aws

Guide du développeur

Amazon CloudFront

Amazon CloudFront: Guide du développeur

Table of Contents

Qu'est-ce qu'Amazon CloudFront ?

Amazon CloudFront est un service Web qui accélère la distribution de votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et les fichiers image, à vos utilisateurs. CloudFront diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques. Lorsqu'un utilisateur demande le contenu que vous diffusez CloudFront, la demande est acheminée vers l'emplacement périphérique offrant la latence la plus faible (délai), afin que le contenu soit diffusé avec les meilleures performances possibles.

- Si le contenu se trouve déjà dans l'emplacement périphérique où la latence est la plus faible, CloudFront il est diffusé immédiatement.
- Si le contenu ne se trouve pas dans cet emplacement périphérique, CloudFront récupérez-le à partir d'une origine que vous avez définie, telle qu'un compartiment Amazon S3, un MediaPackage canal ou un serveur HTTP (par exemple, un serveur Web) que vous avez identifié comme source de la version définitive de votre contenu.

Par exemple, supposons que vous diffusez une image depuis un serveur Web traditionnel, et non depuis CloudFront. Par exemple, vous pouvez diffuser une image, sunsetphoto.png, à l'aide de l'URL `https://example.com/sunsetphoto.png`.

Vos utilisateurs peuvent facilement accéder à cette URL et voir l'image. Néanmoins, jusqu'à ce que l'image soit trouvée, ils ignorent probablement que leur demande a été transmise d'un réseau à un autre par le biais de l'enchevêtrement complexe de réseaux interconnectés qui forment Internet.

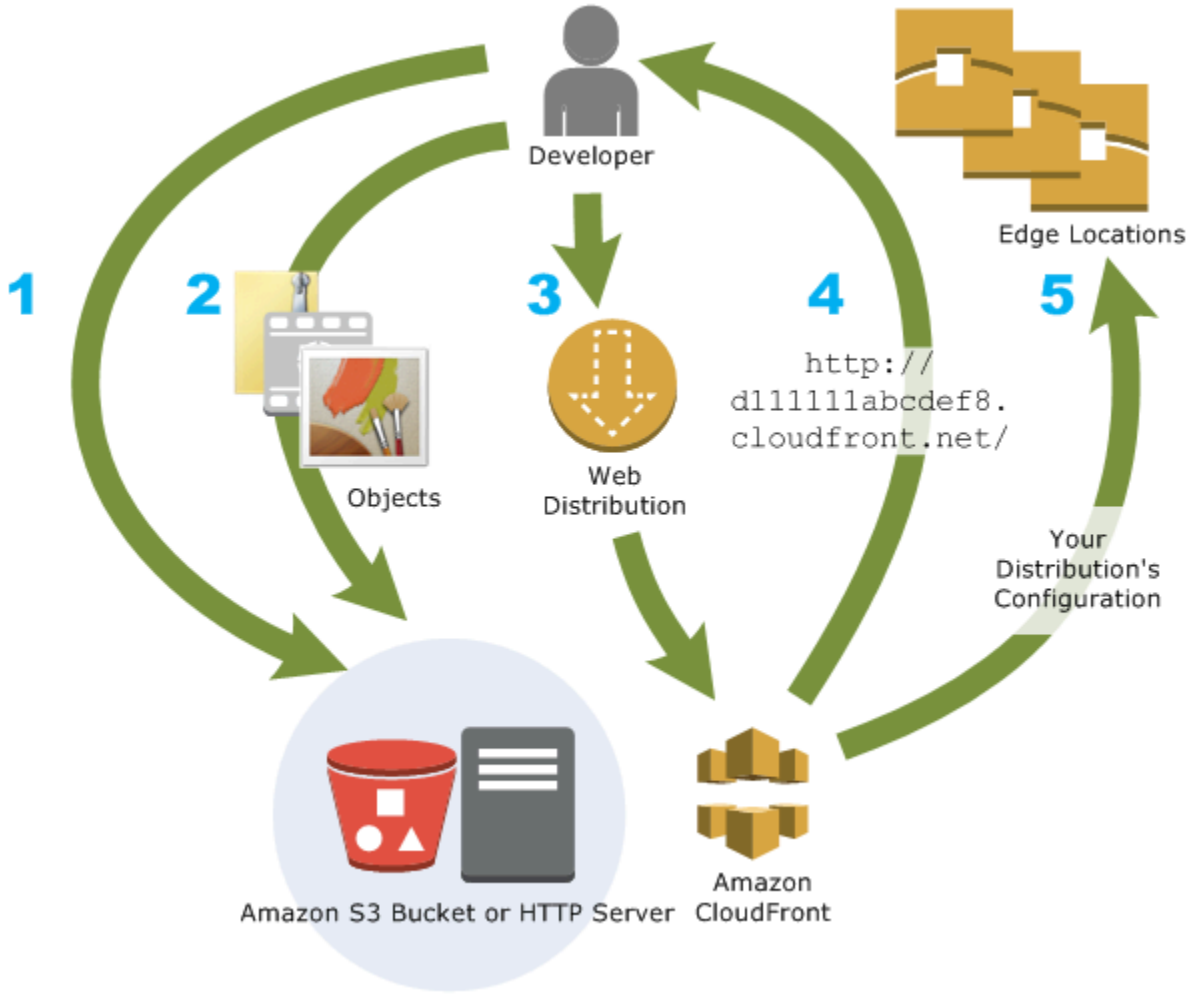
CloudFront accélère la diffusion de votre contenu en acheminant chaque demande utilisateur via le réseau AWS principal vers l'emplacement périphérique le plus à même de servir votre contenu. Il s'agit généralement d'un serveur CloudFront Edge qui fournit la diffusion la plus rapide au spectateur. L'utilisation du AWS réseau réduit considérablement le nombre de réseaux par lesquels les demandes de vos utilisateurs doivent passer, ce qui améliore les performances. Les utilisateurs bénéficient d'une latence plus faible (durée nécessaire au chargement du premier octet du fichier) et de débits de transfert des données plus élevés.

Il en résulte également une fiabilité et une disponibilité accrues, car des copies des fichiers (également appelés objets) sont désormais détenues (ou mises en cache) dans plusieurs emplacements périphériques situés aux quatre coins du monde.

Rubriques

Comment vous configurez CloudFront la diffusion de contenu

Vous créez une CloudFront distribution pour indiquer d' CloudFront où vous souhaitez que le contenu soit diffusé, ainsi que les détails sur le suivi et la gestion de la diffusion du contenu. CloudFront Utilise ensuite des ordinateurs (serveurs périphériques) situés à proximité de vos spectateurs pour diffuser rapidement ce contenu lorsque quelqu'un souhaite le voir ou l'utiliser.



Comment vous configurez CloudFront pour diffuser votre contenu

1. Vous spécifiez les serveurs d'origine, tels qu'un compartiment Amazon S3 ou votre propre serveur HTTP, à partir desquels CloudFront vos fichiers seront ensuite distribués depuis des emplacements CloudFront périphériques dans le monde entier.

   Un serveur d'origine stocke la version d'origine définitive de vos objets. Si vous diffusez du contenu sur HTTP, votre serveur d'origine est soit un compartiment Amazon S3 soit un serveur HTTP, tel qu'un serveur web. Votre serveur HTTP peut s'exécuter sur une instance Amazon Elastic Compute Cloud (Amazon EC2) ou sur un serveur que vous gérez ; ces serveurs sont également appelés origines personnalisées.
2. Téléchargez vos fichiers sur vos serveurs d'origine. Vos fichiers, également appelés objets, incluent généralement des pages web, des images et des fichiers multimédias, mais peuvent être tout ce qui peut être servi via HTTP.

   Si vous utilisez un compartiment Amazon S3 comme serveur d'origine, vous pouvez rendre les objets de votre compartiment lisibles par le public, afin que toute personne connaissant les CloudFront URL de vos objets puisse y accéder. Vous avez également la possibilité de garder des objets privés et de contrôler leur accès. Voir Diffusez du contenu privé avec des URL signées et des cookies signés.
3. Vous créez une CloudFront distribution qui indique sur CloudFront quels serveurs d'origine obtenir vos fichiers lorsque les utilisateurs demandent les fichiers via votre site Web ou votre application. Dans le même temps, vous spécifiez des détails tels que si vous CloudFront souhaitez enregistrer toutes les demandes et si vous souhaitez que la distribution soit activée dès sa création.
4. CloudFront attribue un nom de domaine à votre nouvelle distribution que vous pouvez voir dans la CloudFront console ou qui est renvoyé en réponse à une demande de programmation, par exemple une demande d'API. Si vous le souhaitez, vous pouvez ajouter un nom de domaine alternatif en remplacement.
5. CloudFront envoie la configuration de votre distribution (mais pas votre contenu) à tous ses emplacements périphériques ou points de présence (POP), c'est-à-dire des ensembles de serveurs situés dans des centres de données géographiquement dispersés où des copies de vos fichiers sont mises en CloudFront cache.

Lorsque vous développez votre site Web ou votre application, vous utilisez le nom de domaine qui CloudFront fournit vos URL. Par exemple, si CloudFront le `d111111abcdef8.cloudfront.net`

nom de domaine de votre distribution est renvoyé, l'URL de logo.jpg dans votre compartiment Amazon S3 (ou dans le répertoire racine d'un serveur HTTP) esthttps://d111111abcdef8.cloudfront.net/logo.jpg.

Vous pouvez également CloudFront configurer votre propre nom de domaine pour votre distribution. Dans ce cas, l'URL pourrait être https://www.example.com/logo.jpg.

Vous pouvez éventuellement configurer votre serveur d'origine pour ajouter des en-têtes aux fichiers, afin d'indiquer pendant combien de temps vous souhaitez que les fichiers restent dans le cache aux emplacements CloudFront périphériques. Par défaut, chaque fichier reste 24 heures dans l'emplacement périphérique avant d'arriver à expiration. Le délai d'expiration minimum est de 0 seconde. Il n'existe pas de délai d'expiration maximum. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Tarification

CloudFront frais pour les transferts de données depuis ses emplacements périphériques, ainsi que pour les requêtes HTTP ou HTTPS. Les prix varient en fonction du type d'utilisation, de la région géographique et de la sélection de fonctionnalités.

Le transfert de données de votre source vers CloudFront est toujours gratuit lorsque vous utilisez des AWS sources telles qu'Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing ou Amazon API Gateway. Vous n'êtes facturé que pour le transfert de données sortantes depuis CloudFront le lecteur lorsque vous utilisez AWS Origins.

Pour plus d'informations, consultez les CloudFront tarifs et les FAQ sur les offres groupées de facturation et d'épargne.

Moyens d'utilisation CloudFront

L'utilisation CloudFront peut vous aider à atteindre divers objectifs. Cette section en répertorie quelques-uns, avec des liens vers des informations supplémentaires, pour vous donner une idée des possibilités.

Rubriques

- Accélération de la diffusion de contenu de site web statique
- Diffusion de vidéo en streaming à la demande et en direct

- Chiffrement de champs spécifiques tout au long du traitement du système
- Personnalisation au niveau de l'emplacement périphérique
- Diffusion de contenu privé à l'aide des personnalisations de Lambda@Edge

Accélération de la diffusion de contenu de site web statique

CloudFront peut accélérer la diffusion de votre contenu statique (par exemple, des images, des feuilles de style JavaScript, etc.) aux spectateurs du monde entier. En l'utilisant CloudFront, vous pouvez tirer parti du réseau AWS principal et des serveurs CloudFront périphériques pour offrir à vos visiteurs une expérience rapide, sûre et fiable lorsqu'ils visitent votre site Web.

Une approche simple pour stocker et diffuser du contenu statique consiste à utiliser un compartiment Amazon S3. L'utilisation combinée de S3 CloudFront présente de nombreux avantages, notamment la possibilité d'utiliser le contrôle d'accès à l'origine pour restreindre facilement l'accès à votre contenu S3.

Pour plus d'informations sur l'utilisation conjointe de S3 CloudFront, y compris un AWS CloudFormation modèle pour vous aider à démarrer rapidement, consultez Amazon S3 + Amazon CloudFront : A Match Made in the Cloud.

Diffusion de vidéo en streaming à la demande et en direct

CloudFront propose plusieurs options pour diffuser votre contenu multimédia aux spectateurs du monde entier, qu'il s'agisse de fichiers préenregistrés ou d'événements en direct.

- Pour le streaming vidéo à la demande (VOD), vous pouvez CloudFront utiliser des formats courants tels que MPEG DASH, Apple HLS, Microsoft Smooth Streaming et CMAF, sur n'importe quel appareil.
- Pour diffuser du streaming en direct, vous pouvez mettre en cache des fragments multimédia à l'emplacement périphérique, de sorte que plusieurs requêtes pour le fichier manifeste qui diffuse les fragments dans le bon ordre puissent être combinées, afin de réduire la charge sur votre serveur d'origine.

Pour plus d'informations sur la diffusion de contenu en streaming avec CloudFront, consultezVidéo à la demande et diffusion vidéo en direct avec CloudFront.

Chiffrement de champs spécifiques tout au long du traitement du système

Lorsque vous configurez HTTPS avec CloudFront, vous disposez déjà de end-to-end connexions sécurisées aux serveurs d'origine. Lorsque vous ajoutez du chiffrement au niveau du champ, vous pouvez protéger des données spécifiques tout au long du traitement du système en plus de la sécurité HTTPS, pour que seules certaines applications à votre origine puissent voir les données.

Pour configurer le chiffrement au niveau des champs, vous ajoutez une clé publique CloudFront, puis vous spécifiez l'ensemble de champs que vous souhaitez chiffrer avec cette clé. Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Personnalisation au niveau de l'emplacement périphérique

L'exécution de code sans serveur à l'emplacement périphérique offre un certain nombre de possibilités pour la personnalisation du contenu et de l'expérience des utilisateurs, à une latence réduite. Par exemple, vous pouvez renvoyer un message d'erreur personnalisé lorsque votre serveur d'origine est indisponible à des fins de maintenance, afin que les utilisateurs ne reçoivent pas de message d'erreur HTTP générique. Vous pouvez également utiliser une fonction pour autoriser les utilisateurs et contrôler l'accès à votre contenu, avant de CloudFront transmettre une demande à votre source.

L'utilisation de Lambda @Edge CloudFront permet de personnaliser le contenu diffusé de différentes manières. CloudFront Pour en savoir plus sur Lambda @Edge et sur la façon de créer et de déployer des fonctions avecCloudFront, consultez. Personnalisez à la périphérie avec Lambda @Edge
Pour voir un certain nombre d'exemples de code que vous pouvez personnaliser pour vos propres solutions, consultez Exemples de fonctions Lambda@Edge.

Diffusion de contenu privé à l'aide des personnalisations de Lambda@Edge

L'utilisation de Lambda @Edge peut vous aider à configurer votre CloudFront distribution pour diffuser du contenu privé à partir de votre propre origine personnalisée, en plus d'utiliser des URL signées ou des cookies signés.

Pour diffuser du contenu privé en utilisant CloudFront, procédez comme suit :

- Exigez des utilisateurs qu'ils accèdent au contenu à l'aide d'URL signées ou de cookies signés.
- Limitez l'accès à votre origine afin qu'il ne soit disponible que depuis les serveurs orientés vers CloudFront l'origine. Pour ce faire, vous pouvez procéder de différentes manières :

- Pour une origine Amazon S3, vous pouvez utiliser un contrôle d'accès à l'origine (OAC).
- Pour une origine personnalisée, vous pouvez effectuer les opérations suivantes :
  - Si l'origine personnalisée est protégée par un groupe de sécurité Amazon VPC ou AWS Firewall Manager si vous pouvez utiliser la liste de préfixes CloudFront gérée pour autoriser le trafic entrant vers votre origine uniquement à partir des adresses IP orientées vers CloudFront l'origine.
  - Utilisez un en-tête HTTP personnalisé pour restreindre l'accès aux seules demandes provenant de CloudFront. Pour plus d'informations, consultez the section called "Restreindre l'accès aux fichiers dont l'origine est personnalisée" et the section called "Ajouter des en-têtes personnalisés aux demandes d'origine". Pour voir un exemple dans lequel un en-tête personnalisé limitant l'accès à une origine Application Load Balancer est utilisé, veuillez consulter the section called "Restreindre l'accès aux équilibreurs de charge des applications".
  - Si l'origine personnalisée nécessite une logique de contrôle d'accès personnalisée, vous pouvez utiliser Lambda @Edge pour implémenter cette logique, comme décrit dans ce billet de blog : Serving Private Content Using Amazon & CloudFront Lambda @Edge.

Comment CloudFront diffuse le contenu

Après une certaine configuration initiale, il CloudFront fonctionne avec votre site Web ou votre application et accélère la diffusion de votre contenu. Cette section explique comment CloudFront diffuse votre contenu lorsque les internautes le demandent.

Rubriques

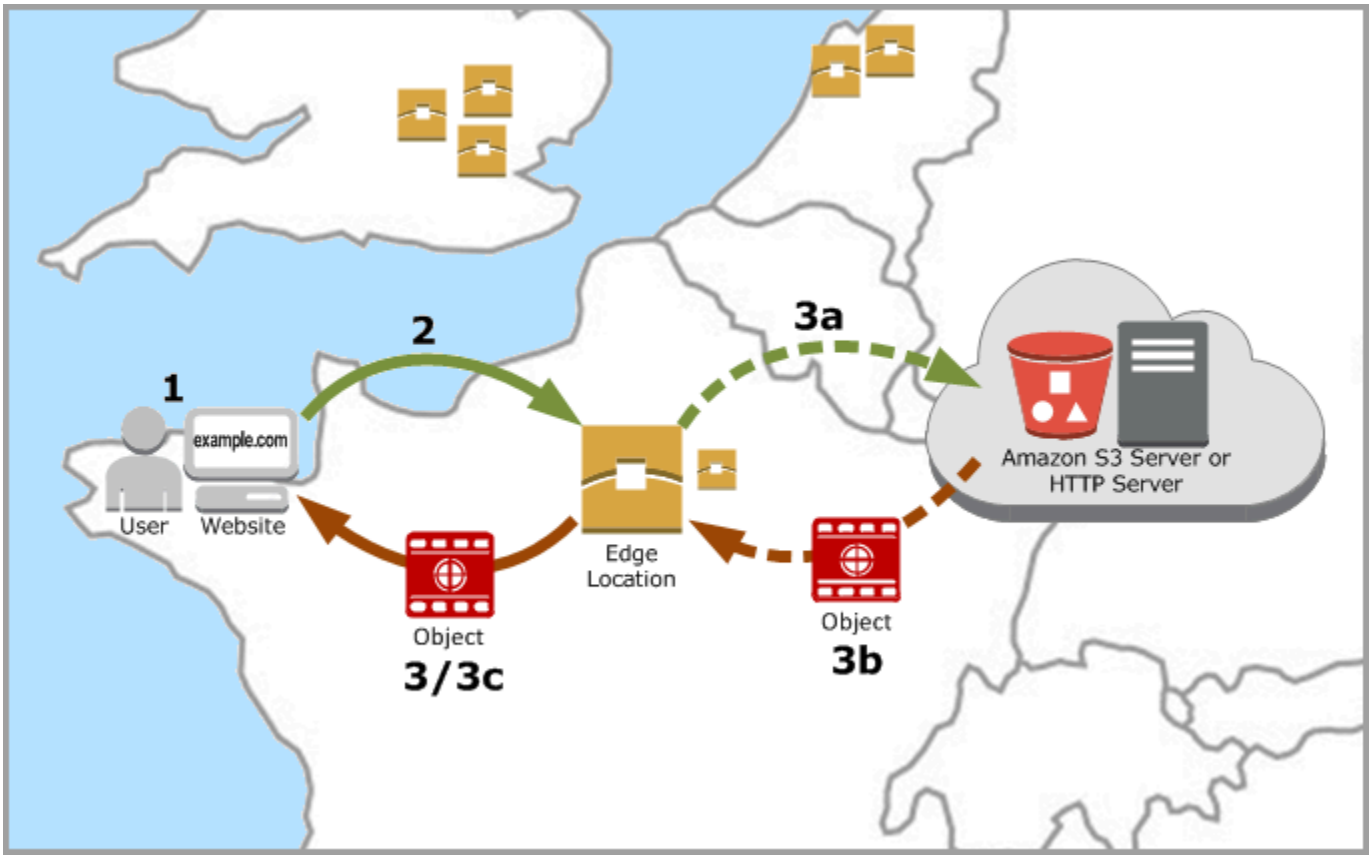
- Comment CloudFront diffuser du contenu à vos utilisateurs
- Comment CloudFront fonctionne avec les caches périphériques régionaux

Comment CloudFront diffuser du contenu à vos utilisateurs

Une fois que vous avez configuré CloudFront la diffusion de votre contenu, voici ce qui se passe lorsque les utilisateurs demandent vos objets :

1. Un utilisateur accède à votre application ou à votre site Web et envoie une demande pour un objet, tel qu'un fichier d'image ou un fichier HTML.

2. Le DNS achemine la demande vers le CloudFront POP (emplacement périphérique) qui peut le mieux répondre à la demande, généralement le CloudFront POP le plus proche en termes de latence.
3. CloudFront vérifie dans son cache l'objet demandé. Si l'objet se trouve dans le cache, il est CloudFront renvoyé à l'utilisateur. Si l'objet n'est pas dans le cache, CloudFront procédez comme suit :
   a. CloudFront compare la demande avec les spécifications de votre distribution et la transmet à votre serveur d'origine pour l'objet correspondant, par exemple à votre compartiment Amazon S3 ou à votre serveur HTTP.
   b. Le serveur d'origine renvoie l'objet vers l'emplacement périphérique.
   c. Dès que le premier octet arrive depuis l'origine, CloudFront commence à transmettre l'objet à l'utilisateur. CloudFront ajoute également l'objet au cache pour la prochaine fois que quelqu'un le demandera.



