier selon que le certificat est importé dans IAM ou dans ACM.
- Le certificat doit être valide au moment de l'importation.
- Les informations détaillées de l'ensemble de vos certificats sont affichées dans la console. Par défaut, toutefois, si vous appelez l'ListCertificatesAPI ou la AWS CLI commande list-certificates sans spécifier le `keyTypes` filtre, seuls `RSA_1024` les `RSA_2048` certificats sont affichés.

Problèmes d'épinglage de certificat

Pour renouveler un certificat, ACM génère une nouvelle paire de clés publiques-privées. Si votre application utiliseÉpinglage de certificat, ce que l'on appelle parfois l'épinglage SSL, pour épingler

un certificat ACM, il est possible qu' AWS elle ne puisse pas se connecter à votre domaine après le renouvellement du certificat. C'est pourquoi nous vous recommandons de ne pas épingler de certificat ACM. Si votre application doit épingler un certificat, vous pouvez procéder comme suit :

- Importez votre propre certificat dans ACM, puis épinglez votre application au certificat importé. ACM ne fournit pas de renouvellement géré pour les certificats importés.
- Si vous utilisez un certificat public, épinglez votre application à tous les Amazon root certificates (certificats racines Amazon) disponibles. Si vous utilisez un certificat privé, épinglez votre application au certificat racine de votre CA.

Problèmes liés à API Gateway

Lorsque vous déployez un point de terminaison d'API optimisé pour les périphériques, API Gateway configure une CloudFront distribution pour vous. La CloudFront distribution appartient à API Gateway, et non à votre compte. La distribution est liée au certificat ACM que vous avez utilisé lors du déploiement de votre API. Pour supprimer la liaison et autoriser ACM à supprimer votre certificat, vous devez supprimer le domaine personnalisé API Gateway qui est associé au certificat.

Lorsque vous déployez un point de terminaison d'API régional, API Gateway crée un équilibreur de charge d'application ALB (Application Load Balancer) en votre nom. L'équilibreur de charge appartient à API Gateway et n'est pas visible par vous. L'équilibreur de charge d'application est lié au certificat ACM que vous avez utilisé lors du déploiement de votre API. Pour supprimer la liaison et autoriser ACM à supprimer votre certificat, vous devez supprimer le domaine personnalisé API Gateway qui est associé au certificat.

Que faire lorsqu'un certificat de travail échoue de manière inattendue ?

Si vous avez correctement associé un certificat ACM à un service intégré, mais que le certificat cesse de fonctionner et que le service intégré commence à renvoyer des erreurs, la cause peut être une modification des autorisations dont le service a besoin pour utiliser un certificat ACM.

Par exemple, Elastic Load Balancing (ELB) nécessite une autorisation pour déchiffrer un fichier AWS KMS key qui, à son tour, déchiffre la clé privée du certificat. Cette autorisation est accordée par une politique basée sur les ressources qu'ACM applique lorsque vous associez un certificat à ELB. Si ELB perd l'octroi de cette autorisation, il échouera la prochaine fois qu'il tentera de déchiffrer la clé du certificat.

Pour étudier le problème, vérifiez l'état de vos subventions à l'aide de la AWS KMS console à l'adressehttps://console.aws.amazon.com/kms. Puis effectuez l'une des opérations suivantes :

- Si vous pensez que les autorisations octroyées à un service intégré ont été révoquées, accédez à la console du service intégré, dissociez le certificat du service, puis associez-le à nouveau. Cela permettra de réappliquer la stratégie basée sur les ressources et de mettre en place un nouvel octroi.
- Si vous pensez que les autorisations accordées à ACM ont été révoquées, contactez l' AWS Support adresse https://console.aws.amazon.com/support/home#/.

Problèmes liés au rôle lié à un service (SLR) ACM

Lorsque vous émettez un certificat signé par une autorité de certification privée qui a été partagé avec vous par un autre compte, ACM tente, lors de la première utilisation, de configurer un rôle lié à un service (SLR) afin d'interagir en tant que principal avec une Autorité de certification privée AWS politique d'accès basée sur les ressources. Si vous émettez un certificat privé à partir d'une autorité de certification partagée et que le rôle SLR n'est pas en place, ACM ne sera pas en mesure de renouveler automatiquement ce certificat.

ACM peut vous avertir qu'il ne peut pas déterminer si un rôle SLR existe sur votre compte. Si l'autorisation `iam:GetRole` requise a déjà été accordée au rôle SLR ACM pour votre compte, l'alerte ne se reproduira pas après la création du rôle SLR. Si elle se reproduit, vous ou votre administrateur de compte devrez peut-être accorder l'autorisation `iam:GetRole` à ACM, ou associer votre compte à la stratégie `AWSCertificateManagerFullAccess` gérée par ACM.

Pour de plus amples informations, veuillez consulter Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM

Gestion des exceptions

Une AWS Certificate Manager commande peut échouer pour plusieurs raisons. Pour de plus amples informations sur chaque exception, veuillez consulter le tableau ci-dessous.

Gestion des exceptions de certificat privé

Les exceptions suivantes peuvent se produire lorsque vous tentez de renouveler un certificat PKI privé émis par Autorité de certification privée AWS.

> **Note**
>
> Autorité de certification privée AWS n'est pas pris en charge dans les régions Chine (Pékin) et Chine (Ningxia).

Code d'échec ACM	Comment
`PCA_ACCESS_DENIED`	L'autorité de certification privée n'a pas accordé d'autorisations ACM. Cela déclenche un code Autorité de certification privée AWS `AccessDeniedException` d'échec. Pour remédier au problème, accordez les autorisations nécessaires au principal du service ACM à l'aide de l' Autorité de certification privée AWS CreatePermissionopération.
`PCA_INVALID_DURATION`	La période de validité du certificat demandé dépasse la période de validité de l'autorité de certification privée émettrice. Cela déclenche un code Autorité de certification privée AWS `ValidationException` d'échec. Pour résoudre le problème, installez un nouveau certificat d'autorité de certification avec une période de validité appropriée.
`PCA_INVALID_STATE`	L'état de l'autorité de certification privée appelée n'est pas correct pour effectuer l'opération ACM demandée. Cela déclenche un code Autorité de certification privée AWS `InvalidStateException` d'échec. Résolvez le problème comme suit : • Si l'autorité de certification a le statut `CREATING`, attendez que la création se

Code d'échec ACM	Comment
	termine, puis installez le certificat d'une autorité de certification. • Si l'autorité de certification a le statut `PENDING_CERTIFICATE` , installez le certificat d'une autorité de certification. • Si l'autorité de certification a un statut `DISABLED`, mettez-le à jour en lui attribuant l'état `ACTIVE`. • Si l'autorité de certification a un statut `DELETED`, restaurez-le. • Si l'autorité de certification a un statut `EXPIRED`, installez un nouveau certificat • Si l'autorité de certification a un statut `FAILED` et que vous ne pouvez pas résoudre le problème, contactez AWS Support.
`PCA_LIMIT_EXCEEDED`	L'autorité de certification privée a atteint un quota d'émission. Cela déclenche un code Autorité de certification privée AWS `LimitExceededException` d'échec. Essayez de répéter votre demande avant de continuer avec cette aide. Si l'erreur persiste, contactez AWS Support pour demander une augmentation du quota.
`PCA_REQUEST_FAILED`	Une erreur réseau ou système s'est produite. Cela déclenche un code Autorité de certification privée AWS `RequestFailedException` d'échec. Essayez de répéter votre demande avant de continuer avec cette aide. Si vous obtenez toujours la même erreur, contactez AWS Support.

Code d'échec ACM	Comment
PCA_RESOURCE_NOT_FOUND	L'autorité de certification privée a été définitivement supprimée. Cela déclenche un code Autorité de certification privée AWS `ResourceNotFoundException` d'échec. Vérifiez que vous avez utilisé l'ARN correct. Si cela échoue, vous ne pourrez pas utiliser cette autorité de certification. Pour remédier au problème, créez une nouvelle autorité de certification.
SLR_NOT_FOUND	Afin de renouveler un certificat signé par une autorité de certification privée résidant dans un autre compte, ACM doit disposer d'un rôle lié à un service (SLR) sur le compte où réside le certificat. Si vous devez recréer un rôle SLR supprimé, consultez Création du rôle SLR pour ACM.