Comment CloudFront fonctionne avec les caches périphériques régionaux

CloudFront les points de présence (également appelés POPs ou emplacements périphériques) garantissent que le contenu populaire peut être diffusé rapidement à vos spectateurs. CloudFront dispose également de caches périphériques régionaux qui permettent de rapprocher une plus grande partie de votre contenu de vos spectateurs, même lorsque le contenu n'est pas assez populaire pour rester sur un POP, afin d'améliorer les performances de ce contenu.

Les caches périphériques régionaux aident tous les types de contenu, notamment ceux ayant tendance à devenir moins populaires au fil du temps. Il peut par exemple s'agir de contenus générés par l'utilisateur, tels que des vidéos, des photos ou des graphiques ; de ressources d’e-commerce telles que des photos et des vidéos de produits ; et de contenus liés à l'actualité et à des événements qui bénéficieraient tout à coup d'un regain de popularité.

Fonctionnement des caches régionaux

Les caches périphériques régionaux sont CloudFront des emplacements déployés dans le monde entier, à proximité de vos spectateurs. Ils sont situés entre votre serveur d'origine et les POP (ces emplacements périphériques mondiaux qui diffusent du contenu directement à vos utilisateurs). À mesure que la popularité des objets diminue, des POP individuels peuvent supprimer ces objets pour céder la place à du contenu plus populaire. Les caches périphériques régionaux disposent d'un plus grand cache qu'un POP individuel, afin que les objets restent plus longtemps dans le cache au niveau de l'emplacement de cache périphérique régional le plus proche. Cela permet de garder une plus grande partie de votre contenu à portée de main de vos spectateurs, de réduire le besoin de CloudFront retourner sur votre serveur d'origine et d'améliorer les performances globales pour les spectateurs.

Lorsqu'un utilisateur effectue une demande sur votre site web ou via votre application, le DNS l'achemine vers le POP qui saura diffuser au mieux la demande de l'utilisateur. Cet emplacement est généralement l'emplacement CloudFront périphérique le plus proche en termes de latence. Dans le POP, CloudFront vérifie la présence de l'objet demandé dans son cache. Si l'objet se trouve dans le cache, il est CloudFront renvoyé à l'utilisateur. S’il n’est pas dans le cache, le POP accède au cache périphérique régional le plus proche pour l’extraire. Pour plus d'informations sur le moment où le POP ignore le cache périphéruqe régional et accède directement à l'origine, reportez-vous à la note suivante.

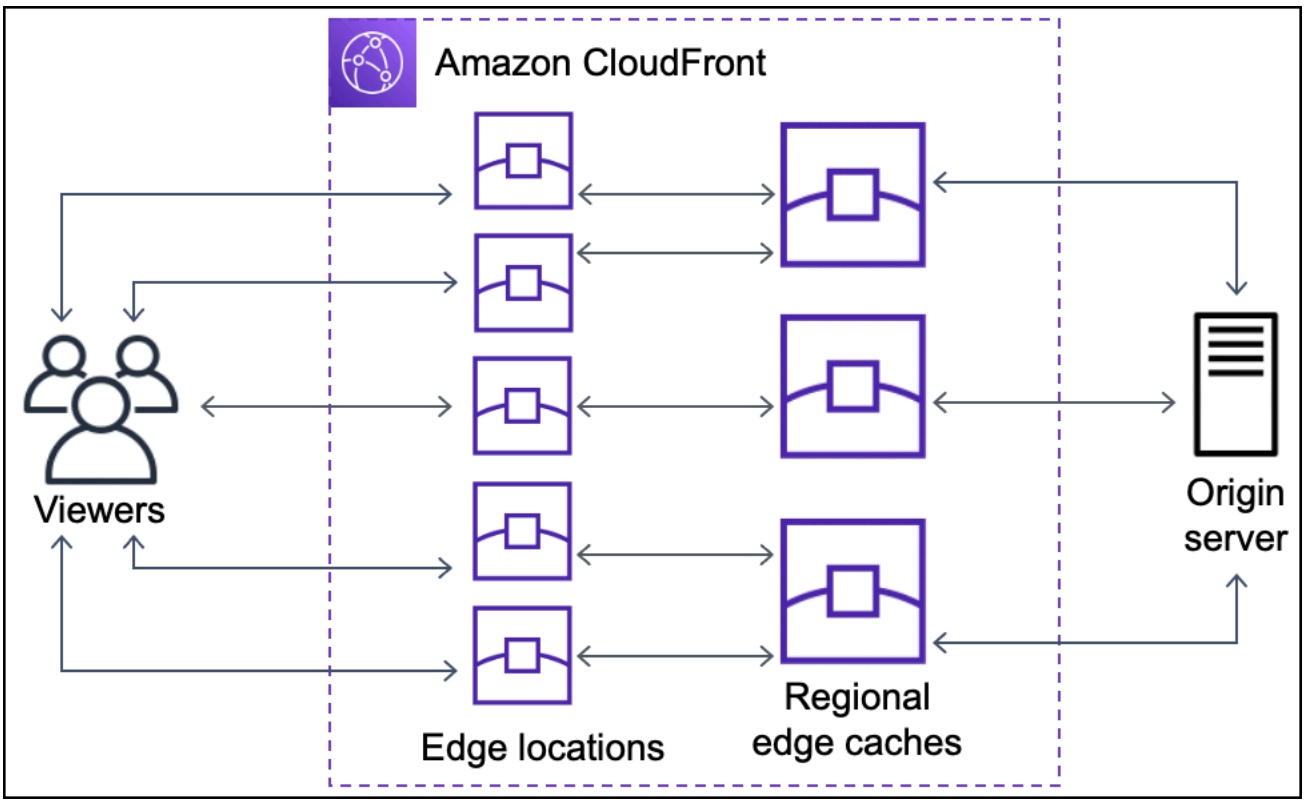
À l'emplacement du cache périphérique régional, vérifie CloudFront à nouveau dans son cache la présence de l'objet demandé. Si l'objet se trouve dans le cache, CloudFront il est transféré au

POP qui l'a demandé. Dès que le premier octet arrive depuis l'emplacement du cache périphérique régional, l'objet CloudFront commence à être transféré à l'utilisateur. CloudFront ajoute également l'objet au cache dans le POP pour la prochaine fois que quelqu'un le demandera.

Pour les objets qui ne sont pas mis en cache à l'emplacement du cache POP ou régional, CloudFront compare la demande avec les spécifications de vos distributions et transmet la demande au serveur d'origine. Une fois que votre serveur d'origine a renvoyé l'objet à l'emplacement du cache périphérique régional, il est transféré au POP, CloudFront puis transmis à l'utilisateur. Dans ce cas, ajoute CloudFront également l'objet au cache situé à l'emplacement du cache périphérique régional en plus du POP pour la prochaine fois qu'un utilisateur le demandera. Cela garantit que tous les POP d'une région partagent un cache local, éliminant ainsi les demandes multiples adressées aux serveurs d'origine. CloudFront maintient également des connexions persistantes avec les serveurs d'origine afin que les objets soient récupérés depuis les serveurs d'origine le plus rapidement possible.

> **Note**
>
> - Les caches périphériques régionaux présentent une parité de fonctionnalités avec les POP. Par exemple, une demande d'invalidation d'un cache supprime un objet à la fois des caches des POP et des caches périphériques régionaux avant son expiration. La prochaine fois qu'un utilisateur demande l'objet, il CloudFront retourne à l'origine pour récupérer la dernière version de l'objet.
> - Les méthodes proxy HTTP (`PUT`, `POST`, `PATCH`, `OPTIONS` et `DELETE`) se dirigent directement vers l'origine depuis les POP sans passer par les caches périphériques régionaux.
> - Les demandes dynamiques, tel que déterminé au moment de la demande, ne circulent pas dans les caches périphériques régionaux, mais vont directement à l'origine.
> - Lorsque l'origine est un compartiment Amazon S3 et que le cache périphérique régional optimal de la demande se trouve dans le même emplacement Région AWS que le compartiment S3, le POP ignore le cache périphérique régional et passe directement dans le compartiment S3.

Le schéma suivant illustre la manière dont les demandes et les réponses circulent dans les emplacements CloudFront périphériques et les caches périphériques régionaux.



Emplacements et plages d'adresses IP des serveurs CloudFront périphériques

Pour obtenir la liste des emplacements des serveurs CloudFront Edge, consultez la page Amazon CloudFront Global Edge Network.

Amazon Web Services (AWS) publie ses plages d'adresses IP actuelles au format JSON. Pour afficher les plages actuelles, téléchargez ip-ranges.json. Pour plus d'informations, consultez AWS IP Address Ranges dans le manuel Référence générale d'Amazon Web Services.

Pour trouver les plages d'adresses IP associées aux serveurs CloudFront Edge, recherchez la chaîne suivante dans ip-ranges.json :

```
"region": "GLOBAL",
"service": "CLOUDFRONT"
```

Vous pouvez également afficher uniquement les plages d' CloudFront adresses IP surhttps://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips.

Utiliser la liste de préfixes CloudFront gérée

La liste des préfixes CloudFront gérés contient les plages d'adresses IP de tous les serveurs orientés CloudFront origine distribués dans le monde entier. Si votre origine est hébergée AWS et protégée par un groupe de sécurité Amazon VPC, vous pouvez utiliser la liste de préfixes CloudFront gérée pour autoriser le trafic entrant vers votre origine uniquement à partir CloudFront des serveurs orientés vers l'origine, empêchant ainsi tout trafic autre que le trafic d'atteindre votre origine. CloudFront CloudFront tient à jour la liste des préfixes gérés afin qu'elle soit toujours à jour avec les adresses IP de tous les serveurs CloudFront mondiaux orientés vers l'origine. Avec la liste de préfixes CloudFront gérée, vous n'avez pas besoin de lire ou de gérer vous-même une liste de plages d'adresses IP.

Par exemple, imaginez que votre origine soit une instance Amazon EC2 située dans la région Europe (Londres) (`eu-west-2`). Si l'instance se trouve dans un VPC, vous pouvez créer une règle de groupe de sécurité qui autorise l'accès HTTPS entrant à partir de la liste de préfixes CloudFront gérés. Cela permet à tous les serveurs CloudFront mondiaux orientés vers l'origine d'accéder à l'instance. Si vous supprimez toutes les autres règles entrantes du groupe de sécurité, vous empêchez tout CloudFront trafic extérieur d'atteindre l'instance.

La liste de CloudFront préfixes gérée s'appelle com.amazonaws.global.cloudfront.origin-facing. Pour plus d'informations, consultez la section Utiliser une liste de préfixes AWS gérée dans le guide de l'utilisateur Amazon VPC.

> **Important**
>
> La liste de préfixes CloudFront gérés est unique en ce qui concerne la manière dont elle s'applique aux quotas Amazon VPC. Pour plus d'informations, consultez la pondération de la liste de préfixes gérés par AWS dans le Guide de l'utilisateur Amazon VPC.

Utilisation CloudFront avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK for C++	AWS SDK for C++ exemples de code

Documentation SDK	Exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Exemple de disponibilité

Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Faire un commentaire en bas de cette page.

CloudFront ressources techniques

Utilisez les ressources suivantes pour obtenir des réponses aux questions techniques concernant CloudFront :

- AWS Re:post — Un site communautaire de questions-réponses permettant aux développeurs de discuter de questions techniques liées à. CloudFront
- AWS Support Centre — Ce site contient des informations sur vos demandes d'assistance récentes, les résultats des bilans de santé AWS Trusted Advisor et les résultats de ceux-ci. Il fournit également des liens vers des forums de discussion, des FAQ techniques, le tableau de bord de santé des services et des informations sur AWS Support les plans.
- AWS Support Premium — Découvrez le Support AWS Premium one-on-one, un canal d'assistance rapide qui vous aide à créer et à exécuter des AWS applications.
- AWS IQ — Obtenez de l'aide auprès de professionnels et d'experts AWS certifiés.

Commencez avec CloudFront

Les rubriques de cette section vous montrent comment commencer à diffuser votre contenu avec Amazon CloudFront.

La Configuration rubrique décrit les prérequis pour les didacticiels suivants, tels que la création d'un Compte AWS et la création d'un utilisateur doté d'un accès administratif.

Le didacticiel de distribution de base explique comment configurer le contrôle d'accès à l'origine (OAC) pour envoyer des demandes authentifiées à une origine Amazon S3.

Le didacticiel de site Web statique sécurisé vous explique comment créer un site Web statique sécurisé pour votre nom de domaine à l'aide d'OAC avec une origine Amazon S3. Le didacticiel utilise un modèle Amazon CloudFront (CloudFront) pour la configuration et le déploiement.

Rubriques

Configuration

Cette rubrique décrit les étapes préliminaires, telles que la création d'un Compte AWS, pour vous préparer à utiliser Amazon CloudFront.

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.

Choisissez le mode d'accès CloudFront

Vous pouvez accéder CloudFront à Amazon de différentes manières :

- AWS Management Console— Les procédures décrites dans ce guide expliquent comment utiliser le AWS Management Console pour effectuer des tâches.

- AWS SDK — Si vous utilisez un langage de programmation qui AWS fournit un SDK pour, vous pouvez utiliser un SDK pour y accéder. CloudFront Les SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et fournissent un accès aux CloudFront commandes. Pour plus d'informations, consultez Utilisation CloudFront avec un AWS SDK.
- CloudFront API — Si vous utilisez un langage de programmation pour lequel aucun SDK n'est disponible, consultez le Amazon CloudFront API Reference pour plus d'informations sur les actions d'API et sur la manière de faire des demandes d'API.
- AWS CLI— Le AWS Command Line Interface (AWS CLI) est un outil de gestion unifié Services AWS. Pour plus d'informations sur l'installation et la configuration du AWS CLI, voir Installer ou mettre à jour la dernière version du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.
- Outils pour Windows PowerShell — Si vous avez de l'expérience avec Windows PowerShell, vous préférerez peut-être utiliser AWS Tools for Windows PowerShell. Pour plus d'informations, consultez Installation d' AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

Commencez avec une CloudFront distribution de base

Les procédures décrites dans cette section vous indiquent comment CloudFront configurer une configuration de base qui effectue les opérations suivantes :

- Crée un compartiment à utiliser comme origine de distribution.
- Stocke les versions originales de vos objets dans un compartiment Amazon Simple Storage Service (Amazon S3).
- Utilise le contrôle d'accès à l'origine (OAC) pour envoyer des demandes authentifiées à votre point d'origine Amazon S3. L'OAC envoie des demandes CloudFront pour empêcher les utilisateurs d'accéder directement à votre compartiment S3. Pour plus d'informations sur l'OAC, consultezRestreindre l'accès à une origine Amazon Simple Storage Service.
- Utilise le nom de CloudFront domaine dans les URL de vos objets (par exemple,`https://d111111abcdef8.cloudfront.net/index.html`).
- Maintient vos objets dans des emplacements CloudFront périphériques pendant la durée par défaut de 24 heures (la durée minimale est de 0 seconde).

La plupart de ces options sont personnalisables. Pour plus d'informations sur la personnalisation de vos options CloudFront de distribution, consultezCréer une distribution.

Rubriques

Prérequis

Avant de commencer, vérifiez que vous avez bien terminé les étapes de Configuration.

Étape 1 : Créer un compartiment Amazon S3

Un compartiment Amazon S3 est un conteneur pour des fichiers (objets) ou des dossiers. CloudFront peut distribuer presque n'importe quel type de fichier pour vous lorsqu'un compartiment S3 est la source. Par exemple, CloudFront peut distribuer du texte, des images et des vidéos. La quantité de données que vous pouvez stocker sur Amazon S3 n'est pas limitée.

Dans le cadre de ce didacticiel, vous allez créer un compartiment S3 avec les `hello world` fichiers d'exemple fournis que vous utiliserez pour créer une page Web de base.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Nous vous recommandons d'utiliser notre exemple Hello World pour ce guide de démarrage. Téléchargez la page Web Hello World : hello-world-html.zip. Décompressez-le et enregistrez le `css` dossier et le `index` fichier dans un emplacement pratique, tel que le bureau sur lequel vous utilisez votre navigateur.
3. Choisissez Créer un compartiment.
4. Entrez un nom de compartiment unique conforme aux règles de dénomination des compartiments à usage général du guide de l'utilisateur d'Amazon Simple Storage Service.
5. Pour la région, nous vous recommandons d'en choisir une Région AWS qui est géographiquement proche de vous. (Cela réduit la latence et les coûts.)

- Le choix d'une autre région fonctionne également. Vous pouvez le faire pour répondre aux exigences réglementaires, par exemple.

6. Conservez aux autres paramètres leurs valeurs par défaut, puis cliquez sur Créer un compartiment.

Étape 2 : charger le contenu dans le compartiment

Après avoir créé votre compartiment Amazon S3, chargez-y le contenu du `hello world` fichier décompressé. (Vous avez téléchargé et décompressé ce fichier.) Étape 1 : Créer un compartiment Amazon S3

Pour charger le contenu dans Amazon S3

1. Dans la section Compartiments à usage général, choisissez le nom de votre nouveau compartiment.
2. Sélectionnez Charger.
3. Sur la page de téléchargement, faites glisser le `css` dossier et le `index` fichier dans la zone de dépôt.
4. Laissez tous les autres paramètres avec leur valeur par défaut, puis sélectionnez Charger.

Étape 3 : créer une CloudFront distribution qui utilise une origine Amazon S3 avec OAC

Dans le cadre de ce didacticiel, vous allez créer une CloudFront distribution qui utilise une origine Amazon S3 avec un contrôle d'accès à l'origine (OAC). OAC vous permet d'envoyer en toute sécurité des demandes authentifiées à votre Amazon S3 d'origine. Pour plus d'informations sur l'OAC, consultezRestreindre l'accès à une origine Amazon Simple Storage Service.

Pour créer une CloudFront distribution avec une origine Amazon S3 qui utilise OAC

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Pour Origin, domaine Origin, choisissez le compartiment S3 que vous avez créé pour ce didacticiel.

4. Pour Origin, Accès à Origin, sélectionnez les paramètres de contrôle d'accès Origin (recommandé).
5. Pour le contrôle d'accès à Origin, choisissez Create new OAC.
6. Dans le volet Create new OAC, conservez les paramètres par défaut et choisissez Create.
7. Pour le Web Application Firewall (WAF), sélectionnez l'une des options.
8. Pour toutes les autres sections et tous les autres paramètres, acceptez les valeurs par défaut. Pour plus d'informations sur ces options, consultez Paramètres de distribution.
9. Choisissez Create distribution (Créer une distribution).
10. Dans la bannière The S3 bucket, la politique doit être mise à jour, lisez le message et choisissez Copy policy.
11. Dans la même bannière, cliquez sur le lien Accéder aux autorisations du compartiment S3 pour mettre à jour la politique. (Cela vous amène à la page détaillée de votre compartiment dans la console Amazon S3.)
12. Sous Bucket policy (Politique de compartiment), choisissez Edit (Modifier).
13. Dans le champ Modifier la déclaration, collez la politique que vous avez copiée à l'étape 10.
14. Sélectionnez Enregistrer les modifications.
15. Retournez à la CloudFront console et consultez la section Détails de votre nouvelle distribution. Lorsque le déploiement de votre distribution est terminé, le champ Dernière modification passe de Déploiement à une date et une heure.
16. Enregistrez le nom de domaine CloudFront attribué à votre distribution. Il ressemble à ce qui suit: `d111111abcdef8.cloudfront.net`.

Avant d'utiliser la distribution et le compartiment S3 décrits dans ce didacticiel dans un environnement de production, assurez-vous de les configurer pour répondre à vos besoins spécifiques. Pour plus d'informations sur la configuration de l'accès dans un environnement de production, consultezConfiguration de l'accès sécurisé et restriction de l'accès au contenu.

Étape 4 : Accédez à votre contenu via CloudFront

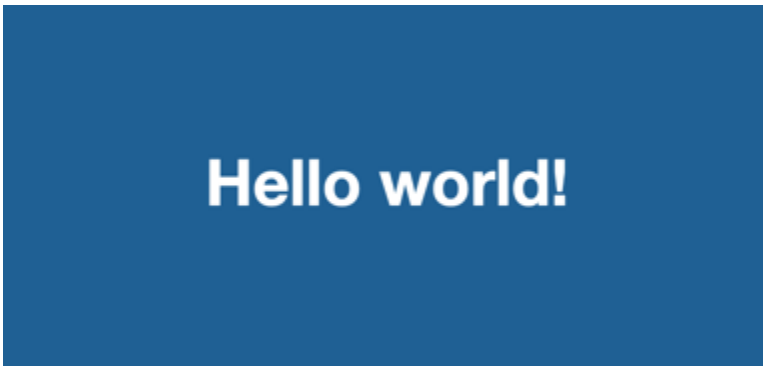
Pour accéder à votre contenu via CloudFront, associez le nom de domaine de votre CloudFront distribution à la page principale de votre contenu. (Vous avez enregistré votre nom de domaine de distribution dansÉtape 3 : créer une CloudFront distribution qui utilise une origine Amazon S3 avec OAC.)

- Le nom de domaine de votre distribution se présente sous cette forme : `d111111abcdef8.cloudfront.net`.
- Le chemin de la page principale d'un site web est généralement `/index.html`.

Par conséquent, l'URL permettant d'accéder à votre contenu CloudFront peut ressembler à ceci :

`https://d111111abcdef8.cloudfront.net/index.html`.

Si vous avez suivi les étapes précédentes et utilisé la page Web Hello World, le contenu suivant devrait s'afficher :



Lorsque vous chargez du contenu supplémentaire dans ce compartiment S3, vous pouvez y accéder en CloudFront combinant le nom de domaine de CloudFront distribution avec le chemin d'accès à l'objet dans le compartiment S3. Par exemple, si vous chargez un nouveau fichier nommé `new-page.html` à la racine de votre compartiment S3, l'URL se présente comme suit :

`https://d111111abcdef8.cloudfront.net/new-page.html`.