Concepts

Cette section fournit les définitions des concepts utilisés par AWS Certificate Manager.

Rubriques

Certificat ACM

ACM génère des certificats X.509 version 3. Chacun d'eux est valide pendant 13 mois (395 jours) et contient les extensions suivantes.

- Contraintes élémentaires : indique si l'objet du certificat est une autorité de certification (CA)
- Authority Key Identifier (Identifiant de clé d'autorité) : permet l'identification de la clé publique qui correspond à la clé privée utilisée pour signer le certificat.

- Subject Key Identifier (Identificateur de clé d'objet) : permet l'identification des certificats qui contiennent une clé publique particulière.
- Key Usage (Utilisation de la clé) : définit l'objectif de la clé publique intégrée dans le certificat.
- Extended Key Usage (Utilisation étendue de la clé) : spécifie un ou plusieurs objectifs pour lesquels la clé publique peut être utilisée en plus des objectifs spécifiés par l'extension Key Usage (Utilisation de la clé).
- CRL Distribution Points (Points de distribution CRL) : indique où obtenir les informations CRL.

Le texte brut d'un certificat émis par ACM se présente comme dans l'exemple suivant :

```
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
```

Autorités de certification racine ACM

Les certificats d'entité finale publics émis par ACM tirent leur approbation des autorités de certification racine Amazon suivantes :

Nom unique	Algorithme de chiffrement
CN=Amazon Root CA 1, O=Amazon, C=US	2048 bits RSA (`RSA_2048`)
CN=Amazon Root CA 2, O=Amazon, C=US	4096 bits RSA (`RSA_4096`)
CN=Amazon Root CA 3, O=Amazon, C=US	Elliptic Prime Curve 256 bits (`EC_prime256v1`)
CN=Amazon Root CA 4, O=Amazon, C=US	Elliptic Prime Curve 384 bits (`EC_secp384r1`)

La racine de confiance par défaut pour les certificats émis par ACM est CN=Amazon Root CA 1,O=Amazon,C=US, qui offre une sécurité RSA 2048 bits. Les autres racines sont réservées à une utilisation future. Toutes les racines sont signées par le certificat de l'autorité de certification racine (Root Certificate Authority) Starfield Services.

Pour de plus amples informations, veuillez consulter Amazon Trust Services.

Domaine apex

veuillez consulter Noms de domaine.

Chiffrement à clé asymétrique

Contrairement à la Chiffrement à clé symétrique, le chiffrement asymétrique utilise des clés différentes mais mathématiquement liées pour chiffrer et déchiffrer le contenu. L'une des clés est publique, et elle est généralement mise à disposition dans un certificat X.509 v3. L'autre clé est privée, et elle est stockée de manière sécurisée. Le certificat X.509 lie l'identité d'un utilisateur, d'un ordinateur ou d'une autre ressource (l'objet du certificat) à la clé publique.

Les certificats ACM sont des certificats SSL/TLS X.509 qui lient l'identité de votre site web et les détails de votre organisation à la clé publique contenue dans le certificat. ACM utilise votre AWS KMS key pour chiffrer la clé privée. Pour plus d'informations, consultez Sécurité des clés privées des certificats.

Autorité de certification

Une autorité de certification (CA) est une entité qui émet des certificats numériques. Dans le commerce, le type le plus courant de certificat numérique repose sur la norme ISO X.509. L'autorité de certification émet des certificats numériques signés qui affirment l'identité de l'objet du certificat et lient cette identité à la clé publique figurant dans le certificat. En règle générale, l'autorité de certification gère la révocation du certificat.

Journalisation de transparence des certificats

Pour assurer une protection contre les certificats SSL/TLS qui sont émis par erreur ou par une CA compromise, certains navigateurs exigent que les certificats publics émis pour votre domaine soient enregistrés dans un journal de transparence de certificats. Le nom de domaine est enregistré. La clé privée ne l'est pas. Les certificats qui ne sont pas consignés génèrent normalement une erreur dans le navigateur.

Vous pouvez surveiller les journaux pour vous assurer que seuls les certificats que vous avez autorisés ont été émis pour votre domaine. Vous pouvez utiliser un service tel que Certificate Search pour vérifier les journaux.

Avant que la CA Amazon émette un certificat SSL/TLS approuvé publiquement pour votre domaine, elle soumet le certificat à au moins trois serveurs de journaux de transparence des certificats. Ces serveurs ajoutent le certificat dans leurs bases de données publiques et renvoient un horodatage de certificat signé (SCT) à la CA Amazon. La CA intègre alors ce SCT dans le certificat, signe le certificat et vous le délivre. Les horodatages sont inclus avec les autres extensions 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 journalisation de transparence des certificats est automatique lorsque vous demandez ou renouvelez un certificat, sauf si vous choisissez de refuser ce processus. Pour plus d'informations sur le refus de la journalisation, consultez Refus de la journalisation de transparence des certificats.

Système de noms de domaine

Le système de noms de domaine (DNS) est un système d'attribution de noms distribué hiérarchique pour les ordinateurs et autres ressources connectés à Internet ou un réseau privé. DNS est utilisé principalement pour convertir les noms de domaine textuels, tels que `aws.amazon.com`, en adresses IP (Internet Protocol) numériques, sous la forme `111.122.133.144`. En revanche, la base de données DNS de votre domaine contient un certain nombre d'enregistrements qui peuvent être utilisé à d'autres fins. Par exemple, avec ACM, vous pouvez utiliser un enregistrement CNAME pour confirmer que vous possédez ou contrôlez un domaine lorsque vous demandez un certificat. Pour plus d'informations, consultez Validation DNS.

Noms de domaine

Un nom de domaine est une chaîne de texte telle que `www.example.com`, qui peut être convertie par le système de noms de domaine (DNS) en adresse IP. Les réseaux informatiques, y compris Internet, utilisent des adresses IP plutôt que des noms textuels. Un nom de domaine se compose d'étiquettes distinctes séparées par des points :

TLD

L'étiquette la plus à droite est appelée « domaine de premier niveau » (TLD). Parmi les exemples courants, citons `.com`, `.net` et `.edu`. En outre, pour les entités enregistrées dans certains pays, le domaine de premier niveau est une abréviation du nom du pays et est appelé « code pays ». Il peut s'agir, par exemple, de `.uk` pour le Royaume-Uni, de `.ru` pour la Russie, et de `.fr` pour la France. Lorsque des codes pays sont utilisés, une hiérarchie de deuxième niveau est souvent introduite pour le domaine de premier niveau afin d'identifier le type de l'entité enregistrée. Par exemple, le domaine de premier niveau `.co.uk` identifie les entreprises commerciales au Royaume-Uni.

Domaine apex

Le nom du domaine apex inclut le domaine de premier niveau et se construit à partir de ce dernier. Pour les noms de domaines qui comprennent un code pays, le domaine apex inclut le code et les étiquettes, le cas échéant, qui identifient le type de l'entité enregistrée. Le domaine apex n'inclut pas les sous-domaines (voir le paragraphe suivant). Dans `www.example.com`, le nom du domaine apex est `example.com`. Dans `www.example.co.uk`, le nom du domaine apex est `example.co.uk`. Les autres noms souvent utilisés en lieu et place d'apex sont notamment : base, simple, racine, apex racine ou zone apex.

Sous-domaine

Les noms de sous-domaine précèdent le nom du domaine apex et sont séparés de celui-ci et les uns des autres par un point. Le nom de sous-domaine le plus courant est `www`, mais n'importe quel nom est possible. Les noms de sous-domaine peuvent avoir plusieurs niveaux. Par exemple, dans `jake.dog.animals.example.com`, les sous-domaines sont `jakedog` et `animals`, dans cet ordre.

Superdomaine

Domaine auquel appartient un sous-domaine.