Étape 5 : nettoyer

Si vous avez créé votre distribution et votre compartiment S3 uniquement à des fins d'apprentissage, supprimez-les afin de ne plus payer de frais. Supprimez d'abord la distribution. Pour plus d'informations, consultez les liens suivants :

- Supprimer une distribution
- Supprimer un bucket

Améliorez votre CloudFront distribution de base

Ce didacticiel de mise en route fournit un cadre minimal pour créer une distribution. Nous vous recommandons d'explorer les améliorations suivantes :

- Par défaut, les fichiers (objets) du compartiment Amazon S3 sont définis comme étant privés. Seul celui Compte AWS qui a créé le compartiment est autorisé à lire ou à écrire les fichiers. Si vous souhaitez autoriser n'importe qui à accéder aux fichiers de votre compartiment Amazon S3 à l'aide d' CloudFront URL, vous devez accorder des autorisations de lecture publiques aux objets.
- Vous pouvez utiliser la fonctionnalité de contenu CloudFront privé pour restreindre l'accès au contenu des compartiments Amazon S3. Pour plus d'informations sur la distribution de contenus privés, consultez Diffusez du contenu privé avec des URL signées et des cookies signés.
- Vous pouvez configurer votre CloudFront distribution pour utiliser un nom de domaine personnalisé (par exemple, `www.example.com` au lieu `ded111111abcdef8.cloudfront.net`). Pour plus d'informations, consultez Utiliser des URL personnalisées.
- Ce didacticiel utilise une origine Amazon S3 avec contrôle d'accès à l'origine (OAC). Toutefois, vous ne pouvez pas utiliser OAC si votre origine est un compartiment S3 configuré comme point de terminaison de site Web. Si tel est le cas, vous devez configurer votre bucket en CloudFront tant qu'origine personnalisée. Pour plus d'informations, consultez Utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web. Pour plus d'informations sur l'OAC, consultezRestreindre l'accès à une origine Amazon Simple Storage Service.

Commencez avec un site Web statique sécurisé

Vous pouvez commencer à utiliser Amazon CloudFront en utilisant la solution décrite dans cette rubrique pour créer un site Web statique sécurisé pour votre nom de domaine. Un site Web statique utilise uniquement des fichiers statiques, tels que du HTML, du CSS, JavaScript des images et des vidéos, et n'a pas besoin de serveurs ou de traitement côté serveur. Avec cette solution, votre site web bénéficie des avantages suivants :

- Utilise le stockage durable d'Amazon Simple Storage Service (Amazon S3) – Cette solution crée un compartiment Amazon S3 pour héberger le contenu de votre site web statique. Pour mettre à jour votre site web, il vous suffit de charger vos nouveaux fichiers dans le compartiment S3.
- Accéléré par le réseau de diffusion de CloudFront contenu Amazon — Cette solution crée une CloudFront distribution pour diffuser votre site Web aux visiteurs avec une faible latence. La

distribution est configurée avec le contrôle d'accès à l'origine (OAC) pour garantir que le site Web est accessible uniquement via S3 CloudFront, et non directement depuis S3.

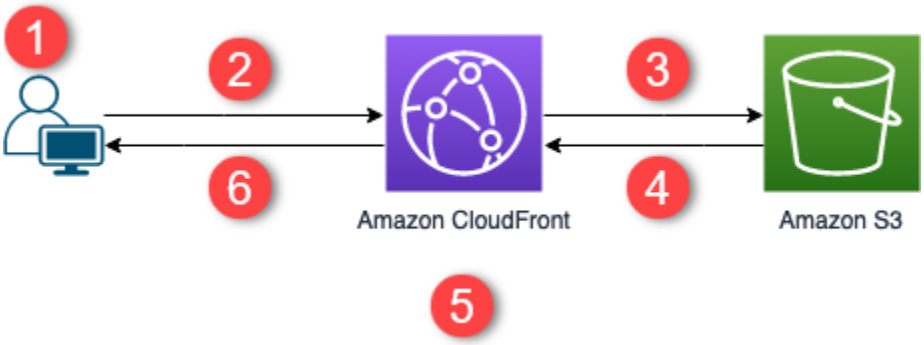
- Est sécurisé par HTTPS et des en-têtes de sécurité : cette solution crée un certificat SSL/TLS dans AWS Certificate Manager (ACM) et l'attache à la distribution. CloudFront Ce certificat permet à la distribution de diffuser le site web de votre domaine en toute sécurité avec HTTPS.
- Est configurée et déployée avec AWS CloudFormation: cette solution utilise un AWS CloudFormation modèle pour configurer tous les composants, afin que vous puissiez vous concentrer davantage sur le contenu de votre site Web et moins sur la configuration des composants.

Cette solution est open source sur GitHub. Pour afficher le code, envoyer une demande d'extraction ou ouvrir un problème, accédez à https://github.com/aws-samples/amazon-cloudfront-secure-static-site.

Rubriques

Présentation de la solution

Le diagramme suivant présente un aperçu du fonctionnement de cette solution de site web statique :



1. L'utilisateur demande le site web à l'adresse www.example.com.
2. Si l'objet demandé est mis en cache, CloudFront renvoie l'objet de son cache au visualiseur.
3. Si l'objet n'est pas dans le CloudFront cache, CloudFront demande l'objet depuis l'origine (un compartiment S3).
4. S3 renvoie l'objet à CloudFront.

5. CloudFront met en cache l'objet.
6. Les objets sont renvoyés au visualiseur. Les demandes suivantes pour l'objet qui arrivent au même emplacement CloudFront périphérique sont traitées à partir du CloudFront cache.

Déployez la solution

Pour déployer cette solution de site web statique sécurisé, vous pouvez choisir l'une des options suivantes :

- Utilisez la AWS CloudFormation console pour déployer la solution avec le contenu par défaut, puis téléchargez le contenu de votre site Web sur Amazon S3.
- Clonez la solution sur votre ordinateur pour ajouter le contenu de votre site web. Puis, déployez la solution avec l' AWS Command Line Interface (AWS CLI).

> **Note**
>
> Vous devez utiliser la région USA Est (Virginie du Nord) pour déployer le CloudFormation modèle.

Rubriques

Prérequis

Pour utiliser cette solution, les prérequis suivant sont nécessaires :

- Un nom de domaine enregistré, par exemple example.com, pointant vers une zone hébergée Amazon Route 53. La zone hébergée doit se trouver dans la même zone que celle Compte AWS où vous déployez cette solution. Si vous n'avez pas de nom de domaine enregistré, vous pouvez en enregistrer un avec Route 53. Si vous possédez un nom de domaine enregistré, mais qu'il ne pointe pas vers une zone hébergée Route 53, configurez Route 53 en tant que votre service DNS.

- AWS Identity and Access Management Autorisations (IAM) pour lancer des CloudFormation modèles qui créent des rôles IAM, et autorisations pour créer toutes les AWS ressources de la solution.

Vous assumez les coûts encourus pour utiliser cette solution. Pour plus d'informations sur les coûts, consultez les pages de tarification correspondantes Service AWS.

Utiliser la AWS CloudFormation console

Pour déployer à l'aide de la CloudFormation console

1. Choisissez Lancer sur AWS pour ouvrir cette solution dans la console AWS CloudFormation . Si nécessaire, connectez-vous à votre Compte AWS.

2. L'assistant de création d'une pile s'ouvre dans la CloudFormation console, avec des champs préremplis qui spécifient le CloudFormation modèle de cette solution.

   Au bas de la page, sélectionnez Next.

3. Dans la page Spécifier les détails de la pile, saisissez des valeurs pour les champs suivants :

   - SubDomain— Entrez le sous-domaine à utiliser pour votre site Web. Par exemple, si le sous-domaine est www, votre site web est disponible à l'adresse *www*.exemple.com. (Remplacez exemple.com par votre nom de domaine, comme expliqué dans la puce suivante.)
   - DomainName— Entrez votre nom de domaine, par exemple *exemple.com*. Ce domaine doit pointer vers une zone hébergée Route 53.
   - HostedZoneId— L'ID de zone hébergée Route 53 de votre nom de domaine.
   - CreateApex— (Facultatif) Créez un alias pour le domaine apex (exemple.com) dans votre CloudFront configuration.

4. Lorsque vous avez terminé, choisissez Next (Suivant).
5. (Facultatif) Dans la page Configure stack options (Configurer les options de pile), ajoutez des balises et d'autres options de pile.
6. Lorsque vous avez terminé, choisissez Next (Suivant).
7. Dans la page Vérification, faites défiler jusqu'au bas de la page, puis sélectionnez les deux cases de la section Capacités. Ces fonctionnalités permettent CloudFormation de créer un rôle IAM qui permet d'accéder aux ressources de la pile et de nommer les ressources de manière dynamique.

8. Choisissez Créer une pile.
9. Attendez la fin de la création de la pile. La pile crée des piles imbriquées, ce qui peut prendre plusieurs minutes. Une fois achevée, l'État passe à CREATE_COMPLETE.

   Lorsque l'état est CREATE_COMPLETE, accédez à https://*www.exemple.com* pour voir votre site web (remplacez www.exemple.com par les noms de sous-domaine et de domaine que vous avez spécifiés à l'étape 3). Vous devriez voir le contenu par défaut du site web :

Pour remplacer le contenu par défaut du site web par le vôtre

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez le bucket dont le nom commence par amazon-cloudfront-secure-static-site-s3bucketroot -.

   > **Note**
   >
   > Assurez-vous de choisir le compartiment dont le nom contient s3bucketroot et pas s3bucketlogs. Le compartiment dont le nom inclut s3bucketroot contient le contenu du site web. Celui dont le nom inclut s3bucketlogs ne contient que des fichiers journaux.

3. Supprimez le contenu par défaut du site web, puis chargez le vôtre.

   > **Note**
   >
   > Si vous avez consulté votre site Web avec le contenu par défaut de cette solution, il est probable qu'une partie du contenu par défaut soit mise en cache dans un emplacement CloudFront périphérique. Pour vous assurer que les visiteurs voient le contenu mis à jour de votre site Web, invalidez les fichiers pour supprimer les copies mises en cache des emplacements CloudFront périphériques. Pour plus d'informations, consultez Invalider des fichiers pour supprimer du contenu.

Cloner la solution localement

Prérequis

Pour ajouter votre contenu du site web avant de déployer cette solution, vous devez empaqueter les artefacts de cette dernière localement, ce qui demande Node.js et npm. Pour de plus amples informations, veuillez consulter https://www.npmjs.com/get-npm.

Pour ajouter votre contenu du site web et déployer la solution

1. Clonez ou téléchargez la solution à partir de https://github.com/aws-samples/amazon-cloudfront-secure-static-site. Après le clonage ou le téléchargement, ouvrez une invite de commande ou un terminal et accédez au dossier `amazon-cloudfront-secure-static-site`.
2. Exécutez la commande suivante pour installer et empaqueter les artefacts de la solution :

   ```
   make package-static
   ```

3. Copiez votre contenu du site web dans le dossier `www`, en écrasant le contenu par défaut du site web.
4. Exécutez la AWS CLI commande suivante pour créer un compartiment Amazon S3 afin de stocker les artefacts de la solution. *example-bucket-for-artifacts*Remplacez-le par votre propre nom de compartiment.

   ```
   aws s3 mb s3://example-bucket-for-artifacts --region us-east-1
   ```

5. Exécutez la AWS CLI commande suivante pour empaqueter les artefacts de la solution sous forme de CloudFormation modèle. *example-bucket-for-artifacts*Remplacez-le par le nom du bucket que vous avez créé à l'étape précédente.

   ```
   aws cloudformation package \
       --region us-east-1 \
       --template-file templates/main.yaml \
       --s3-bucket example-bucket-for-artifacts \
       --output-template-file packaged.template
   ```

6. Exécutez la commande suivante pour déployer la solution avec CloudFormation, en remplaçant les valeurs suivantes :

   - *your- CloudFormation -stack-name* — Remplacez par le nom de la pile. CloudFormation

- *example.com* – Remplacez-le par votre nom de domaine. Ce domaine doit pointer vers une zone hébergée Route 53 dans le même domaine Compte AWS.
- *www* – Remplacez-le par le sous-domaine à utiliser pour votre site web. Par exemple, si le sous-domaine est www, votre site web est disponible à l'adresse www.exemple.com.
- *Hosted-zone-ID — Remplacez-le par l'ID* de zone hébergée Route 53 de votre nom de domaine.

```
aws cloudformation deploy \
    --region us-east-1 \
    --stack-name your-CloudFormation-stack-name \
    --template-file packaged.template \
    --capabilities CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \
    --parameter-overrides DomainName=example.com SubDomain=www HostedZoneId=hosted-
zone-ID
```

- (Facultatif) Pour déployer la pile avec un apex de domaine, exécutez plutôt la commande suivante.

```
aws --region us-east-1 cloudformation deploy \
    --stack-name your-CloudFormation-stack-name \
    --template-file packaged.template \
    --capabilities CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \
    --parameter-overrides  DomainName=example.com SubDomain=www
 HostedZoneId=hosted-zone-ID CreateApex=yes
```

7. Attendez la fin de la création de la CloudFormation pile. La pile crée des piles imbriquées, ce qui peut prendre plusieurs minutes. Une fois achevée, l'État passe à CREATE_COMPLETE.

   Lorsque l'état passe à CREATE_COMPLETE, accédez à https ://www.exemple.com pour voir votre site web (remplacez www.exemple.com par les noms de sous-domaine et de domaine que vous avez spécifiés à l'étape précédente). Vous devriez voir le contenu de votre site web.

Recherche des journaux d'accès

Cette solution active les journaux d'accès pour la CloudFront distribution. Procédez comme suit pour localiser les journaux d'accès de la distribution.

Pour localiser les journaux d'accès de la distribution

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez le bucket dont le nom commence par amazon-cloudfront-secure-static-site-s3bucketlogs -.

   > **Note**
   >
   > Assurez-vous de choisir le compartiment dont le nom contient s3bucketlogs et pas s3bucketroot. Le compartiment dont le nom inclut s3bucketlogs contient des fichiers journaux. Celui dont le nom inclut s3bucketroot contient le contenu du site web.

3. Le dossier nommé cdn contient les journaux CloudFront d'accès.

Configuration des distributions

Vous créez une CloudFront distribution Amazon pour indiquer CloudFront d'où vous souhaitez que le contenu soit diffusé, ainsi que les informations relatives au suivi et à la gestion de la diffusion du contenu.

Choisissez parmi les paramètres de configuration suivants :

- L'origine de votre contenu : le compartiment, le AWS Elemental MediaPackage canal, le AWS Elemental MediaStore conteneur, l'équilibreur de charge Elastic Load Balancing ou le serveur HTTP Amazon S3 à partir CloudFront duquel les fichiers doivent être distribués. Vous pouvez spécifier n'importe quelle combinaison pouvant aller jusqu'à 25 origines pour une distribution unique.
- Accès : si vous voulez que l’accès aux fichiers soit possible pour tout le monde ou si vous souhaitez le restreindre à certains utilisateurs.
- Sécurité : si vous souhaitez activer la protection AWS WAF et exiger des utilisateurs qu’ils emploient le protocole HTTPS pour accéder à votre contenu.
- Clé de cache : valeurs, le cas échéant, que vous souhaitez inclure dans la clé de cache. La clé de cache identifie de manière unique chaque fichier du cache pour une distribution donnée.
- Paramètres de la demande d'origine : si vous CloudFront souhaitez inclure des en-têtes HTTP, des cookies ou des chaînes de requête dans les demandes envoyées à votre origine.
- Restrictions géographiques : si vous CloudFront souhaitez empêcher les utilisateurs de certains pays d'accéder à votre contenu.
- Journaux : que vous souhaitiez CloudFront créer des journaux standard ou des journaux en temps réel qui montrent l'activité des spectateurs.

Pour plus d’informations, consultez Référence des paramètres de distribution.

Pour connaître le nombre maximal actuel de distributions que vous pouvez créer pour chaque AWS compte, consultezQuotas généraux sur les distributions. Il n’y a pas de nombre maximum de fichiers que vous pouvez servir par distribution.

Vous pouvez utiliser des distributions pour diffuser le contenu suivant via HTTP ou HTTPS :

- Contenu de téléchargement statique et dynamique, tel que des fichiers HTML JavaScript, CSS et images, via HTTP ou HTTPS.

- La vidéo à la demande dans différents formats, notamment Apple HTTP Live Streaming (HLS) et Microsoft Smooth Streaming. Pour plus d'informations, consultez Diffusez des vidéos à la demande avec CloudFront.
- Un événement en direct, tel qu'une réunion, une conférence ou un concert en temps réel. Pour le streaming en direct, vous pouvez créer la distribution automatiquement à l'aide d'une AWS CloudFormation pile. Pour plus d'informations, consultez Diffusez des vidéos en direct avec CloudFront et AWS Media Services.

Les rubriques suivantes fournissent plus de détails sur les CloudFront distributions et sur la manière de les configurer pour répondre aux besoins de votre entreprise. Pour plus d'informations sur la création d'une distribution, reportez-vous à Créer une distribution.

Rubriques

Créer une distribution

Cette rubrique explique comment utiliser la CloudFront console pour créer une distribution.

Présentation de la création d'une distribution

1. Créez un ou plusieurs compartiments Amazon S3 ou configurez les serveurs HTTP en tant que serveurs d'origine. Une origine désigne l'emplacement où vous stockez la version originale de votre contenu. Lorsque CloudFront vous recevez une demande pour vos fichiers, elle est

envoyée à l'origine pour récupérer les fichiers qu'elle distribue aux emplacements périphériques. Vous pouvez utiliser toute combinaison de compartiments Amazon S3 et de serveurs HTTP comme serveurs d'origine.

- Si vous utilisez Amazon S3, le nom de votre compartiment doit être intégralement en lettres minuscules et ne peut pas contenir d'espaces.
- Si vous utilisez un serveur Amazon EC2 ou une autre origine personnalisée, consultez Utiliser Amazon EC2 (ou une autre origine personnalisée).
- Pour connaître le nombre maximal actuel d'origines que vous pouvez créer pour une distribution ou pour demander un quota plus élevé, consultez Quotas généraux sur les distributions.

2. Téléchargez votre contenu sur vos serveurs d'origine. Vous rendez vos objets lisibles par le public ou vous pouvez utiliser des URL CloudFront signées pour restreindre l'accès à votre contenu.

   > **Important**
   >
   > Vous devez garantir la sécurité de votre serveur d'origine. Vous devez vous assurer qu'il CloudFront est autorisé à accéder au serveur et que les paramètres de sécurité protègent votre contenu.

3. Créez votre CloudFront distribution :

   - Pour une procédure détaillée de création d'une distribution dans la CloudFront console, consultezCréer une distribution.
   - Pour plus d'informations sur la création d'une distribution à l'aide de l' CloudFront API, consultez CreateDistributionle Amazon CloudFront API Reference.

4. (Facultatif) Si vous utilisez la CloudFront console pour créer votre distribution, créez davantage de comportements de cache ou d'origines pour la distribution. Pour plus d'informations sur les comportements et les origines, consultez Pour mettre à jour une CloudFront distribution.
5. Testez votre distribution. Pour plus d'informations sur les tests, consultez Tester une distribution.
6. Développez votre site Web ou votre application pour accéder à votre contenu en utilisant le nom de domaine CloudFront renvoyé après avoir créé votre distribution à l'étape 3. Par exemple, si le nom de domaine de votre distribution est CloudFront renvoyé d111111abcdef8.cloudfront.net, l'URL du fichier dans un compartiment `image.jpg` Amazon S3 ou dans le répertoire racine d'un serveur HTTP est. `https://d111111abcdef8.cloudfront.net/image.jpg`

Si vous avez spécifié un ou plusieurs noms de domaine alternatifs (CNAME) quand vous avez créé votre distribution, vous pouvez utiliser votre propre nom de domaine. Dans ce cas, l'URL de `image.jpg` pourrait être `https://www.example.com/image.jpg`.

Remarques :

- Si vous voulez utiliser des URL signées pour limiter l'accès à votre contenu, consultez Diffusez du contenu privé avec des URL signées et des cookies signés.
- Si vous voulez livrer un contenu compressé, consultez Servir des fichiers compressés.
- Pour plus d'informations sur le comportement des CloudFront demandes et des réponses pour Amazon S3 et sur les origines personnalisées, consultezComportement des demandes et des réponses.

Rubriques

Création d'une CloudFront distribution dans la console

Pour créer une distribution (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez Créer une distribution.
3. Spécifiez les paramètres de la distribution. Pour plus d'informations, consultez Référence des paramètres de distribution.
4. Enregistrez vos modifications.
5. Après avoir CloudFront créé votre distribution, la valeur de la colonne État de votre distribution passera de Déploiement à la date et à l'heure de déploiement de la distribution. Si vous avez choisi d'activer la distribution, elle sera prête à traiter les demandes à ce stade.

   Le nom de domaine CloudFront attribué à votre distribution apparaît dans la liste des distributions. (Elle apparaît aussi sous l'onglet General d'une distribution sélectionnée.)

> **Tip**
>
> Vous pouvez utiliser un autre nom de domaine au lieu du nom qui vous a été attribué par CloudFront ; en suivant les étapes décrites dansUtilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames).

6. Lorsque votre distribution est déployée, vérifiez que vous pouvez accéder à votre contenu à l'aide de votre nouvelle CloudFront URL ou de votre nouveau CNAME. Pour plus d'informations, consultez Tester une distribution.

Valeurs CloudFront affichées dans la console

Lorsque vous créez une nouvelle distribution ou que vous mettez à jour une distribution existante, CloudFront affiche les informations suivantes dans la CloudFront console.

> **Note**
>
> Les signataires fiables actifs, c'est-à-dire les AWS comptes dotés d'une paire de CloudFront clés active et pouvant être utilisés pour créer des URL signées valides, ne sont actuellement pas visibles dans la CloudFront console.

ID de distribution

Lorsque vous effectuez une action sur une distribution à l'aide de l' CloudFront API, vous utilisez l'ID de distribution pour spécifier la distribution à utiliser, par exemple`EDFDVBD6EXAMPLE`. Vous ne pouvez pas modifier l'ID d'une distribution.

Déploiement et statut

Lorsque vous déployez une distribution, l'état du déploiement s'affiche dans la colonne Dernière modification. Attendez que le déploiement de la distribution soit terminé et assurez-vous que la colonne État indique Activé. Pour plus d'informations, consultez État de la distribution.

Dernière modification

Date et heure de dernière modification de la distribution, à l'aide du format ISO 8601 : par exemple, 2012-05-19T19:37:58Z. Pour plus d'informations, consultez https://www.w3.org/TR/NOTE-datetime.

Nom de domaine

Vous utilisez le nom de domaine de la distribution dans les liens vers vos objets. Par exemple, si le nom de domaine de votre distribution est `d111111abcdef8.cloudfront.net`, le lien vers `/images/image.jpg` sera `https://d111111abcdef8.cloudfront.net/images/image.jpg`. Vous ne pouvez pas modifier le nom de CloudFront domaine de votre distribution. Pour plus d'informations sur CloudFront les URL des liens vers vos objets, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.

Si vous avez spécifié un ou plusieurs noms de domaine alternatifs (CNAME), vous pouvez utiliser vos propres noms de domaine pour les liens vers vos objets au lieu d'utiliser le nom de CloudFront domaine. Pour plus d'informations sur les CNAME, consultez Noms de domaine alternatifs (CNAME).

> **Note**
>
> CloudFront les noms de domaine sont uniques. Le nom de domaine de votre distribution n'avait jamais été utilisé pour une distribution précédente et ne sera jamais réutilisé pour une autre distribution à l'avenir.

Liens supplémentaires

Pour plus d'informations sur la création d'une distribution, consultez les liens suivants.

- Pour savoir comment créer une distribution qui utilise l'origine d'un bucket Amazon Simple Storage Service (Amazon S3) avec contrôle d'accès à l'origine (OAC), consultez. Commencez avec une CloudFront distribution de base
- Pour plus d'informations sur l'utilisation des CloudFront API pour créer une distribution, consultez CreateDistributionle Amazon CloudFront API Reference.
- Pour plus d'informations sur la mise à jour d'une distribution (par exemple, pour ajouter ou modifier des comportements de cache), consultezMettre à jour une distribution.
- Pour afficher le nombre maximum actuel de distributions que vous pouvez créer pour chaque compte AWS ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Référence des paramètres de distribution

Lorsque vous utilisez la CloudFrontconsole pour créer une nouvelle distribution ou mettre à jour une distribution existante, vous spécifiez les valeurs suivantes.

Pour plus d'informations sur la création ou la mise à jour d'une distribution à l'aide de la CloudFront console, consultez the section called “Créer une distribution” outhe section called “Mettre à jour une distribution”.

Rubriques

Paramètres d’origine

Lorsque vous utilisez la CloudFront console pour créer ou mettre à jour une distribution, vous fournissez des informations sur un ou plusieurs emplacements, appelés origines, où vous stockez les versions originales de votre contenu Web. CloudFront récupère votre contenu Web depuis vos origines et le diffuse aux spectateurs via un réseau mondial de serveurs périphériques.

Pour connaître le nombre maximal actuel d’origines que vous pouvez créer pour une distribution ou pour demander un quota plus élevé, consultez the section called “Quotas généraux sur les distributions”.

Si vous voulez supprimer une origine, vous devez d’abord modifier ou supprimer les comportements de cache associés à cette origine.

> **Important**
>
> Si vous supprimez une origine, confirmez que les fichiers qui étaient précédemment remis par cette origine sont disponibles dans une autre origine et que vos comportements de cache acheminent désormais ces fichiers vers la nouvelle origine.

Lorsque vous créez ou mettez à jour une distribution web, vous spécifiez les valeurs suivantes pour chaque origine.

Rubriques

Domaine d'origine

Le domaine d'origine est le nom de domaine DNS du compartiment Amazon S3 ou du serveur HTTP à partir duquel vous CloudFront souhaitez obtenir des objets correspondant à cette origine, par exemple :

- Compartiment Amazon S3 – `DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com`

> **Note**
>
> Si vous avez récemment créé le compartiment S3, la CloudFront distribution peut renvoyer `HTTP 307 Temporary Redirect` des réponses pendant 24 heures au maximum. La propagation du nom du compartiment S3 dans toutes les AWS régions peut prendre jusqu'à 24 heures. Lorsque la propagation est terminée, la distribution arrête automatiquement l’envoi de ces réponses de redirection ; vous n’avez pas besoin de prendre d’action. Pour de plus amples informations, veuillez consulter Pourquoi

Amazon S3 m'envoie-t-il une réponse de redirection temporaire HTTP 307 ? et Redirection de demande temporaire.

- Compartiment Amazon S3 configuré en tant que site web – *DOC-EXAMPLE-BUCKET*.s3-website.*us-west-2*.amazonaws.com
- MediaStore contenant — *examplemediastore*.data.mediastore.*us-west-1*.amazonaws.com
- MediaPackage point de terminaison — *examplemediapackage*.mediapackage.*us-west-1*.amazonaws.com
- Instance Amazon EC2 – *ec2-203-0-113-25*.compute-1.amazonaws.com
- Équilibreur de charge Elastic Load Balancing – *example-load-balancer-1234567890*.*us-west-2*.elb.amazonaws.com
- Votre propre serveur web – https://www.example.com

Choisissez le nom de domaine dans le champ Domaine d'origine ou saisissez le nom. Le nom de domaine n'est pas sensible à la casse.

Si votre origine est un compartiment Amazon S3, notez les points suivants :

- Si le compartiment est configuré comme site web, entrez le point de terminaison de l'hébergement du site web statique Amazon S3 de votre compartiment ; ne sélectionnez pas le nom du compartiment dans la liste du champ Origin domain (Domaine d'origine). Le point de terminaison de l'hébergement du site web statique s'affiche dans la console Amazon S3, sur la page Properties (Propriétés) sous Static Website Hosting (Hébergement de site Web statique). Pour plus d'informations, consultez the section called "Utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web".
- Si vous avez configuré Amazon S3 Transfer Acceleration pour votre compartiment, ne spécifiez pas le point de terminaison s3-accelerate pour Origin domain (Domaine d'origine).
- Si vous utilisez un bucket provenant d'un autre AWS compte et si le bucket n'est pas configuré en tant que site Web, entrez le nom au format suivant :

  bucket-name.s3.*region*.amazonaws.com

  Si votre compartiment se trouve dans la région USA et que vous voulez qu'Amazon S3 route les demandes vers une installation située en Virginie du Nord, utilisez le format suivant :

  bucket-name.s3.us-east-1.amazonaws.com

- Les fichiers doivent être lisibles par le public, sauf si vous sécurisez votre contenu dans Amazon S3 à l'aide d'un contrôle CloudFront d'accès à l'origine. Pour plus d'informations sur le contrôle d'accès, consultez the section called "Restreindre l'accès à une origine Amazon Simple Storage Service".

> **Important**
>
> Si l'origine est un compartiment Amazon S3, le nom du compartiment doit être conforme aux exigences de dénomination DNS. Pour plus d'informations, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Lorsque vous modifiez la valeur du domaine d'origine pour une origine, commence CloudFront immédiatement à répliquer la modification aux emplacements CloudFront périphériques. Jusqu'à ce que la configuration de distribution soit mise à jour dans un emplacement périphérique donné, CloudFront continue de transférer les demandes vers l'origine précédente. Dès que la configuration de distribution est mise à jour dans cet emplacement périphérique, CloudFront commence à transférer les demandes vers la nouvelle origine.

La modification de l'origine ne nécessite pas CloudFront de repeupler les caches périphériques avec des objets provenant de la nouvelle origine. Tant que les demandes du lecteur dans votre application n'ont pas changé, CloudFront continue à servir les objets qui se trouvent déjà dans un cache périphérique jusqu'à ce que le TTL de chaque objet expire ou jusqu'à ce que les objets rarement demandés soient expulsés.

Protocole (origines personnalisées uniquement)

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

La politique de protocole que vous CloudFront souhaitez utiliser lors de la récupération d'objets depuis votre origine.

Choisissez l'une des valeurs suivantes :

- HTTP uniquement : CloudFront utilise uniquement le protocole HTTP pour accéder à l'origine.

> **Important**
>
> HTTP only (HTTP uniquement) est le paramètre par défaut lorsque l'origine est un point de terminaison d'hébergement de site web statique Amazon S3, car Amazon S3 ne prend pas en charge les connexions HTTPS pour les points de terminaison d'hébergement de sites web statiques. La CloudFront console ne prend pas en charge la modification de ce paramètre pour les points de terminaison d'hébergement de sites Web statiques Amazon S3.

- HTTPS uniquement : CloudFront utilise uniquement le protocole HTTPS pour accéder à l'origine.
- Match Viewer : CloudFront communique avec votre source via HTTP ou HTTPS, selon le protocole de la demande du spectateur. CloudFront ne met en cache l'objet qu'une seule fois, même si les utilisateurs font des demandes à l'aide des protocoles HTTP et HTTPS.

> **Important**
>
> Pour les demandes du lecteur HTTPS qui CloudFront sont transférées vers cette origine, l'un des noms de domaine figurant dans le certificat SSL/TLS de votre serveur d'origine doit correspondre au nom de domaine que vous avez spécifié pour le domaine d'origine. Sinon, CloudFront répond aux demandes du spectateur avec un code d'état HTTP 502 (Bad Gateway) au lieu de renvoyer l'objet demandé. Pour plus d'informations, consultez the section called "Exigences relatives à l'utilisation de certificats SSL/TLS avec CloudFront".

Rubriques

Port HTTP

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

(Facultatif) Vous pouvez spécifier le port HTTP sur lequel l'origine personnalisée est à l'écoute. Valeurs valides : ports 80, 443, et 1024 à 65535. La valeur par défaut est le port 80.

> **Important**
>
> Le port 80 est le paramètre par défaut lorsque l'origine est un point de terminaison d'hébergement de site web statique Amazon S3, car Amazon S3 prend uniquement en charge le port 80 pour les points de terminaison d'hébergement de sites web statiques. La CloudFront console ne prend pas en charge la modification de ce paramètre pour les points de terminaison d'hébergement de sites Web statiques Amazon S3.

Port HTTPS

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

(Facultatif) Vous pouvez spécifier le port HTTPS sur lequel l'origine personnalisée est à l'écoute. Valeurs valides : ports 80, 443, et 1024 à 65535. La valeur par défaut est le port 443. Quand Protocol (Protocole) a la valeur HTTP only (HTTP uniquement), vous ne pouvez pas spécifier une valeur pourHTTPS port (Port HTTPS).

Minimum de protocole SSL d'origine

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

Choisissez le protocole TLS/SSL minimal à CloudFront utiliser lorsqu'il établit une connexion HTTPS avec votre point d'origine. Les protocoles TLS inférieurs sont moins sécurisés, nous vous recommandons donc de choisir le dernier protocole TLS que votre origine prend en charge. QuandProtocol (Protocole) a la valeur HTTP only (HTTP uniquement), vous ne pouvez pas spécifier une valeur pour Minimum origin SSL protocol (Minimum de protocole SSL d'origine).

Si vous utilisez l' CloudFront API pour définir le protocole TLS/SSL CloudFront à utiliser, vous ne pouvez pas définir de protocole minimum. Au lieu de cela, vous spécifiez tous les protocoles TLS/

SSL qui CloudFront peuvent être utilisés avec votre origine. Pour plus d'informations, consultez OriginSslProtocolsle Amazon CloudFront API Reference.

Chemin d’origine

Si vous souhaitez demander votre contenu CloudFront à partir d'un répertoire de votre origine, entrez le chemin du répertoire, en commençant par une barre oblique (/). CloudFront ajoute le chemin du répertoire à la valeur du domaine d'origine, par exemple,**`cf-origin.example.com/production/images`**. N’ajoutez pas un slash (/) à la fin du chemin d’accès.

Imaginons que vous ayez, par exemple, les valeurs suivantes pour votre distribution :

- Origin domain (Domaine d’origine) – Compartiment Amazon S3 nommé **`DOC-EXAMPLE-BUCKET`**
- Chemin d’origine – **`/production`**
- Noms de domaine alternatifs (CNAME) – **`example.com`**

Lorsqu'un utilisateur entre `example.com/index.html` dans un navigateur, il CloudFront envoie une demande à Amazon S3 pour`DOC-EXAMPLE-BUCKET/production/index.html`.

Lorsqu'un utilisateur entre `example.com/acme/index.html` dans un navigateur, il CloudFront envoie une demande à Amazon S3 pour`DOC-EXAMPLE-BUCKET/production/acme/index.html`.

Nom

Un nom est une chaîne qui identifie de façon unique cette origine dans cette distribution. Si vous créez des comportements de cache en plus du comportement de cache par défaut, vous utilisez le nom que vous spécifiez ici pour identifier l'origine CloudFront vers laquelle vous souhaitez acheminer une demande lorsque la demande correspond au modèle de chemin correspondant à ce comportement de cache.

Accès à l'origine (origines Amazon S3 uniquement)

> **Note**
>
> Cela s’applique uniquement aux origines du compartiment Amazon S3 (celles qui n’utilisent pas le point de terminaison statique du site web S3).

Choisissez les paramètres de contrôle d'accès Origin (recommandés) si vous souhaitez permettre de restreindre l'accès à l'origine d'un compartiment Amazon S3 à des CloudFront distributions spécifiques uniquement.

Choisissez Public si l'origine du compartiment Amazon S3 est accessible au public.

Pour plus d’informations, consultez the section called “Restreindre l'accès à une origine Amazon Simple Storage Service”.

Pour plus d'informations sur la manière d'obliger les utilisateurs à accéder à des objets sur une origine personnalisée en utilisant uniquement CloudFront des URL, consultezthe section called “Restreindre l'accès aux fichiers dont l'origine est personnalisée”.

Ajout d'en-tête personnalisé

Si vous CloudFront souhaitez ajouter des en-têtes personnalisés chaque fois qu'une demande est envoyée à votre origine, spécifiez le nom de l'en-tête et sa valeur. Pour plus d’informations, consultez the section called “Ajouter des en-têtes personnalisés aux demandes d'origine”.

Pour obtenir le nombre maximum actuel d’en-têtes personnalisés que vous pouvez ajouter, la longueur maximale d’un nom et d’une valeur d’en-tête personnalisé, et la longueur totale maximale de tous les noms et valeurs d’en-tête, veuillez consulter Quotas.

Activer Origin Shield

Choisissez Oui pour activer CloudFront Origin Shield. Pour plus d'informations au sujet de Origin Shield, consultez the section called “Utilisation d'Origin Shield”.

Tentatives de connexion

Vous pouvez définir le nombre de CloudFront tentatives de connexion à l'origine. Vous pouvez spécifier 1, 2 ou 3 tentatives. Le nombre par défaut (sauf indication contraire) est 3.

Utilisez ce paramètre avec le délai d'expiration de la connexion pour spécifier le temps d' CloudFront attente avant de tenter de vous connecter à l'origine secondaire ou de renvoyer une réponse d'erreur au visualiseur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d’attente de connexion plus court, ou les deux.

Si le nombre de tentatives de connexion spécifié échoue, CloudFront effectue l'une des opérations suivantes :

- Si l'origine fait partie d'un groupe d'origine, CloudFront tente de se connecter à l'origine secondaire. Si le nombre spécifié de tentatives de connexion à l'origine secondaire échouent, CloudFront renvoie une réponse d'erreur au visualiseur.
- Si l'origine ne fait pas partie d'un groupe d'origine, CloudFront renvoie une réponse d'erreur au visualiseur.

Pour une origine personnalisée (y compris un compartiment Amazon S3 configuré avec un hébergement de site Web statique), ce paramètre spécifie également le nombre de CloudFront tentatives d'obtention d'une réponse de la part de l'origine. Pour plus d’informations, consultez the section called “Délai de réponse (origines personnalisées uniquement)”.

Délai de connexion

Le délai d'expiration de la connexion est le nombre de secondes qui CloudFront attendent lorsque vous essayez d'établir une connexion avec l'origine. Vous pouvez spécifier un nombre de secondes compris entre 1 et 10 (inclus). Le délai d’expiration par défaut (sauf indication contraire) est de 10 secondes.

Utilisez ce paramètre avec les tentatives de connexion pour spécifier le temps d' CloudFront attente avant de tenter de vous connecter à l'origine secondaire ou avant de renvoyer une réponse d'erreur au visualiseur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d’attente de connexion plus court, ou les deux.

S'il CloudFront n'établit pas de connexion avec l'origine dans le délai de secondes spécifié, CloudFront effectue l'une des opérations suivantes :

- Si le nombre de tentatives de connexion spécifié est supérieur à 1, CloudFront essaie à nouveau d'établir une connexion. CloudFront essaie jusqu'à 3 fois, en fonction de la valeur des tentatives de connexion.
- Si toutes les tentatives de connexion échouent et que l'origine fait partie d'un groupe d'origine, CloudFront tente de se connecter à l'origine secondaire. Si le nombre spécifié de tentatives de connexion à l'origine secondaire échouent, CloudFront renvoie une réponse d'erreur au visualiseur.

- Si toutes les tentatives de connexion échouent et que l'origine ne fait pas partie d'un groupe d'origine, CloudFront renvoie une réponse d'erreur au visualiseur.

Délai de réponse (origines personnalisées uniquement)

Le délai de réponse de l'origine, également appelé délai de demande à l'origine ou délai d'attente des opérations de lecture depuis l'origine, s'applique aux deux valeurs suivantes :

- Durée (en secondes) d' CloudFront attente d'une réponse après avoir transmis une demande à l'origine.
- Durée (en secondes) d' CloudFront attente après réception d'un paquet de réponse de l'origine et avant de recevoir le paquet suivant.

> **Tip**
>
> Si vous souhaitez augmenter la valeur de délai de réponse de l'origine parce que les utilisateurs rencontrent des erreurs de code d'état HTTP 504, envisagez d'explorer d'autres moyens pour éliminer ces erreurs avant de modifier la valeur de délai. Consultez les suggestions de dépannage dans the section called "Code d'état HTTP 504 (délai d'expiration de la passerelle)".

CloudFront le comportement dépend de la méthode HTTP utilisée dans la requête du visualiseur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas ou cesse de répondre dans le délai imparti, interrompt CloudFront la connexion. CloudFront essaie à nouveau de se connecter en fonction de la valeur dethe section called "Tentatives de connexion".
- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` demandes : si l'origine ne répond pas pendant le délai de lecture, interrompt CloudFront la connexion et n'essaie plus de contacter l'origine. Le client peut soumettre à nouveau la demande si nécessaire.

Délai d'attente des connexions actives (origines personnalisées uniquement)

Le délai de conservation correspond à la durée (en secondes) des CloudFront tentatives de maintien d'une connexion à votre origine personnalisée après réception du dernier paquet de réponse. Maintenir une connexion persistante permet de gagner le temps requis pour ré-établir la connexion

TCP et établir une autre liaison TLS pour les demandes ultérieures. L'augmentation du délai de conservation permet d'améliorer la request-per-connection métrique des distributions.

> **Note**
>
> Pour que la valeur Délai d'attente des connexions actives ait un effet, votre origine doit être configurée pour autoriser les connexions persistantes.

Quotas de délai de réponse et de maintien en vie

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

- Pour le délai de réponse, la valeur par défaut est de 30 secondes.
- Pour le délai de conservation, la valeur par défaut est de 5 secondes.
- Pour l'un ou l'autre des quotas, vous pouvez spécifier une valeur comprise entre 1 et 60 secondes. Pour demander une augmentation, créez un dossier dans le AWS Support Center Console/.

Après avoir demandé une augmentation du délai d'expiration pour votre Compte AWS, mettez à jour les origines de votre distribution afin qu'elles présentent les valeurs de délai de réponse et de délai de maintien en vie souhaitées. Une augmentation du quota de votre compte ne met pas automatiquement à jour vos origines. Par exemple, si vous utilisez une fonction Lambda @Edge pour définir un délai de maintien en vie de 90 secondes, votre origine doit déjà avoir un délai de maintien en vie de 90 secondes ou plus. Dans le cas contraire, votre fonction Lambda @Edge risque de ne pas s'exécuter.

Pour plus d'informations sur les quotas de distribution, consultezQuotas généraux sur les distributions.

Paramètres de comportement du cache

En définissant le comportement du cache, vous pouvez configurer diverses CloudFront fonctionnalités pour un modèle de chemin d'URL donné pour les fichiers de votre site Web. Par exemple, un comportement de cache peut s'appliquer à tous les `.jpg` fichiers du `images` répertoire

d'un serveur Web que vous utilisez comme serveur d'origine CloudFront. Les fonctionnalités que vous pouvez configurer pour chaque comportement de cache sont les suivantes :

- Le modèle de chemin d’accès
- Si vous avez configuré plusieurs origines pour votre CloudFront distribution, l'origine vers laquelle vous CloudFront souhaitez transférer vos demandes
- S’il convient ou non de transférer les chaînes de requête à votre origine
- Si l’accès aux fichiers spécifiés requiert ou non des URL signées
- S’il convient ou non d’exiger que les utilisateurs utilisent HTTPS pour accéder à ces fichiers
- Durée minimale pendant laquelle ces fichiers restent dans le CloudFront cache, quelle que soit la valeur des `Cache-Control` en-têtes ajoutés aux fichiers par votre origine

Lorsque vous créez une distribution, vous spécifiez les paramètres du comportement de cache par défaut, lequel achemine automatiquement toutes les demandes vers l’origine que vous spécifiez lors de la création de la distribution. Après avoir créé une distribution, vous pouvez créer des comportements de cache supplémentaires qui définissent le mode de CloudFront réponse lorsqu'il reçoit une demande d'objets correspondant à un modèle de chemin, par exemple,`*.jpg`. Si vous créez des comportements de cache supplémentaires, le comportement de cache par défaut est toujours le dernier à être traité. Les autres comportements de cache sont traités dans l'ordre dans lequel ils sont répertoriés dans la CloudFront console ou, si vous utilisez l' CloudFront API, dans l'ordre dans lequel ils sont répertoriés dans l'`DistributionConfig`élément de distribution. Pour plus d’informations, consultez Modèle de chemin d’accès.