FQDN

Le nom de domaine complet (FQDN) est le nom DNS complet d'un ordinateur, d'un site Web ou d'une autre ressource connectée à un réseau ou à Internet. Par exemple, `aws.amazon.com` est le nom de domaine complet d'Amazon Web Services. Un nom de domaine complet inclut tous les domaines jusqu'au domaine de premier niveau. Par exemple, $[subdomain_1].[subdomain_2]...[subdomain_n].[apex\ domain].[top\text{-}level\ domain]$ représente le format général d'un nom de domaine complet.

PQDN

Un nom de domaine qui n'est pas entièrement qualifié est appelé « nom de domaine partiellement qualifié » (PQDN), et il s'agit d'un nom ambigu. Un nom comme $[subdomain_1.subdomain_2.]$ est un nom de domaine partiellement qualifié parce que le domaine racine ne peut pas être déterminé.

Inscription

Le droit d'utiliser un nom de domaine est délégué par des bureaux d'enregistrement de nom de domaine. Ces bureaux sont généralement accrédités par l'ICANN (Internet Corporation for

Assigned Names and Numbers). En outre, d'autres outils appelés registres conservent les bases de données des domaines de premier niveau. Lorsque vous demandez un nom de domaine, le bureau d'enregistrement envoie vos informations au registre du domaine de premier niveau approprié. Le registre attribue un nom de domaine, met à jour la base de données du domaine de premier niveau et publie vos informations sur WHOIS. Généralement, les noms de domaine doivent être achetés.

Chiffrement et déchiffrement

Le chiffrement est le processus qui assure la confidentialité des données. Le déchiffrement inverse le processus et récupère les données d'origine. Les données non chiffrées sont généralement appelées « texte brut », qu'il s'agisse de texte ou non. Les données chiffrées sont généralement appelées « texte chiffré ». Le chiffrement HTTPS des messages entre les clients et les serveurs utilise des algorithmes et des clés. Les algorithmes définissent la step-by-step procédure par laquelle les données en texte brut sont converties en texte chiffré (chiffrement) et le texte chiffré est reconverti en texte clair d'origine (décryptage). Les clés sont utilisées par les algorithmes pendant le processus de chiffrement ou de déchiffrement. Les clés peuvent être publiques ou privées.

Nom de domaine complet (FQDN)

veuillez consulter Noms de domaine.

Infrastructure à clés publiques (ICP)

Une infrastructure à clés publiques (ICP) se compose des matériels, logiciels, personnes, stratégies, documents et procédures nécessaires pour créer, émettre, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques. L'ICP facilite le transfert sécurisé des informations sur les réseaux informatiques.

Certificat racine

Une autorité de certification (CA) appartient généralement à une structure hiérarchique qui contient plusieurs autres autorités de certification liées par des relations parent-enfant clairement établies. Les autorités de certification subordonnées sont certifiées par leurs autorités de certification parent, ce qui crée une chaîne de certificats. L'autorité de certification située en haut de la hiérarchie est appelée l'autorité de certification racine, et son certificat est appelé le certificat racine. En général, ce certificat est auto-signé.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) et Transport Layer Security (TLS) sont des protocoles cryptographiques qui assurent la sécurité des communications sur un réseau informatique. TLS est le successeur de SSL. Ils utilisent tous deux des certificats X.509 pour authentifier le serveur. Les deux protocoles négocient une clé symétrique entre le client et le serveur, qui sert à chiffrer les données circulant entre les deux entités.

HTTPS sécurisé

HTTPS signifie HTTP via SSL/TLS, une forme sécurisée de HTTP prise en charge par tous les navigateurs et serveurs principaux. Toutes les demandes et réponses HTTP sont chiffrées avant d'être envoyées sur un réseau. HTTPS combine le protocole HTTP avec les techniques cryptographiques symétriques, asymétriques et basées sur le certificat X.509. HTTPS fonctionne en insérant une couche de sécurité cryptographique sous la couche d'application HTTP et au-dessus de la couche de transport TCP dans le modèle Open Systems Interconnection (OSI). La couche de sécurité utilise le protocole Secure Sockets Layer (SSL) ou le protocole Transport Layer Security (TLS).