Lorsque vous créez un comportement de cache, vous spécifiez l'origine à partir de laquelle vous CloudFront souhaitez obtenir les objets. Par conséquent, si vous CloudFront souhaitez distribuer des objets provenant de toutes vos origines, vous devez avoir au moins autant de comportements de cache (y compris le comportement de cache par défaut) que d'origines. Par exemple, si vous avez deux origines et que vous utilisez uniquement le comportement de cache par défaut, le comportement de cache par défaut permet d'obtenir des objets CloudFront à partir de l'une des origines, mais l'autre origine n'est jamais utilisée.

Pour connaître le nombre maximum actuel de comportements de cache que vous pouvez ajouter à une distribution ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Rubriques

- Modèle de chemin d’accès

- Origine ou groupe d’origines
- Viewer Protocol Policy
- Méthodes HTTP autorisées
- Configuration du chiffrement au niveau du champ
- Méthodes HTTP mises en cache
- Mise en cache basée sur des en-têtes de demande sélectionnés
- En-têtes de la liste d’autorisation
- Mise en cache d’un objet
- Durée de vie minimale
- Durée de vie (TTL) maximale
- TTL par défaut
- Réacheminer les cookies
- Cookies de la liste d’autorisation
- Réacheminement et mise en cache des chaînes de requête
- Liste d’autorisation des chaînes de requête
- Smooth Streaming
- Restreindre l’accès des utilisateurs (utiliser des URL signées ou des cookies signés)
- Signataires autorisés
- Compte AWS chiffres
- Compresser des objets automatiquement
- CloudFront événement
- ARN de fonction Lambda
- Inclure le corps

Modèle de chemin d’accès

Un modèle de chemin d’accès (par exemple, `images/*.jpg`) spécifie les demandes auxquelles vous voulez que ce comportement de cache s’applique. Lors de la CloudFront réception d'une demande d'utilisateur final, le chemin demandé est comparé aux modèles de chemin dans l'ordre dans lequel les comportements du cache sont répertoriés dans la distribution. La première correspondance détermine le comportement de cache qui s’applique à la demande. Imaginons, par

exemple, que vous ayez trois comportements de cache avec les trois modèles de chemin suivants classés par ordre :

- `images/*.jpg`
- `images/*`
- `*.gif`

> **Note**
>
> Vous pouvez éventuellement inclure une barre oblique (/) au début du modèle de tracé, par exemple,`/images/*.jpg`. CloudFront le comportement est le même avec ou sans le premier /. Si vous ne spécifiez pas le/au début du chemin, ce caractère est automatiquement implicite ; CloudFront traite le chemin de la même manière, avec ou sans le premier /. Par exemple, CloudFront traite `/*product.jpg` la même chose que `*product.jpg`

Une demande du fichier `images/sample.gif` ne correspondant pas au premier modèle de chemin d'accès, les comportements de cache associés ne s'appliquent pas à la demande. Comme le fichier satisfait bel et bien au second modèle, les comportements de cache associés au deuxième modèle s'appliquent même si la demande correspond aussi au troisième modèle.

> **Note**
>
> Lorsque vous créez une distribution, la valeur de Modèle de chemin pour le comportement de cache par défaut est définie sur * (tous les fichiers) et ne peut pas être modifiée. Cette valeur CloudFront entraîne le transfert de toutes les demandes relatives à vos objets vers l'origine que vous avez spécifiée dans le Domaine d'origine champ. Si la demande d'un objet ne correspond au modèle de chemin d'aucun autre comportement de cache, CloudFront applique le comportement que vous spécifiez dans le comportement de cache par défaut.

> **Important**
>
> Définissez soigneusement les modèles de chemin et leur séquence, sans quoi vous risquez d'offrir aux utilisateurs un accès non souhaité à votre contenu. Par exemple, imaginons qu'une demande corresponde au modèle de chemin de deux comportements de cache. Le premier comportement de cache n'exige pas d'URL signées, à l'inverse

du second comportement de cache. Les utilisateurs peuvent accéder aux objets sans utiliser d'URL signée car CloudFront traite le comportement du cache associé à la première correspondance.

Si vous travaillez avec un MediaPackage canal, vous devez inclure des modèles de chemin spécifiques pour le comportement du cache que vous définissez pour le type de point de terminaison de votre origine. Par exemple, pour un point de terminaison DASH, tapez `*.mpd` pour Path Pattern (Modèle de chemin). Pour plus d'informations et pour obtenir des instructions spécifiques, consultez Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.

Le chemin que vous spécifiez s'applique aux demandes pour tous les fichiers du répertoire spécifié et des sous-répertoires situés sous le répertoire spécifié. CloudFront ne prend pas en compte les chaînes de requête ou les cookies lors de l'évaluation du modèle de chemin. Par exemple, si un répertoire `images` contient les sous-répertoires `product1` et `product2`, le modèle de chemin d'accès `images/*.jpg` s'applique aux demandes concernant un fichier .jpg des répertoires `images`, `images/product1` et `images/product2`. Si vous voulez appliquer un autre comportement de cache aux fichiers du répertoire `images/product1` qu'à ceux des répertoires `images` et `images/product2`, créez un comportement de cache distinct pour `images/product1` et déplacez ce comportement de cache vers un emplacement au-dessus (avant) du comportement de cache du répertoire `images`.

Vous pouvez utiliser les caractères génériques suivants dans votre modèle de chemin d'accès :

- `*` correspond à 0 caractère ou plus.
- `?` correspond à 1 caractère exactement.

L'exemple suivant montre le fonctionnement des caractères génériques :

Modèle de chemin d'accès	Fichiers correspondant au modèle de chemin d'accès
`*.jpg`	Tous les fichiers .jpg.
`images/*.jpg`	Tous les fichiers .jpg dans le répertoire `images` et dans les sous-répertoires du répertoire `images`.

Modèle de chemin d'accès	Fichiers correspondant au modèle de chemin d'accès
`a*.jpg`	• Tous les fichiers .jpg dont le nom commence par `a` : par exemple, `apple.jpg` et `appalachian_trail_2012_05_21.jpg` . • Tous les fichiers .jpg dont le chemin d'accès commence par `a` : par exemple, `abra/cadabra/magic.jpg` .
`a??.jpg`	Tous les fichiers .jpg dont le nom commence par `a`, suivi de deux autres caractères exactement : par exemple, `ant.jpg` et `abe.jpg`.
`*.doc*`	Tous les fichiers .jpg dont l'extension de nom de fichier commence par `.doc` : par exemple, les fichiers `.doc`, `.docx` et `.docm`. Vous ne pouvez pas utiliser le modèle de chemin d'accès `*.doc?` dans ce cas, parce que ce modèle ne s'appliquerait pas aux demandes relatives aux fichiers `.doc` ; le caractère générique ? remplace exactement un seul caractère.

La longueur maximale d'un modèle de chemin est de 255 caractères. La valeur peut contenir l'un des caractères suivants :

- A-Z, a-z

  Les modèles de chemin d'accès étant sensibles à la casse, le modèle de chemin d'accès `*.jpg` ne s'applique pas au fichier `LOGO.JPG`.
- 0-9
- _ - . * $ / ~ " ' @ : +
- &, transmis et renvoyé comme `&`

Normalisation des trajectoires

CloudFront normalise les chemins d'URI conformément à la RFC 3986, puis fait correspondre le chemin avec le comportement de cache correct. Une fois que le comportement du cache correspond,

CloudFront envoie le chemin d'URI brut à l'origine. S'ils ne correspondent pas, les demandes sont associées à votre comportement de cache par défaut.

Certains caractères sont normalisés et supprimés du chemin, tels que les barres obliques multiples (`//`) ou les points (). `..` Cela peut modifier l'URL CloudFront utilisée pour qu'elle corresponde au comportement de cache prévu.

Example Exemple

Vous spécifiez les `/a*` chemins `/a/b*` et pour le comportement de votre cache.

- Un visualiseur qui envoie le `/a/b?c=1` chemin correspondra au comportement du `/a/b*` cache.
- Un visualiseur qui envoie le `/a/b/..?c=1` chemin correspondra au comportement du `/a*` cache.

Pour contourner les chemins normalisés, vous pouvez mettre à jour les chemins de vos requêtes ou le modèle de chemin correspondant au comportement du cache.

Origine ou groupe d’origines

Ce paramètre s'applique uniquement lorsque vous créez ou mettez à jour un comportement de cache pour une distribution existante.

Entrez la valeur d’une origine ou d’un groupe d’origines existant. Cela identifie l'origine ou le groupe d'origine vers lequel vous souhaitez CloudFront acheminer les demandes lorsqu'une demande (telle que https://example.com/logo.jpg) correspond au modèle de chemin d'un comportement de cache (tel que *.jpg) ou au comportement de cache par défaut (*).

Viewer Protocol Policy

Choisissez la politique de protocole que vous souhaitez que les spectateurs utilisent pour accéder à votre contenu dans des emplacements CloudFront périphériques :

- HTTP et HTTPS : les deux protocoles peuvent être utilisés.
- Rediriger HTTP vers HTTPS : les deux protocoles peuvent être utilisés, mais les requêtes HTTP sont automatiquement redirigées vers des requêtes HTTPS.
- HTTPS uniquement : l’accès au contenu ne peut se faire qu’à l’aide du protocole HTTPS.

Pour plus d’informations, consultez Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

Méthodes HTTP autorisées

Spécifiez les méthodes HTTP que vous CloudFront souhaitez traiter et transmettre à votre origine :

- GET, HEAD : Vous ne pouvez l'utiliser CloudFront que pour récupérer des objets depuis votre origine ou pour obtenir des en-têtes d'objets.
- GET, HEAD, OPTIONS : vous CloudFront ne pouvez les utiliser que pour obtenir des objets depuis votre origine, obtenir des en-têtes d'objets ou récupérer une liste des options prises en charge par votre serveur d'origine.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE : vous pouvez les utiliser CloudFront pour obtenir, ajouter, mettre à jour et supprimer des objets, ainsi que pour obtenir des en-têtes d'objets. De plus, vous pouvez exécuter d'autres opérations POST telles que l'envoi de données à partir d'un formulaire web.

> **Note**
>
> CloudFront met en cache les réponses aux `HEAD` demandes `GET` et, éventuellement, `OPTIONS` aux demandes. Les réponses aux `OPTIONS` demandes sont mises en cache séparément des réponses aux `HEAD` demandes `GET` et aux demandes (la `OPTIONS` méthode est incluse dans la clé de cache pour les `OPTIONS` demandes). CloudFront ne met pas en cache les réponses aux demandes utilisant d'autres méthodes.

> **Important**
>
> Si vous choisissez GET, HEAD, OPTIONS ou GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE, il se peut que vous ayez besoin de limiter l'accès à votre compartiment Amazon S3 ou à votre origine personnalisée pour empêcher que les utilisateurs n'exécutent des opérations qu'ils ne sont pas autorisés à faire. Les exemples suivants expliquent comment limiter l'accès :
>
> - Si vous utilisez Amazon S3 comme origine pour votre distribution : créez un contrôle CloudFront d'accès à l'origine pour restreindre l'accès à votre contenu Amazon S3 et autorisez le contrôle d'accès à l'origine. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes uniquement parce que vous souhaitez les utiliserPUT, vous devez tout de même configurer les politiques de compartiment Amazon S3 afin de

traiter les DELETE demandes de manière appropriée. Pour plus d'informations, consultez Restreindre l'accès à une origine Amazon Simple Storage Service.

- Si vous utilisez une origine personnalisée : configurez votre serveur d'origine pour qu'il gère toutes les méthodes. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes uniquement parce que vous souhaitez les utiliserPOST, vous devez tout de même configurer votre serveur d'origine pour traiter les DELETE demandes de manière appropriée.

Configuration du chiffrement au niveau du champ

Si vous souhaitez appliquer un chiffrement au niveau du champ à des champs de données spécifiques, dans la liste déroulante, choisissez une configuration de chiffrement au niveau du champ.

Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Méthodes HTTP mises en cache

Spécifiez si vous souhaitez CloudFront mettre en cache la réponse depuis votre origine lorsqu'un utilisateur envoie une OPTIONS demande. CloudFront met toujours en cache les réponses GET et les HEAD demandes.

Mise en cache basée sur des en-têtes de demande sélectionnés

Spécifiez si vous souhaitez CloudFront mettre en cache les objets en fonction des valeurs des en-têtes spécifiés :

- Aucune (améliore la mise en cache) : CloudFront ne met pas en cache vos objets en fonction des valeurs d'en-tête.
- Allowlist — met en CloudFront cache vos objets en fonction uniquement des valeurs des en-têtes spécifiés. Utilisez Allowlist Headers pour choisir les en-têtes sur lesquels vous souhaitez CloudFront baser la mise en cache.
- Tout : CloudFront ne met pas en cache les objets associés à ce comportement de cache. Au lieu de cela, CloudFront envoie chaque demande à l'origine. (Déconseillé pour les origines Amazon S3.)

Quelle que soit l'option que vous choisissez, CloudFront transfère certains en-têtes vers votre origine et prend des mesures spécifiques en fonction des en-têtes que vous transférez. Pour plus d'informations sur le mode de CloudFront gestion du transfert d'en-têtes, consultezEn-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3).

Pour plus d'informations sur la configuration de la mise en cache à l'aide CloudFront des en-têtes de demande, consultez. Contenu du cache basé sur les en-têtes des demandes

En-têtes de la liste d’autorisation

Ces paramètres s'appliquent uniquement lorsque vous choisissez Allowlist for Cache en fonction des en-têtes de demande sélectionnés.

Spécifiez les en-têtes que vous souhaitez prendre en compte lors CloudFront de la mise en cache de vos objets. Sélectionnez les en-têtes dans la liste des en-têtes disponibles et choisissez Ajouter. Pour transmettre un en-tête personnalisé, entrez le nom de l’en-tête dans le champ et choisissez Ajouter un en-tête personnalisé.

Pour connaître le nombre maximal actuel d’en-têtes qu’il est possible d’ajouter en liste d’autorisation pour chaque comportement de cache, ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas sur les en-têtes.

Mise en cache d’un objet

Si votre serveur d'origine ajoute un `Cache-Control` en-tête à vos objets pour contrôler la durée pendant laquelle les objets restent dans le CloudFront cache et si vous ne souhaitez pas modifier la `Cache-Control` valeur, choisissez Utiliser les en-têtes du cache d'origine.

Pour définir la durée minimale et maximale pendant laquelle vos objets restent dans le CloudFront cache, quels que soient `Cache-Control` les en-têtes, et la durée par défaut pendant laquelle vos objets restent dans le CloudFront cache lorsque l'`Cache-Control`en-tête est absent d'un objet, choisissez Personnaliser. Puis, dans les champs Durée de vie minimale, Durée de vie par défaut et Durée de vie maximale, spécifiez la valeur applicable.

Pour plus d’informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Durée de vie minimale

Spécifiez la durée minimale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant d' CloudFront envoyer une autre demande à l'origine pour déterminer si l'objet a été mis à jour.

Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Durée de vie (TTL) maximale

Spécifiez la durée maximale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de demander CloudFront à votre origine si l'objet a été mis à jour. La valeur que vous spécifiez pour Durée de vie maximale s'applique uniquement quand votre origine ajoute aux objets les en-têtes HTTP tels que `Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires`. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Pour spécifier une valeur pour Durée de vie maximale, vous devez choisir l'option Personnaliser pour le paramètre Mise en cache d'un objet.

La valeur par défaut de Durée de vie maximale est 31 536 000 secondes (soit 1 année). Si vous remplacez la valeur de Durée de vie minimale ou Durée de vie par défaut par une valeur supérieure à 31 536 000 secondes, la valeur par défaut de Durée de vie maximale prend la valeur de Durée de vie par défaut.

TTL par défaut

Spécifiez la durée par défaut, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de transmettre une CloudFront autre demande à votre origine afin de déterminer si l'objet a été mis à jour. La valeur que vous spécifiez pour Default TTL (TTL par défaut) s'applique uniquement quand votre origine n'ajoute aps des en-têtes HTTP tels que`Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires` aux objets. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Pour spécifier une valeur pour Durée de vie par défaut, vous devez choisir l'option Personnaliser pour le paramètre Mise en cache d'un objet.

La valeur par défaut de Durée de vie par défaut est 86 400 secondes (soit 1 journée). Si vous remplacez la valeur de Durée de vie minimale par une valeur supérieure à 86 400 secondes, la valeur par défaut de Durée de vie par défaut prend la valeur de Durée de vie minimale.

Réacheminer les cookies

> **Note**
>
> Pour les origines Amazon S3, cette option s'applique uniquement aux compartiments configurés en tant que point de terminaison de site Web.

Spécifiez si vous CloudFront souhaitez transférer les cookies vers votre serveur d'origine et, dans l'affirmative, lesquels. Si vous choisissez de transférer uniquement les cookies sélectionnés (liste d'autorisation de cookies), entrez les noms de cookies dans le champ Cookies de la liste d'autorisation. Si vous choisissez Tout, CloudFront transfère tous les cookies, quel que soit le nombre utilisé par votre application.

Amazon S3 ne traite pas les cookies, et la transmission des cookies à l'origine réduit la capacité de mise en cache. Pour les comportements de cache qui transmettent les demandes à une origine Amazon S3, choisissez None (Aucun) pour Forward Cookies (Réacheminer les cookies).

Pour plus d'informations sur la transmission des cookies à l'origine, consultez Contenu du cache basé sur les cookies.

Cookies de la liste d'autorisation

> **Note**
>
> Pour les origines Amazon S3, cette option s'applique uniquement aux compartiments configurés en tant que point de terminaison de site Web.

Si vous avez choisi Allowlist dans la liste des cookies de transfert, entrez dans le champ Allowlist Cookies les noms des cookies que vous souhaitez transférer CloudFront vers votre serveur d'origine pour ce comportement de cache. Entrez chaque nom de cookie sur une nouvelle ligne.

Vous pouvez utiliser les caractères génériques suivants pour spécifier les noms de cookie :

- * correspond à 0 caractère ou plus dans le nom de cookie
- ? correspond à 1 caractère exactement dans le nom de cookie.

Imaginons, par exemple, qu'une demande inclue un cookie nommé :

`userid_`*`member-number`*

Où chacun de vos utilisateurs possède une valeur unique pour *`member-number`*. Vous souhaitez CloudFront mettre en cache une version distincte de l'objet pour chaque membre. Vous pouvez y parvenir en transférant tous les cookies vers votre source, mais les demandes des utilisateurs incluent certains cookies que vous ne souhaitez pas mettre CloudFront en cache. Vous pouvez également spécifier la valeur suivante comme nom de cookie, ce qui entraîne CloudFront le transfert à l'origine de tous les cookies commençant par `userid_` :

`userid_*`

Pour connaître le nombre maximal actuel de noms de cookies qu'il est possible d'ajouter en liste d'autorisation pour chaque comportement de cache, ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas sur les cookies (paramètres de cache hérités).

Réacheminement et mise en cache des chaînes de requête

CloudFront peut mettre en cache différentes versions de votre contenu en fonction des valeurs des paramètres de chaîne de requête. Choisissez l'une des options suivantes :

Aucun (optimise la mise en cache)

Choisissez cette option si votre origine renvoie la même version d'un objet quelles que soient les valeurs des paramètres de la chaîne de requête. Cela augmente la probabilité de CloudFront répondre à une demande depuis le cache, ce qui améliore les performances et réduit la charge sur votre origine.

Tout réacheminer, cache basé sur la liste d'autorisation

Sélectionnez cette option si votre serveur d'origine renvoie des versions différentes de vos objets en fonction d'un ou de plusieurs paramètres de la chaîne de requête. Spécifiez ensuite les paramètres que vous CloudFront souhaitez utiliser comme base pour la mise en cache dans le Liste d'autorisation des chaînes de requête champ.

Tout réacheminer, cache basé sur tout

Sélectionnez cette option si votre serveur d'origine renvoie des versions différentes de vos objets en fonction de tous les paramètres de la chaîne de requête.

Pour plus d'informations sur la mise en cache en fonction des paramètres de la chaîne de requête, y compris sur la façon d'améliorer les performances, consultez la page Contenu du cache basé sur les paramètres de chaîne de requête.

Liste d’autorisation des chaînes de requête

Ce paramètre s'applique uniquement lorsque vous choisissez Transférer tout, cache basé sur la liste d'autorisation pourRéacheminement et mise en cache des chaînes de requête. Vous pouvez spécifier les paramètres de chaîne de requête que vous CloudFront souhaitez utiliser comme base pour la mise en cache.

Smooth Streaming

Choisissez Oui si vous voulez distribuer des fichiers multimédias au format Microsoft Smooth Streaming et que vous n’avez pas de serveur IIS.

Choisissez Non si vous avez un serveur Microsoft IIS que vous souhaitez utiliser comme origine pour distribuer des fichiers multimédias au format Microsoft Smooth Streaming ou si vous ne distribuez pas de fichiers multimédias Smooth Streaming.

> **Note**
>
> Si vous spécifiez Oui, vous pouvez continuer à distribuer d’autres contenus en utilisant ce comportement de cache s’ils correspondent à la valeur de Modèle de chemin.

Pour plus d’informations, consultez Configuration de la vidéo à la demande pour Microsoft Smooth Streaming.

Restreindre l’accès des utilisateurs (utiliser des URL signées ou des cookies signés)

Si vous voulez des demandes d’objets qui correspondent à la valeur de `PathPattern` pour que le comportement de cache utilise des URL publiques, choisissez Non.

Si vous voulez des demandes d’objets qui correspondent à la valeur de `PathPattern` pour que le comportement de cache utilise des URL signées, choisissez Oui. Spécifiez ensuite les AWS comptes que vous souhaitez utiliser pour créer des URL signées ; ces comptes sont appelés signataires approuvés.

Pour plus d’informations sur les utilisateurs de confiance, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.

Signataires autorisés

Ce paramètre s'applique uniquement lorsque vous sélectionnez Oui pour Restreindre l'accès des spectateurs (utiliser des URL signées ou des cookies signés).

Choisissez les AWS comptes que vous souhaitez utiliser comme signataires approuvés pour ce comportement de cache :

- Auto-signature : utilisez le compte avec lequel vous êtes actuellement connecté en AWS Management Console tant que signataire de confiance. Si vous êtes actuellement connecté en tant qu'utilisateur IAM, le AWS compte associé est ajouté en tant que signataire de confiance.
- Spécifier des comptes : saisissez les numéros de comptes des utilisateurs de confiance dans le champ Numéros de comptes AWS .

Pour créer des URL signées, un AWS compte doit disposer d'au moins une paire de CloudFront clés active.

> **Important**
>
> Si vous chargez une distribution que vous utilisez déjà pour distribuer le contenu, n'ajoutez des utilisateurs de confiance que lorsque vous êtes prêt à démarrer la génération d'URL signées pour vos objets. Après que vous avez ajouté les utilisateurs de confiance à une distribution, les utilisateurs doivent employer les URL signées pour accéder à un objet qui correspond à la valeur de `PathPattern` pour ce comportement de cache.

Compte AWS chiffres

Ce paramètre s'applique uniquement lorsque vous choisissez Spécifier les comptes pour les signataires approuvés.

Si vous souhaitez créer des URL signées Comptes AWS en plus ou à la place du compte courant, entrez un Compte AWS chiffre par ligne dans ce champ. Notez ce qui suit :

- Les comptes que vous spécifiez doivent avoir au moins une paire de CloudFront clés active. Pour plus d'informations, consultez Créez des paires de clés pour vos signataires.
- Vous ne pouvez pas créer de paires de CloudFront clés pour les utilisateurs IAM. Vous ne pouvez donc pas utiliser les utilisateurs IAM comme signataires de confiance.

- Pour savoir comment obtenir le Compte AWS numéro d'un compte, consultez la section Vos Compte AWS identifiants dans le Référence générale d'Amazon Web Services.
- Si vous entrez le numéro de compte du compte courant, cochez CloudFront automatiquement la case Automatique et supprimez le numéro de compte de la liste des numéros de AWS compte.

Compresser des objets automatiquement

Si vous souhaitez CloudFront compresser automatiquement certains types de fichiers lorsque les utilisateurs acceptent le contenu compressé, choisissez Oui. Lorsque CloudFront vous compressez votre contenu, les téléchargements sont plus rapides car les fichiers sont plus petits et vos pages Web s'affichent plus rapidement pour vos utilisateurs. Pour plus d'informations, consultez Servir des fichiers compressés.

CloudFront événement

Ce paramètre s'applique aux associations de fonctions Lambda.

Vous pouvez choisir d'exécuter une fonction Lambda lorsqu'un ou plusieurs des CloudFront événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un téléspectateur (demande du téléspectateur)
- Avant CloudFront de transmettre une demande à l'origine (demande d'origine)
- Quand CloudFront reçoit une réponse de l'origine (réponse d'origine)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)

Pour plus d'informations, consultez Décidez quel CloudFront événement utiliser pour déclencher une fonction Lambda @Edge.

ARN de fonction Lambda

Ce paramètre s'applique aux associations de fonctions Lambda.

Spécifiez l'Amazon Resource Name (ARN) de la fonction Lambda pour laquelle vous voulez ajouter un déclencheur. Pour savoir comment obtenir l'ARN d'une fonction, reportez-vous à l'étape 1 de la procédure Ajouter des déclencheurs à l'aide de la CloudFront console.

Inclure le corps

Ce paramètre s'applique aux associations de fonctions Lambda.

Pour plus d'informations, consultez la section Inclure le corps.

Paramètres de distribution

Les valeurs suivantes s’appliquent à la totalité de la distribution.

Rubriques

- Catégorie de tarifs
- AWS WAF ACL Web
- Noms de domaine alternatifs (CNAME)
- Certificat SSL
- Prise en charge d’un client SSL personnalisé
- Politique de sécurité (version SSL/TLS minimale)
- Versions de HTTP prises en charge
- Objet racine par défaut
- Journalisation
- Compartiment pour les journaux
- Préfixe de journal
- Journalisation des cookies
- Activation d’IPv6
- Comment
- État de la distribution

Catégorie de tarifs

Choisissez la classe de prix qui correspond au prix maximum que vous souhaitez payer pour le CloudFront service. Par défaut, CloudFront diffuse vos objets à partir d'emplacements périphériques dans toutes les CloudFront régions.

Pour plus d'informations sur les classes de prix et sur l'impact de votre choix sur les CloudFront performances de votre distribution, consultez la section CloudFront Tarification.

AWS WAF ACL Web

Vous pouvez protéger votre CloudFront distribution à l'aide AWS WAFd'un pare-feu d'applications Web qui vous permet de sécuriser vos applications Web et d'API afin de bloquer les demandes avant

qu'elles n'atteignent vos serveurs. Vous pouvez le faire Activer AWS WAF pour les distributions lors de la création ou de la modification d'une CloudFront distribution.

Vous pouvez éventuellement configurer ultérieurement des protections de sécurité supplémentaires pour d'autres menaces spécifiques à votre application dans la AWS WAF console à l'adresse https://console.aws.amazon.com/wafv2/.

Pour plus d'informations à ce sujet AWS WAF, consultez le guide du AWS WAF développeur.

Noms de domaine alternatifs (CNAME)

Facultatif. Spécifiez un ou plusieurs noms de domaine que vous souhaitez utiliser pour les URL de vos objets au lieu du nom de domaine attribué lors de CloudFront la création de votre distribution. Vous devez être propriétaire du nom de domaine ou disposer de l'autorisation de l'utiliser. Vous vérifiez cela en ajoutant un certificat SSL/TLS.

Par exemple, si vous voulez que l'URL de l'objet :

`/images/image.jpg`

se présente ainsi :

`https://www.example.com/images/image.jpg`

et non comme suit :

`https://d111111abcdef8.cloudfront.net/images/image.jpg`

Ajoutez un CNAME pour `www.example.com`.

> **Important**
>
> Si vous ajoutez un CNAME pour `www.example.com` à votre distribution, vous devez également effectuer les opérations suivantes :
>
> - Créez (ou mettez à jour) un enregistrement CNAME avec votre service DNS pour acheminer les requêtes de `www.example.com` vers `d111111abcdef8.cloudfront.net`.
> - Ajoutez un certificat CloudFront auprès d'une autorité de certification (CA) approuvée qui couvre le nom de domaine (CNAME) que vous ajoutez à votre distribution, afin de valider votre autorisation d'utiliser le nom de domaine.

Vous devez avoir l'autorisation de créer un enregistrement CNAME avec le fournisseur de services DNS du domaine. Cela signifie normalement que le domaine vous appartient ou que vous développez une application pour le propriétaire du domaine.

Pour connaître le nombre maximum actuel de noms de domaine alternatifs que vous pouvez ajouter à une distribution ou demander un quota plus élevé (auparavant appelé limite), veuillez consulter Quotas généraux sur les distributions.

Pour plus d'informations sur les noms de domaine alternatifs, consultez Utilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames). Pour plus d'informations sur CloudFront les URL, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.

Certificat SSL

Si vous avez spécifié un nom de domaine alternatif à utiliser avec votre distribution, choisissez Certificat SSL personnalisé, puis, pour valider votre autorisation d'utiliser le nom de domaine alternatif, choisissez un certificat qui couvre cela. Pour que vos utilisateurs utilisent HTTPS pour accéder à vos objets, sélectionnez la valeur applicable.

Note

Avant de pouvoir spécifier un certificat SSL personnalisé, vous devez définir un nom de domaine alternatif valide. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs et Utiliser des noms de domaine alternatifs et le protocole HTTPS.

- CloudFront Certificat par défaut (*.cloudfront.net) : choisissez cette option si vous souhaitez utiliser le nom de CloudFront domaine dans les URL de vos objets, tels que. `https://d111111abcdef8.cloudfront.net/image1.jpg`
- Certificat SSL personnalisé – Choisissez cette option si vous souhaitez utiliser votre propre nom de domaine dans les URL de vos objets en tant que nom de domaine alternatif, tel que `https://example.com/image1.jpg`. Ensuite, choisissez un certificat à utiliser qui couvre le nom de domaine alternatif. La liste des certificats peut inclure l'un des éléments suivants :
  - Certificats fournis par AWS Certificate Manager

- Les certificats que vous avez achetés auprès d'une autorité de certification tierce et chargés dans ACM
- Les certificats que vous avez achetés auprès d'une autorité de certification tierce et chargés dans le magasin de certificats IAM

Si vous choisissez cette valeur, il est recommandé de n'utiliser qu'un nom de domaine alternatif dans vos URL d'objets (https://example.com/logo.jpg). Si vous utilisez votre nom de domaine de CloudFront distribution (https://d111111abcdef8.cloudfront.net/logo.jpg) et qu'un client utilise un ancien visualiseur qui ne prend pas en charge le SNI, la façon dont le lecteur réagit dépend de la valeur que vous avez choisie pour Clients pris en charge :

- Tous les clients : le visualiseur affiche un avertissement car le nom de CloudFront domaine ne correspond pas au nom de domaine de votre certificat SSL/TLS.
- Uniquement les clients qui supportent l'indication du nom du serveur (SNI) : CloudFront abandonne la connexion avec le visualiseur sans renvoyer l'objet.

Prise en charge d'un client SSL personnalisé

S'applique uniquement lorsque vous choisissez un certificat SSL personnalisé (exemple.com) pour le certificat SSL. Si vous avez indiqué un ou plusieurs noms de domaine alternatifs et un certificat SSL personnalisé pour la distribution, choisissez la manière dont vous CloudFront souhaitez traiter les requêtes HTTPS :

- Clients prenant en charge l'indication de nom de serveur (SNI, Server Name Indication) - (recommandé) – Avec ce paramètre, pratiquement tous les navigateurs et clients web modernes peuvent se connecter à la distribution, car ils prennent en charge SNI. Cependant, certains utilisateurs peuvent utiliser d'anciens navigateurs web ou clients qui ne prennent pas en charge SNI, ce qui signifie qu'ils ne peuvent pas se connecter à la distribution.

  Pour appliquer ce paramètre à l'aide de l' CloudFront API, spécifiez-le `sni-only` dans le `SSLSupportMethod` champ. Dans AWS CloudFormation, le champ est nommé `SslSupportMethod` (notez les différentes majuscules).
- Support des clients hérités : avec ce paramètre, les anciens navigateurs web et clients qui ne prennent pas en charge SNI peuvent se connecter à la distribution. Toutefois, ce paramètre entraîne des frais mensuels supplémentaires. Pour connaître le prix exact, rendez-vous sur la page CloudFront des tarifs d'Amazon et recherchez le SSL personnalisé sur la page Dedicated IP.

Pour appliquer ce paramètre à l'aide de l' CloudFront API, spécifiez-le `vip` dans le `SSLSupportMethod` champ. Dans AWS CloudFormation, le champ est nommé `SslSupportMethod` (notez les différentes majuscules).

Pour plus d'informations, consultez Choisissez le mode de CloudFront traitement des requêtes HTTPS.

Politique de sécurité (version SSL/TLS minimale)

Spécifiez la politique de sécurité que vous CloudFront souhaitez utiliser pour les connexions HTTPS avec les utilisateurs (clients). Une politique de sécurité détermine deux paramètres :

- Protocole SSL/TLS minimal CloudFront utilisé pour communiquer avec les utilisateurs.
- Les chiffrements qui CloudFront peuvent être utilisés pour chiffrer le contenu renvoyé aux spectateurs.

Pour de plus amples informations sur les politiques de sécurité, y compris les protocoles et les chiffrements inclus dans chacune d'elles, veuillez consulter Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

Les politiques de sécurité disponibles dépendent des valeurs que vous spécifiez pour le certificat SSL et le support client SSL personnalisé (connu sous le nom `CloudFrontDefaultCertificate` et `SSLSupportMethod` dans l' CloudFront API) :

- Lorsque le certificat SSL est le CloudFront certificat par défaut (*.cloudfront.net) (lorsqu'il `CloudFrontDefaultCertificate` se trouve `true` dans l'API), définit CloudFront automatiquement la politique de sécurité sur TLSv1.
- Lorsque SSL Certificate (Certificat SSL) est Custom SSL Certificate (example.com) [Certificat SSL personnalisé (example.com)] et que Custom SSL Client Support (Prise en charge d'un client SSL personnalisé) est Clients that Support Server Name Indication (SNI) - (Recommended) [Clients qui prennent en charge l'indication de nom de serveur (SNI) - (Recommandé)] (lorsque `CloudFrontDefaultCertificate` est `false` et que `SSLSupportMethod` est `sni-only` dans l'API), , vous pouvez choisir parmi les politiques de sécurité suivantes :
  - TLSv1.2_2021
  - TLSV1.2_2019
  - TLSv1.2_2018

- TLSv1.1_2016
- TLSv1_2016
- TLSv1

- Lorsque SSL Certificate (Certificat SSL) est Custom SSL Certificate (example.com) [SSL personnalisé (example.com)] et que Custom SSL Client Support (Prise en charge d'un client SSL personnalisé) est Legacy Clients Support (Prise en charge de clients hérités) (lorsque `CloudFrontDefaultCertificate` est `false` et que `SSLSupportMethod` est `vip` dans l'API), vous pouvez choisir parmi les politiques de sécurité suivantes :

  - TLSv1
  - SSLv3

  Dans cette configuration, les politiques de sécurité TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 et TLSv1_2016 ne sont pas disponibles dans la console ou dans l'API. CloudFront Si vous souhaitez utiliser l'une de ces politiques de sécurité, vous disposez des options suivantes :

  - Évaluez si votre distribution a besoin d'une prise en charge de client hérité avec adresses IP dédiées. Si vos utilisateurs prennent en charge l'indication de nom de serveur (SNI), nous vous recommandons de mettre à jour le paramètre Custom SSL Client Support (Prise en charge d'un client SSL personnalisé) de votre distribution sur Clients that Support Server Name Indication (SNI) [Clients qui prennent en charge Server Name Indication (SNI)] (définissez `SSLSupportMethod` sur `sni-only` dans l'API). Cela vous permet d'utiliser n'importe laquelle des politiques de sécurité TLS disponibles, et cela peut également réduire vos CloudFront frais.
  - Si vous devez conserver la prise en charge de clients hérités avec des adresses IP dédiées, vous pouvez demander une des autres politiques de sécurité TLS (TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 ou TLSv1_2016) en créant un dossier dans le Centre de support AWS.

    > **Note**
    >
    > Avant de contacter le AWS Support pour demander cette modification, prenez en compte les points suivants :
    >
    > - Lorsque vous ajoutez l'une de ces politiques de sécurité (TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 ou TLSv1_2016) à une distribution d'assistance aux anciens clients, la politique de sécurité est appliquée à toutes les demandes de support des anciens clients de votre compte qui ne sont pas des utilisateurs du SNI. AWS Toutefois, lorsque les visionneuses envoient des demandes

SNI à une distribution avec prise en charge de client hérité, la politique de sécurité de cette distribution s'applique. Pour vous assurer que la politique de sécurité souhaitée est appliquée à toutes les demandes des utilisateurs envoyées à toutes les distributions Legacy Clients Support de votre AWS compte, ajoutez la politique de sécurité souhaitée à chaque distribution individuellement.

- Par définition, la nouvelle politique de sécurité ne prend pas en charge les mêmes chiffrements et protocoles que l'ancienne. Par exemple, si vous choisissez de mettre à niveau la politique de sécurité d'une distribution de TLSv1 vers TLSv1.1_2016, cette distribution ne prendra plus en charge le chiffrement DES-CBC3-SHA. Pour de plus amples informations sur les chiffrements et les protocoles pris en charge par chaque politique de sécurité, veuillez consulter Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

Versions de HTTP prises en charge

Choisissez les versions HTTP que vous souhaitez que votre distribution prenne en charge lorsque les utilisateurs communiquent avec elles CloudFront.

Pour les utilisateurs et CloudFront pour utiliser le protocole HTTP/2, ils doivent prendre en charge le protocole TLSv1.2 ou version ultérieure et l'indication du nom du serveur (SNI). CloudFront n'offre pas de support natif pour gRPC sur HTTP/2.

Pour les utilisateurs et CloudFront pour utiliser le protocole HTTP/3, ils doivent prendre en charge le protocole TLSv1.3 et l'indication du nom du serveur (SNI). CloudFront prend en charge la migration des connexions HTTP/3 pour permettre au spectateur de changer de réseau sans perdre la connexion. Pour plus d'informations sur la migration des connexions à distance, consultez Migration des connexions au RFC 9000.

> **Note**
>
> Pour plus d'informations sur les chiffrements TLSv1.3 pris en charge, consultez Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

Objet racine par défaut

Facultatif. L'objet que vous souhaitez demander CloudFront à votre origine (par exemple,`index.html`) lorsqu'un utilisateur demande l'URL racine de votre distribution (`https://www.example.com/`) au lieu d'un objet de votre distribution (`https://www.example.com/product-description.html`). Spécifier un objet racine par défaut permet d'éviter d'exposer le contenu de votre distribution.

La longueur maximale du nom est de 255 caractères. Le nom peut contenir l'un des caractères suivants :

- A-Z, a-z
- 0-9
- _ - . * $ / ~ " '
- &, transmis et renvoyé comme `&`

Lorsque vous spécifiez l'objet racine par défaut, entrez uniquement le nom de l'objet, par exemple, `index.html`. N'ajoutez pas `/` devant le nom de l'objet.

Pour plus d'informations, consultez Spécifier un objet racine par défaut.

Journalisation

Si vous souhaitez CloudFront enregistrer les informations relatives à chaque demande d'objet et stocker les fichiers journaux dans un compartiment Amazon S3. Vous pouvez activer ou désactiver la journalisation à tout moment. L'activation de la journalisation ne fait l'objet d'aucuns frais supplémentaires, mais vous augmentez le coût habituel Amazon S3 pour le stockage des fichiers et l'accès à ces fichiers dans un compartiment Amazon S3. Vous pouvez supprimer les fichiers journaux à tout moment. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

Compartiment pour les journaux

Si vous avez choisi Activé pour la journalisation, le compartiment Amazon S3 dans lequel vous CloudFront souhaitez stocker l'accès se connecte, par exemple,*myLogs-*`DOC-EXAMPLE-BUCKET.s3.amazonaws.com`.

Important

Ne choisissez pas de compartiment Amazon S3 dans l'une des régions suivantes, car il CloudFront ne fournit pas de journaux standard aux compartiments de ces régions :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Canada Ouest (Calgary)
- Europe (Milan)
- Europe (Espagne)
- Europe (Zurich)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)

Si vous activez la journalisation, CloudFront enregistre les informations relatives à chaque demande d'objet par un utilisateur final et stocke les fichiers dans le compartiment Amazon S3 spécifié. Vous pouvez activer ou désactiver la journalisation à tout moment. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d’accès).

Note

Vous devez avoir les autorisations nécessaires pour obtenir et mettre à jour les listes de contrôle d’accès (ACL) du compartiment Amazon S3 et la liste ACL S3 du compartiment doit vous accorder `FULL_CONTROL`. Cela permet CloudFront d'autoriser le `awslogsdelivery` compte à enregistrer les fichiers journaux dans le compartiment. Pour plus d’informations, consultez Autorisations requises pour configurer la journalisation standard et accéder à vos fichiers journaux.

Préfixe de journal

Facultatif. Si vous avez choisi Activé pour la journalisation, spécifiez la chaîne, le cas échéant, que vous CloudFront souhaitez préfixer aux noms des fichiers journaux d'accès pour cette distribution, par exemple,`exampleprefix/`. La barre oblique de fin (/) est facultative, mais recommandée pour simplifier la navigation dans vos fichiers-journaux. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

Journalisation des cookies

Si vous CloudFront souhaitez inclure des cookies dans les journaux d'accès, choisissez Activé. Si vous choisissez d'inclure des cookies dans les CloudFront journaux, enregistre tous les cookies, quelle que soit la manière dont vous configurez les comportements de cache pour cette distribution : transférer tous les cookies, ne transférer aucun cookie ou transmettre une liste spécifiée de cookies à l'origine.

Comme Amazon S3 ne traite pas les cookies, à moins que votre distribution n'inclue aussi une origine Amazon EC2 ou autre origine personnalisée, nous vous recommandons de choisir Off (Désactivé) comme valeur de Cookie Logging (Journalisation des cookies).

Pour plus d'informations sur les cookies, consultez Contenu du cache basé sur les cookies.

Activation d'IPv6

IPv6 est une nouvelle version du protocole IP. Il remplace éventuellement l'IPv4 et utilise un espace d'adressage plus important. CloudFront répond toujours aux requêtes IPv4. Si vous souhaitez répondre CloudFront aux demandes provenant d'adresses IP IPv4 (telles que 192.0.2.44) et aux demandes provenant d'adresses IPv6 (telles que 2001:0 db 8:85 a3 : :8a2e : 0370:7334), sélectionnez Activer IPv6.