Certificats de serveur SSL

Les transactions HTTPS requièrent des certificats de serveur pour authentifier un serveur. Un certificat de serveur est une structure de données X.509 v3 qui lie la clé publique figurant dans le certificat à l'objet du certificat. Le certificat SSL/TLS est signé par une autorité de certification (CA) et contient, entre autres, le nom du serveur, la période de validité, la clé publique et l'algorithme de signature.

Chiffrement à clé symétrique

Le chiffrement à clé symétrique utilise la même clé pour chiffrer et déchiffrer les données numériques. Voir aussi Chiffrement à clé asymétrique.

protocole TLS (Transport Layer Security)

veuillez consulter Secure Sockets Layer (SSL).

Approbation

Pour permettre à un navigateur Web d'approuver l'identité d'un site Web, le navigateur doit être en mesure de vérifier le certificat de ce site. Toutefois, les navigateurs n'approuvent qu'un petit nombre de certificats appelés certificats d'autorité de certification racine. Un tiers de confiance, appelé autorité de certification (CA), valide l'identité du site Web et émet un certificat numérique signé pour l'opérateur du site Web. Le navigateur peut ensuite vérifier la signature numérique afin de valider l'identité du site Web. Si la validation aboutit, le navigateur affiche une icône de verrouillage dans la barre d'adresse.

Historique du document

Le tableau suivant décrit l'historique des publications de la AWS Certificate Manager documentation depuis 2018.

Modification	Description	Date
Obsolète de la validation des e-mails par l'échangeur de courrier (MX)	ACM ne prend plus en charge l'échangeur de courrier (MX). Utilisez plutôt la validatio n DNS ou spécifiez un superdomaine pour recevoir la validation par e-mail.	27 juin 2024
Ajouter les meilleures pratiques en matière de séparation au niveau des comptes	Utilisez la séparation au niveau du compte dans vos polices dans la mesure du possible. Si cela n'est pas possible, vous pouvez restreindre les autorisations au niveau du compte ou via des clés de condition de contexte de chiffrement dans vos politiques.	11 juin 2024
Prochaine dépréciation de la vérification des e-mails WHOIS	Ajout d'une note concernant la dépréciation de la vérification des e-mails WHOIS à compter de juin 2024.	5 février 2024
Ajout d'un support de clé de condition	Ajout de la prise en charge des clés de condition IAM lors de la demande de certifica ts ACM. Pour afficher la liste des types de conditions prises en charge, consultez https://	24/08/2023

	docs.aws.amazon.com/acm/latest/userguide/acm-conditions.html#acm-conditions-supported.	
Ajout de la prise en charge d'ECDSA	Ajout de la prise en charge du Elliptic Curve Digital Signature Algorithm (ECDSA) lors de la demande d'un certificat public ACM. Pour obtenir la liste des algorithmes de clés pris en charge, consultez https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate.html#algorithms.	8 novembre 2022
Nouveaux CloudWatch événements	Ajout d'un certificat ACM expiré, certificat ACM disponible et evénements nécessitant une action de renouvellement du certificat ACM. Pour obtenir la liste des CloudWatch événements pris en charge, consultezhttps://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	27 octobre 2022

Mise à jour des types d'algorithmes de clés pour l'importation	Les certificats importés dans ACM peuvent maintenant disposer de clés avec des algorithmes RSA et Elliptic Curve supplémentaires. Pour obtenir la liste des algorithmes de clés actuellement pris en charge, consultez https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-prerequisites.html.	14 juillet 2021
Promotion de « Surveillance et journalisation » en tant que chapitre distinct	Déplacement de la documentation relative à la surveillance et à la journalisation vers son propre chapitre. Cette modification couvre les CloudWatch métriques, les CloudWatch événements/ EventBridge et CloudTrail. Pour plus d'informations, consultez https://docs.aws.amazon.com/acm/latest/userguide/monitoring-and-logging.html.	23 mars 2021
Support supplémentaire CloudWatch pour les métriques et les événements	Ajout de DaysToExpiry métriques, d'événements et d'API de support. Pour plus d'informations, consultez https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-metrics.html et https://docs.aws.amazon.com/acm/latest/userguide/cloudwatch-events.html.	3 mars 2021