En règle générale, vous devez activer IPv6 si certains de vos utilisateurs sur les réseaux IPv6 souhaitent accéder à vos contenus. Cependant, si vous utilisez des URL ou des cookies signés pour limiter l'accès à vos contenus, ainsi qu'une politique personnalisée qui inclut le paramètre `IpAddress` afin de limiter les adresses IP autorisées à accéder à vos contenus, n'activez pas IPv6. Si vous souhaitez limiter l'accès à un contenu spécifique par adresse IP et ne pas limiter l'accès aux autres contenus (ou limiter l'accès, mais pas par adresse IP), vous pouvez créer deux distributions. Pour plus d'informations sur la création d'URL signées à l'aide d'une politique personnalisée, consultez Création d'une URL signée à l'aide d'une politique personnalisée. Pour plus d'informations sur la création de cookies signés à l'aide d'une politique personnalisée, consultez Définissez des cookies signés à l'aide d'une politique personnalisée.

Si vous utilisez un jeu d'enregistrements de ressources d'alias Route 53 pour acheminer le trafic vers votre CloudFront distribution, vous devez créer un deuxième ensemble d'enregistrements de ressources d'alias lorsque les deux conditions suivantes sont remplies :

- Vous activez IPv6 pour la distribution
- Vous utilisez d'autres noms de domaine dans les URL de vos objets

Pour plus d'informations, consultez la section Acheminer le trafic vers une CloudFront distribution Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

Si vous avez créé un jeu d'enregistrements de ressources CNAME, que ce soit avec Route 53 ou avec un autre service DNS, vous n'avez besoin d'effectuer aucune modification. Un enregistrement CNAME achemine le trafic vers votre distribution, quel que soit le format d'adresse IP de la requête de visionneuse.

Si vous activez IPv6 et les journaux d' CloudFront accès, la `c-ip` colonne inclut des valeurs au format IPv4 et IPv6. Pour plus d'informations, consultez Configuration et utilisation des journaux standard (journaux d'accès).

> **Note**
>
> Pour maintenir une haute disponibilité des clients, CloudFront répondez aux demandes des utilisateurs en utilisant l'IPv4 si nos données suggèrent qu'IPv4 offrira une meilleure expérience utilisateur. Pour connaître le pourcentage de demandes traitées via CloudFront IPv6, activez la CloudFront journalisation de votre distribution et analysez la `c-ip` colonne, qui contient l'adresse IP de l'utilisateur à l'origine de la demande. Ce pourcentage augmentera dans le temps, mais il restera minoritaire car IPv6 n'est pas encore pris en charge par tous les réseaux du monde des utilisateurs. Certains réseaux d'utilisateur offrent une excellente prise en charge d'IPv6, tandis que d'autres ne prennent pas du tout en charge IPv6. (Un réseau de visionneuse est similaire à votre opérateur sans fil ou Internet).
> Pour plus d'informations sur notre support pour IPv6, consultez la CloudFront FAQ. Pour plus d'informations sur l'activation des journaux d'accès, consultez les champs Journalisation, Compartiment pour les journaux et Préfixe de journal.

Comment

Facultatif. Lorsque vous créez une distribution, vous pouvez inclure un commentaire de 128 caractères au plus. Vous pouvez mettre à jour le commentaire à tout moment.

État de la distribution

Indique si vous voulez que la distribution soit activée ou désactivée une fois déployée :

- Activé signifie que dès que la distribution est entièrement déployée, vous pouvez déployer les liens qui utilisent le nom de domaine de la distribution et que les utilisateurs peuvent extraire le contenu. Chaque fois qu'une distribution est activée, CloudFront accepte et gère toutes les demandes de contenu des utilisateurs finaux utilisant le nom de domaine associé à cette distribution.

  Lorsque vous créez, modifiez ou supprimez une CloudFront distribution, la propagation des modifications dans la CloudFront base de données prend du temps. Une demande immédiate d'informations sur une distribution peut ne pas afficher la modification. La propagation s'effectue généralement en quelques minutes, mais une charge système ou une partition du réseau élevées peuvent augmenter cette durée.
- Désactivé signifie que même si la distribution peut être déployée et prête à être utilisée, les utilisateurs ne peuvent pas l'utiliser. Chaque fois qu'une distribution est désactivée, CloudFront n'accepte aucune demande d'utilisateur final utilisant le nom de domaine associé à cette distribution. Tant que vous n'avez pas basculé la distribution de « disabled » en « enabled » (en mettant à jour la configuration de la distribution), personne ne peut l'utiliser.

Vous pouvez basculer une distribution de désactivée à activée (et inversement) aussi souvent que vous le voulez. Suivez la procédure de mise à jour de la configuration d'une distribution. Pour plus d'informations, consultez Mettre à jour une distribution.

Pages d'erreur personnalisées et mise en cache des erreurs

Vous pouvez avoir CloudFront renvoyé un objet au lecteur (par exemple, un fichier HTML) lorsque votre Amazon S3 ou votre origine personnalisée renvoie un code de statut HTTP 4xx ou 5xx à. CloudFront Vous pouvez également spécifier la durée pendant laquelle une réponse d'erreur provenant de votre origine ou d'une page d'erreur personnalisée est mise en cache dans les CloudFront caches périphériques. Pour plus d'informations, consultez Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques.

> **Note**
>
> Comme les valeurs suivantes ne sont pas incluses dans l'Assistant Create Distribution, vous ne pouvez configurer les pages d'erreur personnalisées que lorsque vous mettez à jour une distribution.

Rubriques

Code d'erreur HTTP

Code d'état HTTP pour lequel vous souhaitez CloudFront renvoyer une page d'erreur personnalisée. Vous pouvez configurer CloudFront pour renvoyer des pages d'erreur personnalisées pour aucun, certains ou tous les codes d'état HTTP mis en CloudFront cache.

Chemin de la page de réponse

Le chemin d'accès à la page d'erreur personnalisée (par exemple,`/4xx-errors/403-forbidden.html`) que vous souhaitez renvoyer CloudFront à un lecteur lorsque votre origine renvoie le code d'état HTTP que vous avez spécifié pour le code d'erreur (par exemple, 403). Si vous souhaitez stocker vos objets et vos pages d'erreur personnalisées dans des emplacements différents, votre distribution doit inclure un comportement de cache pour lequel les conditions suivantes sont vraies :

- La valeur de Modèle de chemin correspond au chemin d'accès de vos messages d'erreur personnalisés. Par exemple, supposons que vous ayez enregistré des pages d'erreur personnalisées pour les erreurs 4xx dans un compartiment Amazon S3 d'un répertoire nommé `/4xx-errors`. Votre distribution doit inclure un comportement de cache pour lequel le modèle de chemin transmet les demandes de vos pages d'erreur personnalisées vers cet emplacement, par exemple, /erreurs-4xx/*.
- La valeur d'Origine spécifie la valeur d'ID d'origine pour l'origine qui contient vos pages d'erreur personnalisées.

Code de réponse HTTP

Le code d'état HTTP que vous CloudFront souhaitez renvoyer au visualiseur avec la page d'erreur personnalisée.

Erreur de mise en cache de TTL minimum (secondes)

Durée minimale pendant laquelle vous souhaitez mettre en cache CloudFront les réponses aux erreurs depuis votre serveur d'origine.

Restrictions géographiques

Si vous devez empêcher les utilisateurs de certains pays d'accéder à votre contenu, vous pouvez configurer votre CloudFront distribution avec une liste d'autorisation ou une liste de blocage. Il n'y a pas de frais supplémentaires pour la configuration de restrictions géographiques. Pour plus d'informations, consultez Limitez la distribution géographique de votre contenu.

Tester une distribution

Une fois que vous avez créé votre distribution, CloudFront vous savez où se trouve votre serveur d'origine et vous connaissez le nom de domaine associé à la distribution. Pour tester votre distribution, procédez comme suit :

1. Attendez que votre distribution soit déployée.
   - Consultez les détails de votre distribution dans la console. Lorsque le déploiement de votre distribution est terminé, le champ Dernière modification passe de Déploiement à une date et une heure.
2. Créez des liens vers vos objets avec le nom de CloudFront domaine en suivant la procédure ci-dessous.
3. Testez les liens. CloudFront fournit les objets à votre page Web ou à votre application.

Créez des liens vers vos objets

Utilisez la procédure suivante pour créer des liens de test pour les objets de votre distribution CloudFront Web.

Pour créer des liens aux objets dans une distribution web

1. Copiez le code HTML suivant dans un nouveau fichier, remplacez *nom-domaine* par le nom de domaine de votre distribution et remplacez *nom-objet* par le nom de votre objet.

   ```
   <html>
   <head>My CloudFront Test</head>
   <body>
   <p>My text content goes here.</p>
   <p><img src="https://domain-name/object-name" alt="my test image"
   </body>
   </html>
   ```

   Par exemple, si votre nom de domaine était `d111111abcdef8.cloudfront.net` et que votre objet était `image.jpg`, l'URL du lien sera :

   `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Si votre objet se trouve dans un dossier de votre serveur d'origine, le dossier doit également être inclus dans l'URL. Par exemple, si image.jpg se trouvait dans le dossier images de votre serveur d'origine, l'URL serait :

   `https://d111111abcdef8.cloudfront.net/images/image.jpg`
2. Enregistrez le code HTML dans un fichier ayant .html comme extension de nom de fichier.
3. Ouvrez votre page web dans un navigateur, afin de vous assurer que vous voyez votre objet.

Le navigateur renvoie votre page avec le fichier image intégré, diffusé à partir de l'emplacement périphérique qui a été CloudFront déterminé comme approprié pour servir l'objet.

Mettre à jour une distribution

Dans la CloudFront console, vous pouvez voir les CloudFront distributions associées à votre AWS compte, consulter les paramètres d'une distribution et mettre à jour la plupart des paramètres. Sachez que les modifications que vous apportez aux paramètres ne prennent effet qu'après propagation de la distribution aux emplacements périphériques AWS .

Pour mettre à jour une CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez l'ID d'une distribution. La liste inclut toutes les distributions associées au AWS compte que vous avez utilisé pour vous connecter à la CloudFront console.
3. Pour afficher ou modifier les paramètres d'une distribution, sélectionnez l'onglet Paramètres de distribution.
4. Pour mettre à jour les paramètres généraux, choisissez Modifier. Sinon, choisissez l'onglet correspondant aux paramètres que vous souhaitez afficher ou mettre à jour : Origines ou Comportements.
5. Apportez les mises à jour souhaitées puis, pour enregistrer vos modifications, choisissez Oui, Modifier. Pour plus d'informations sur les champs, consultez les rubriques suivantes :
   - Paramètres généraux : Paramètres de distribution
   - Paramètres d'origine : Paramètres d'origine
   - Paramètres de comportement du cache : Paramètres de comportement du cache
6. Pour supprimer une origine de votre distribution, procédez comme suit :
   a. Choisissez Comportements et assurez-vous d'avoir déplacé tous les comportements de cache par défaut associés à l'origine vers une autre origine.
   b. Choisissez Origines, puis sélectionnez une origine.
   c. Sélectionnez Delete.

Vous pouvez également mettre à jour une distribution à l'aide de l' CloudFront API :

- Pour mettre à jour une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

> **Important**
>
> Lorsque vous mettez à jour votre distribution, sachez qu'un certain nombre de champs supplémentaires sont requis qui ne sont pas nécessaires pour créer une distribution. Pour vous assurer que tous les champs obligatoires sont inclus lorsque vous utilisez l' CloudFront

API pour mettre à jour une distribution, suivez les étapes décrites UpdateDistributiondans le manuel Amazon CloudFront API Reference.

Lorsque vous enregistrez les modifications apportées à votre configuration de distribution, les modifications CloudFront commencent à être propagées à tous les emplacements périphériques. Les modifications de configuration successives se propagent dans leur ordre respectif. Jusqu'à ce que votre configuration soit mise à jour dans un emplacement périphérique CloudFront, continuez à diffuser votre contenu à partir de cet emplacement en fonction de la configuration précédente. Une fois votre configuration mise à jour dans un emplacement périphérique, vous CloudFront commencez immédiatement à diffuser votre contenu à partir de cet emplacement en fonction de la nouvelle configuration.

Vos modifications ne se propagent pas à tous les emplacements périphériques en même temps. Lors CloudFront de la propagation de vos modifications, nous ne pouvons pas déterminer si un emplacement périphérique donné diffuse votre contenu en fonction de la configuration précédente ou de la nouvelle configuration.

Pour savoir quand vos modifications sont propagées, consultez les détails de votre distribution dans la console. Le champ Dernière modification passe de Déploiement à la date et à l'heure auxquelles le déploiement est terminé.

Marquer une distribution

Les balises sont des mots ou des phrases que vous pouvez utiliser pour identifier et organiser vos AWS ressources. Vous pouvez ajouter plusieurs balises à une ressource, chacune de ces balises étant composée d’une clé et d’une valeur que vous définissez. Par exemple, vous pouvez choisir la clé « domaine » et la valeur « exemple.com ». Vous pouvez rechercher et filtrer vos ressources en fonction des balises que vous ajoutez.

Vous pouvez utiliser des balises avec CloudFront, comme dans les exemples suivants :

- Appliquez des autorisations basées sur des balises sur les CloudFront distributions. Pour plus d’informations, consultez ABAC avec CloudFront.
- Suivez les informations de facturation dans différentes catégories. Lorsque vous appliquez des balises à des CloudFront distributions ou à d'autres AWS ressources (telles que des instances Amazon EC2 ou des compartiments Amazon S3) et que vous activez les balises, vous AWS

générez un rapport de répartition des coûts sous forme de valeur séparée par des virgules (fichier CSV) avec votre utilisation et vos coûts agrégés par vos balises actives.

Vous pouvez appliquer des balises associées à des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires) pour organiser les coûts relatifs à divers services. Pour en savoir plus sur l'utilisation des identifications pour la répartition des coûts, consultez Utilisation des identifications de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

Remarques

- Vous pouvez appliquer des balises aux distributions, mais pas aux invalidations ni aux identités Origin Access Identity.
- L'éditeur de balises et les groupes de ressources ne sont actuellement pas pris en charge pourCloudFront.
- Pour connaître le nombre maximum de balises que vous pouvez actuellement ajouter à une distribution, veuillez consulter la page Quotas généraux.

Table des matières

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises :

- Pour connaître le nombre maximal de balises par distribution, consultezQuotas généraux.
- Longueur de clé maximale – 128 caractères Unicode
- Longueur de valeur maximale – 256 caractères Unicode
- Caractères acceptés pour les clés et valeurs – a-z, A-Z, 0-9, espace et les caractères suivants : _ . : / = + - and @
- Les clés et valeurs de balise sont sensibles à la casse

- N'utilisez pas `aws:` comme préfixe pour les clés. Ce préfixe est réservé pour l'utilisation par AWS .

Ajouter, modifier et supprimer des balises pour les distributions

Vous pouvez utiliser la CloudFront console pour gérer les balises de vos distributions.

Pour ajouter, modifier ou supprimer des balises dans une distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Sélectionnez l'onglet Balises.
4. Choisissez Gérer les balises.
5. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour ajouter un tag, entrez une clé et, éventuellement, une valeur pour le tag. Choisissez Ajouter un nouveau tag pour ajouter d'autres tags.
   - Pour modifier une étiquette, modifiez la clé de l'étiquette, sa valeur ou les deux. Vous pouvez supprimer la valeur d'une étiquette, mais la clé est obligatoire.
   - Pour supprimer une balise, sélectionnez Remove (Supprimer).
6. Sélectionnez Enregistrer les modifications.

Balisage programmatique

Vous pouvez également utiliser l' CloudFront API AWS Command Line Interface (AWS CLI), AWS les SDK et AWS Tools for Windows PowerShell appliquer des balises. Pour plus d'informations, consultez les rubriques suivantes :

- CloudFront Opérations de l'API :
  - ListTagsForResource
  - TagResource
  - UntagResource
- AWS CLI — Voir cloudfront dans le manuel de référence des AWS CLI commandes
- AWS SDK — Consultez la documentation du SDK applicable sur la page de AWS documentation

- Outils pour Windows PowerShell — Voir Amazon CloudFront dans le manuel de référence des AWS Tools for PowerShell applets de commande

Supprimer une distribution

La procédure suivante supprime une distribution à l'aide de la CloudFront console. Pour plus d'informations sur la suppression à l'aide de l' CloudFront API, consultez DeleteDistributionle manuel Amazon CloudFront API Reference.

Si vous devez supprimer une distribution avec un OAC attaché à un compartiment S3, consultez Supprimer une distribution avec un OAC attaché à un compartiment S3 les informations importantes.

> **Note**
>
> Sachez qu'avant de pouvoir supprimer une distribution, vous devez la désactiver, ce qui nécessite l'autorisation de la mettre à jour.
> Si vous désactivez une distribution associée à un autre nom de domaine, elle CloudFront cesse d'accepter du trafic pour ce nom de domaine (tel que www.exemple.com), même si une autre distribution possède un nom de domaine alternatif avec un caractère générique (*) correspondant au même domaine (par exemple *.exemple.com).

Pour supprimer une CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet droit de la CloudFront console, recherchez la distribution que vous souhaitez supprimer.
   - Si la colonne État indique Désactivé, passez à l'étape 6.
   - Si le statut indique Activé mais que la distribution indique toujours Déploiement dans la colonne Dernière modification, attendez que le déploiement soit terminé avant de passer à l'étape 3.
3. Dans le volet droit de la CloudFront console, cochez la case correspondant à la distribution que vous souhaitez supprimer.
4. Choisissez Disable (Désactiver) pour désactiver la distribution, puis Yes, Disable (Oui, désactiver) pour confirmer. Sélectionnez ensuite Fermer.

- La valeur de la colonne Status devient immédiatement Disabled.

5. Attendez que le nouvel horodatage apparaisse sous la colonne Dernière modification.

   - La propagation de votre modification CloudFront à tous les emplacements périphériques peut prendre quelques minutes.

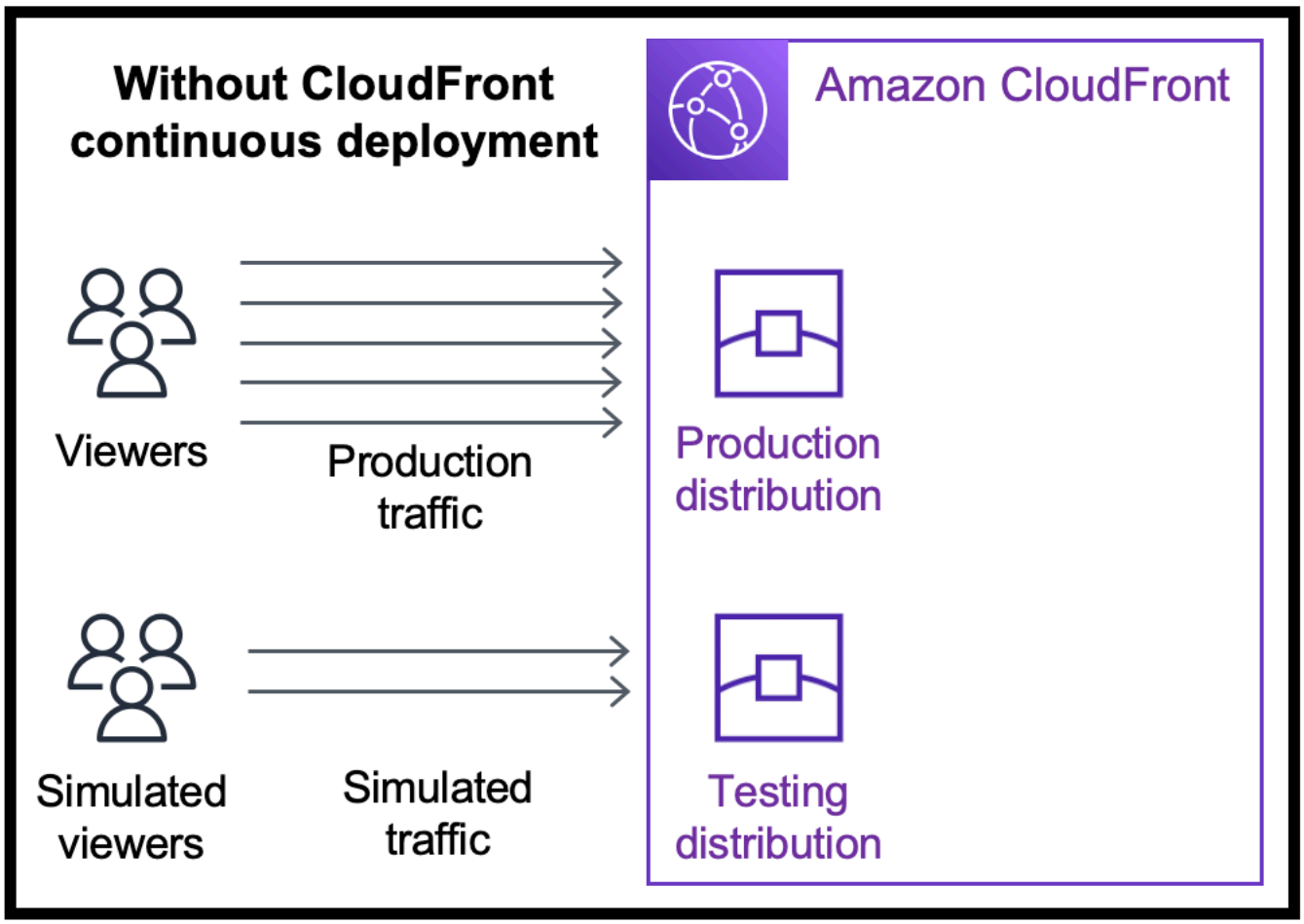
6. Cochez la case correspondant à la distribution que vous souhaitez supprimer.
7. Choisissez Delete (Supprimer), Delete (Supprimer).