Ajout de la prise en charge entre comptes	Ajout du support multi-comptes pour l'utilisation d'autorités de certification privées à partir de Autorité de certification privée AWS. Pour plus d'informations, consultez https://docs.aws.amazon.com/acm/latest/userguide/ca-access.html.	17 août 2020
Prise en charge de régions supplémentaires	Ajout du support régional pour les régions de AWS Chine (Pékin et Ningxia). Pour obtenir la liste complète des régions prises en charge, veuillez consulter https://docs.aws.amazon.com/general/latest/gr/rande.html#acm-pca_region.	4 mars 2020
Ajout d'une fonctionnalité de test des flux de travail de renouvellement	Les clients peuvent désormais tester manuellement la configuration de leur flux de travail de renouvellement géré ACM. Pour plus d'informations, consultez Test de la configuration de renouvellement géré ACM.	14 mars 2019
La journalisation de transparence des certificats est activée désormais par défaut	Ajout de la possibilité de publier des certificats publics ACM dans les journaux de transparence des certificats par défaut.	24 avril 2018

Lancement Autorité de certification privée AWS	Lancement d'ACM Private Certificate Manager (CM), AWS Certificate Manager dont l'extension permet aux utilisateurs d'établir une infrastructure gérée sécurisée pour l'émission et la révocation de certificats numériques privés. Pour plus d'informations, consultez AWS Private Certificate Authority.	4 avril 2018
Journalisation de transparence des certificats	Ajout de la journalisation de transparence de certificats aux bonnes pratiques	27 mars 2018

Le tableau suivant décrit l'historique des publications de documentation AWS Certificate Manager antérieures à 2018.

Modification	Description	Date de parution
Nouveau contenu	Ajout de validation DNS à Validation DNS.	21 novembre 2017
Nouveau contenu	Ajout de nouveaux exemples de code Java à Utilisation de l'API (exemples Java).	12 octobre 2017
Nouveau contenu	Informations sur les enregistrements CAA ajoutées à (Facultatif) Configuration d'un enregistrement CAA.	21 septembre 2017
Nouveau contenu	Ajout d'informations sur les domaines .IO à Résolution des problèmes.	07 juillet 2017

Modification	Description	Date de parution
Nouveau contenu	Ajout d'informations sur la réimportation d'un certificat à Réimportation d'un certificat.	07 juillet 2017
Nouveau contenu	Ajout d'informations sur l'épinglage de certificat à Bonnes pratiques et à Résolution des problèmes.	07 juillet 2017
Nouveau contenu	Ajouté AWS CloudFormation àServices intégrés à AWS Certificate Manager.	27 mai 2017
Mettre à jour	Ajout d'informations à Quotas.	27 mai 2017
Nouveau contenu	Ajout de la documentation sur Identity and Access Management pour AWS Certificate Manager.	28 avril 2017
Mettre à jour	Ajout d'un graphique pour montrer les adresses auxquelles l'e-mail de validation est envoyé. veuillez consulter Validation par courriel.	21 avril 2017
Mettre à jour	Ajout d'informations sur la configuration de l'e-mail pour votre domaine. veuillez consulter (Facultatif) Configuration d'une adresse électronique pour votre domaine.	6 avril 2017

Modification	Description	Date de parution
Mettre à jour	Ajout d'informations sur la vérification du statut de renouvellement d'un certificat dans la console. veuillez consulter Vérifier le statut de renouvellement d'un certificat.	28 mars 2017
Mettre à jour	Mise à jour de la documentation relative à l'utilisation d'Elastic Load Balancing	21 mars 2017
Nouveau contenu	Ajout de la prise AWS Elastic Beanstalk en charge d'Amazon API Gateway. veuillez consulter Services intégrés à AWS Certificate Manager.	21 mars 2017
Mettre à jour	Mise à jour de la documentation sur Renouvellement géré.	20 février 2017
Nouveau contenu	Ajout de la documentation sur Importer des certificats.	13 octobre 2016
Nouveau contenu	Ajout du AWS CloudTrail support pour les actions ACM. Consultez Utilisation CloudTrail avec AWS Certificate Manager.	25 mars 2016
Nouveau guide	Cette version présente AWS Certificate Manager.	21 janvier 2016

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.