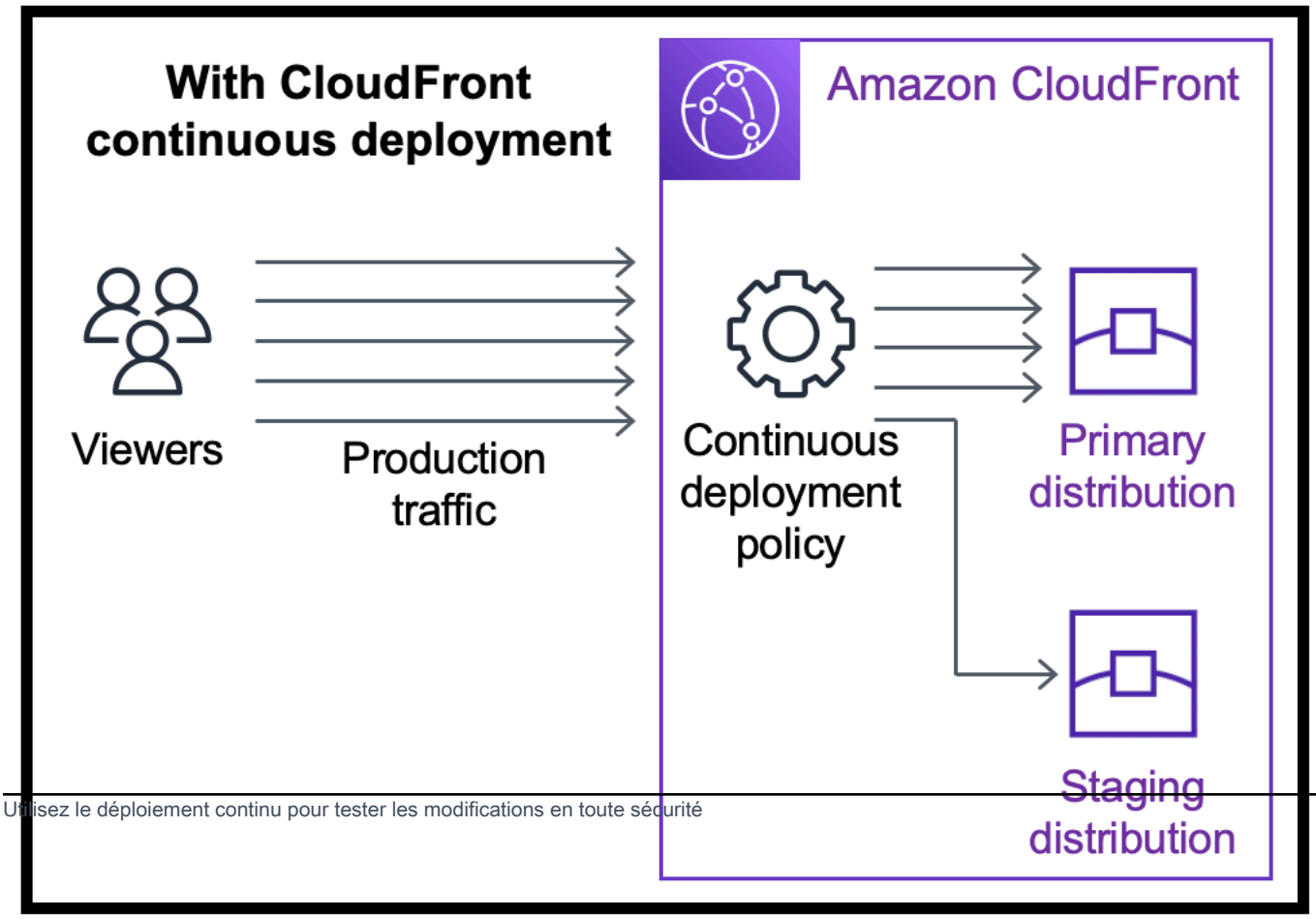
   - Si l'option Supprimer n'est pas disponible, cela signifie que CloudFront votre modification continue de se propager aux emplacements périphériques. Attendez que le nouvel horodatage apparaisse sous la colonne Dernière modification, puis répétez les étapes 6 et 7.

Utilisez le déploiement CloudFront continu pour tester en toute sécurité les modifications de configuration du CDN

Avec le déploiement CloudFront continu d'Amazon, vous pouvez déployer en toute sécurité les modifications apportées à votre configuration CDN en effectuant d'abord des tests avec un sous-ensemble du trafic de production. Vous pouvez utiliser une distribution intermédiaire et une politique de déploiement continu pour envoyer une partie du trafic provenant d’utilisateurs réels (de production) vers la nouvelle configuration du CDN et vérifier qu'elle fonctionne comme prévu. Vous pouvez surveiller les performances de la nouvelle configuration en temps réel et promouvoir la nouvelle configuration pour qu'elle serve l’ensemble du trafic via la distribution principale lorsque vous êtes prêt.

Le schéma suivant montre les avantages du déploiement CloudFront continu. Sans cela, vous devriez tester les changements de configuration du CDN sur un trafic simulé. Avec le déploiement continu, vous pouvez tester les changements sur un sous-ensemble du trafic de production, puis promouvoir les changements vers la distribution principale lorsque vous êtes prêt.


Without CloudFront continuous deployment
Amazon CloudFront
Viewers
Production traffic
Production distribution
Simulated viewers
Simulated traffic
Testing distribution


With CloudFront continuous deployment
Amazon CloudFront
Viewers
Production traffic
Continuous deployment policy
Primary distribution
Staging distribution

Pour en savoir plus sur l'utilisation du déploiement continu, consultez les rubriques suivantes.

Rubriques

CloudFront flux de travail de déploiement continu

Le flux de travail de haut niveau suivant explique comment tester et déployer en toute sécurité des modifications de configuration dans le cadre d' CloudFront un déploiement continu.

1. Choisissez la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production.
2. À partir de la distribution principale, créez une distribution intermédiaire. Une distribution intermédiaire commence comme une copie de la distribution principale.
3. Créez une configuration de trafic dans une politique de déploiement continu et associez-la à la distribution principale. Cela détermine la manière dont le trafic est CloudFront acheminé vers la distribution intermédiaire. Pour plus d'informations sur l’acheminement des demandes vers une distribution intermédiaire, consultez the section called “Acheminer les demandes vers la distribution intermédiaire”.
4. Mettez à jour la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mettre à jour les distributions principales et intermédiaires”.
5. Surveillez la distribution intermédiaire pour déterminer si les changements de configuration fonctionnent comme prévu. Pour plus d'informations sur la surveillance d’une distribution intermédiaire, consultez the section called “Surveiller une distribution intermédiaire”.

   Lorsque vous surveillez la distribution intermédiaire, vous pouvez :

   - Remettre à jour la configuration de la distribution intermédiaire pour continuer à tester les changements de configuration.
   - Mettre à jour la politique de déploiement continu (configuration du trafic) pour envoyer plus ou moins de trafic vers la distribution intermédiaire.

6. Lorsque vous êtes satisfait des performances de la distribution intermédiaire, promouvez la configuration de la distribution intermédiaire vers la distribution principale. La configuration de la distribution intermédiaire est ainsi copiée vers la distribution principale. Cela désactive également la politique de déploiement continu, ce qui signifie que tout le trafic est CloudFront acheminé vers la distribution principale.

Vous pouvez créer une automatisation qui surveille les performances de la distribution intermédiaire (étape 5) et promeut automatiquement la configuration (étape 6) lorsque certains critères sont remplis.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour plus d'informations sur l'utilisation des distributions intermédiaires et des politiques de déploiement continu dans la CloudFront console AWS CLI, l'API ou l' CloudFront API, consultez la section suivante.

Travaillez avec une politique de distribution progressive et de déploiement continu

Vous pouvez créer, mettre à jour et modifier des distributions intermédiaires et des politiques de déploiement continu dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Créez une distribution intermédiaire avec une politique de déploiement continu

Les procédures suivantes vous montrent comment créer une distribution intermédiaire avec une politique de déploiement continu.

Console

Vous pouvez créer une distribution intermédiaire avec une politique de déploiement continu en utilisant le AWS Management Console.

Pour créer une distribution intermédiaire et une politique de déploiement continu (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.

3. Choisissez la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production, c'est celle à partir de laquelle vous allez créer la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Create staging distribution (Créer une distribution intermédiaire). L'assistant Create staging distribution (Créer une distribution intermédiaire) s'ouvre.
5. Dans l'assistant Create staging distribution (Créer une distribution intermédiaire), procédez comme suit :

   a. (Facultatif) Saisissez une description pour la distribution intermédiaire.

   b. Choisissez Next (Suivant).

   c. Modifiez la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mettre à jour les distributions principales et intermédiaires”.

      Lorsque vous avez terminé de modifier la configuration de la distribution intermédiaire, choisissez Next (Suivant).

   d. Utilisez la console pour spécifier la configuration du trafic. Cela détermine la manière dont le trafic est CloudFront acheminé vers la distribution intermédiaire. (CloudFront stocke la configuration du trafic dans une politique de déploiement continu.)

      Pour plus d'informations sur les options d'une configuration de trafic, consultez the section called “Acheminer les demandes vers la distribution intermédiaire”.

      Lorsque vous avez terminé la configuration du trafic, choisissez Next (Suivant).

   e. Passez en revue la configuration de la distribution intermédiaire, y compris la configuration du trafic, puis choisissez Create staging distribution (Créer une distribution intermédiaire).

Lorsque vous avez terminé l'assistant de création d'une distribution intermédiaire dans la CloudFront console CloudFront , procédez comme suit :

- Crée une distribution intermédiaire avec les paramètres que vous avez spécifiés (à l'étape 5c)
- Crée une politique de déploiement continu avec la configuration du trafic que vous avez spécifiée (à l'étape 5d)

- Attache la politique de déploiement continu à la distribution principale à partir de laquelle vous avez créé la distribution intermédiaire

Lorsque la configuration de la distribution principale, avec la politique de déploiement continu attachée, est déployée vers des emplacements périphériques, CloudFront commence à envoyer la partie spécifiée du trafic à la distribution intermédiaire en fonction de la configuration du trafic.

CLI

Pour créer une distribution intermédiaire et une politique de déploiement continu avec le AWS CLI, utilisez les procédures suivantes.

Pour créer une distribution intermédiaire (interface de ligne de commande)

1. Utilisez les commandes aws cloudfront get-distribution et grep ensemble pour obtenir la valeur `ETag` de la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production, c'est celle à partir de laquelle vous allez créer la distribution intermédiaire.

   Voici un exemple de commande. Dans l'exemple suivant, remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.

   ```
   aws cloudfront get-distribution --id primary_distribution_ID | grep 'ETag'
   ```

   Copiez la valeur `ETag` car vous en aurez besoin à l'étape suivante.

2. Utilisez la commande aws cloudfront copy-distribution pour créer une distribution intermédiaire. L'exemple de commande suivant utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande. Dans l'exemple de commande suivant :

   - Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.
   - Remplacez *`primary_distribution_ETag`* par la valeur `ETag` de la distribution principale (que vous avez obtenue à l'étape précédente).
   - (Facultatif) Remplacez *`CLI_example`* par l'ID de la référence appelant de votre choix.

```
aws cloudfront copy-distribution --primary-distribution-
id primary_distribution_ID \
                                 --if-match primary_distribution_ETag \
                                 --staging \
                                 --caller-reference 'CLI_example'
```

La sortie de la commande affiche des informations sur la distribution intermédiaire et sa configuration. Copiez le nom de CloudFront domaine de la distribution intermédiaire, car vous en aurez besoin pour l'étape suivante.

Pour créer une politique de déploiement continu (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `continuous-deployment-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-continuous-deployment-policy. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront create-continuous-deployment-policy --generate-cli-skeleton yaml-
input \
                                                    > continuous-deployment-
policy.yaml
```

2. Ouvrez le fichier nommé `continuous-deployment-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de la politique de déploiement continu de votre choix, puis enregistrez le fichier. Lorsque vous modifiez le fichier :

   - Dans la section `StagingDistributionDnsNames` :
     - Remplacez la valeur de `Quantity` par 1.
     - Pour cela`Items`, collez le nom de CloudFront domaine de la distribution intermédiaire (que vous avez enregistré lors d'une étape précédente).
   - Dans la section `TrafficConfig` :
     - Choisissez un `Type`, `SingleWeight` ou `SingleHeader`.
     - Supprimez les paramètres de l'autre type. Par exemple, si vous souhaitez une configuration du trafic basée sur le poids, définissez `Type` sur `SingleWeight`, puis supprimez les paramètres de `SingleHeaderConfig`.

- Pour utiliser une configuration de trafic basée sur le poids, définissez la valeur de `Weight` sur un nombre décimal compris entre `.01` (un pour cent) et `.15` (quinze pour cent).

Pour plus d'informations sur les options de `TrafficConfig`, consultez the section called "Acheminer les demandes vers la distribution intermédiaire" et the section called "Permanence des sessions pour les configurations basées sur le poids".

3. Utilisez la commande suivante pour créer la politique de déploiement continu à l'aide des paramètres d'entrée du fichier `continuous-deployment-policy.yaml`.

```
aws cloudfront create-continuous-deployment-policy --cli-input-yaml file://
continuous-deployment-policy.yaml
```

Copiez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de la politique de déploiement continu, dont vous aurez besoin lors d'une étape suivante.

Pour attacher une politique de déploiement continu à une distribution principale (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la distribution principale dans un fichier nommé `primary-distribution.yaml`. Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.

```
aws cloudfront get-distribution-config --id primary_distribution_ID --output
 yaml > primary-distribution.yaml
```

2. Ouvrez le fichier nommé `primary-distribution.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Collez l'ID de la politique de déploiement continu (que vous avez copié lors d'une étape précédente) dans le champ `ContinuousDeploymentPolicyId`.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution principale afin d'utiliser la politique de déploiement continu. Remplacez *primary_distribution_ID* par l'ID de la distribution principale.

```
aws cloudfront update-distribution --id primary_distribution_ID --cli-input-yaml
 file://primary-distribution.yaml
```

Lorsque la configuration de la distribution principale, avec la politique de déploiement continu attachée, est déployée vers des emplacements périphériques, CloudFront commence à envoyer la partie spécifiée du trafic à la distribution intermédiaire en fonction de la configuration du trafic.

API

Pour créer une politique de distribution intermédiaire et de déploiement continu avec l' CloudFront API, utilisez les opérations d'API suivantes :

- CopyDistribution
- CreateContinuousDeploymentPolicy

Pour plus d'informations sur les champs que vous spécifiez dans ces appels d'API, consultez :

- the section called “Acheminer les demandes vers la distribution intermédiaire”
- the section called “Permanence des sessions pour les configurations basées sur le poids”
- La documentation de référence de l'API pour votre AWS SDK ou autre client d'API

Après avoir créé une distribution intermédiaire et une politique de déploiement continu, utilisez UpdateDistribution(sur la distribution principale) pour associer la stratégie de déploiement continu à la distribution principale.

Mettre à jour une distribution intermédiaire

Les procédures suivantes vous montrent comment mettre à jour une distribution intermédiaire avec une politique de déploiement continu.

Console

Vous pouvez mettre à jour certaines configurations pour la distribution principale et la distribution intermédiaire. Pour plus d'informations, consultez Mettre à jour les distributions principales et intermédiaires.

Pour mettre à jour une distribution intermédiaire (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s'agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Choisissez View staging distribution (Afficher la distribution intermédiaire).
5. Utilisez la console pour modifier la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called "Mettre à jour les distributions principales et intermédiaires".

Dès que la configuration de la distribution intermédiaire est déployée vers des emplacements périphériques, elle prend effet pour le trafic entrant acheminé vers la distribution intermédiaire.

CLI

Pour mettre à jour une distribution intermédiaire (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la distribution intermédiaire dans un fichier nommé `staging-distribution.yaml`. Remplacez *`staging_distribution_ID`* par l'ID de la distribution intermédiaire.

```
aws cloudfront get-distribution-config --id staging_distribution_ID --output
 yaml > staging-distribution.yaml
```

2. Ouvrez le fichier nommé `staging-distribution.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Modifiez la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mettre à jour les distributions principales et intermédiaires”.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la configuration de la distribution intermédiaire. Remplacez *`staging_distribution_ID`* par l’ID de la distribution intermédiaire.

```
aws cloudfront update-distribution --id staging_distribution_ID --cli-input-yaml
 file://staging-distribution.yaml
```

Dès que la configuration de la distribution intermédiaire est déployée vers des emplacements périphériques, elle prend effet pour le trafic entrant acheminé vers la distribution intermédiaire.

API

Pour mettre à jour la configuration d'une distribution intermédiaire, utilisez UpdateDistribution(sur la distribution intermédiaire) pour modifier la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mettre à jour les distributions principales et intermédiaires”.

Mettre à jour une politique de déploiement continu

Les procédures suivantes vous montrent comment mettre à jour une politique de déploiement continu.

Console

Vous pouvez mettre à jour la configuration du trafic de votre distribution en mettant à jour la politique de déploiement continu.

Pour mettre à jour une politique de déploiement continu (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s'agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Edit policy (Modifier la politique).
5. Modifiez la configuration du trafic dans la politique de déploiement continu. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Lorsque la configuration de la distribution principale avec la politique de déploiement continu mise à jour est déployée sur des emplacements périphériques, CloudFront commence à envoyer du trafic vers la distribution intermédiaire en fonction de la configuration de trafic mise à jour.

CLI

Pour mettre à jour une politique de déploiement continu (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la politique de déploiement continu dans un fichier nommé `continuous-deployment-policy.yaml`. Remplacez *`continuous_deployment_policy_ID`* par l'ID de la politique de déploiement continu. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront get-continuous-deployment-policy-config --
id continuous_deployment_policy_ID \
                                                    --output yaml >
 continuous-deployment-policy.yaml
```

2. Ouvrez le fichier nommé `continuous-deployment-policy.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Modifiez la configuration de la politique de déploiement continu comme vous le souhaitez. Par exemple, vous pouvez passer d'une configuration de trafic basée sur l'en-tête à une configuration de trafic basée sur le poids, ou vous pouvez modifier le pourcentage de trafic

(poids) pour une configuration basée sur le poids. Pour plus d'informations, consultez the section called "Acheminer les demandes vers la distribution intermédiaire" et the section called "Permanence des sessions pour les configurations basées sur le poids".

- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la politique de déploiement continu. Remplacez *`continuous_deployment_policy_ID`* par l'ID de la politique de déploiement continu. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront update-continuous-deployment-policy --
id continuous_deployment_policy_ID \
                                                --cli-input-yaml file://
continuous-deployment-policy.yaml
```

Lorsque la configuration de la distribution principale avec la politique de déploiement continu mise à jour est déployée sur des emplacements périphériques, CloudFront commence à envoyer du trafic vers la distribution intermédiaire en fonction de la configuration de trafic mise à jour.

API

Pour mettre à jour une politique de déploiement continu, utilisez UpdateContinuousDeploymentPolicy.

Promouvoir une configuration de distribution intermédiaire

Les procédures suivantes vous montrent comment promouvoir une configuration de distribution intermédiaire.

Console

Lorsque vous faites la promotion d'une distribution intermédiaire, CloudFront copie la configuration de la distribution intermédiaire vers la distribution principale. CloudFront désactive également la politique de déploiement continu et achemine tout le trafic vers la distribution principale.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour promouvoir la configuration d'une distribution intermédiaire (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s’agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Promote (Promouvoir).
5. Saisissez **`confirm`**, puis choisissez Promote (Promouvoir).

CLI

Lorsque vous faites la promotion d'une distribution intermédiaire, CloudFront copie la configuration de la distribution intermédiaire vers la distribution principale. CloudFront désactive également la politique de déploiement continu et achemine tout le trafic vers la distribution principale.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour promouvoir la configuration d'une distribution intermédiaire (interface de ligne de commande)

- Utilisez la commande aws cloudfront update-distribution-with-staging-config pour promouvoir la configuration de la distribution intermédiaire vers la distribution principale. L'exemple de commande suivant utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande. Dans l’exemple de commande suivant :
  - Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.
  - Remplacez *`staging_distribution_ID`* par l'ID de la distribution intermédiaire.
  - Remplacez *`primary_distribution_ETag`* et *`staging_distribution_ETag`* par les valeurs `ETag` des distributions principale et intermédiaire. Assurez-vous que la valeur de la distribution principale s’affiche en premier, comme indiqué dans l'exemple.

```
aws cloudfront update-distribution-with-staging-config --
id primary_distribution_ID \
                                                    --staging-distribution-
id staging_distribution_ID \
                                                    --if-match
 'primary_distribution_ETag,staging_distribution_ETag'
```

API

Pour promouvoir la configuration d'une distribution intermédiaire vers la distribution principale, utilisez UpdateDistributionWithStagingConfig.

Surveiller une distribution intermédiaire

Pour surveiller les performances d'une distribution intermédiaire, vous pouvez utiliser les mêmes mesures, journaux et rapports que ceux CloudFront fournis pour toutes les distributions. Par exemple :

- Vous pouvez consulter les mesures de CloudFront distribution par défaut (telles que le nombre total de demandes et le taux d'erreur) dans la CloudFront console, et vous pouvez activer des mesures supplémentaires (telles que le taux de réussite du cache et le taux d'erreur par code d'état) moyennant des frais supplémentaires. Vous pouvez également créer des alarmes en fonction de ces métriques.
- Vous pouvez consulter les journaux standard et les journaux en temps réel pour obtenir des informations détaillées sur les demandes reçues par la distribution intermédiaire. Les journaux standard contiennent les deux champs suivants qui vous aident à identifier la distribution principale à laquelle la demande a été initialement envoyée avant de l' CloudFront acheminer vers la distribution intermédiaire : `primary-distribution-id` et`primary-distribution-dns-name`.
- Vous pouvez consulter et télécharger des rapports dans la CloudFront console, par exemple le rapport sur les statistiques du cache.

Découvrez comment fonctionne le déploiement continu

Les rubriques suivantes expliquent le fonctionnement du déploiement CloudFront continu.

Rubriques

Acheminer les demandes vers la distribution intermédiaire

Lorsque vous utilisez le déploiement CloudFront continu, il n'est pas nécessaire de modifier quoi que ce soit concernant les demandes des utilisateurs. Les utilisateurs ne peuvent pas envoyer directement de demandes à une distribution intermédiaire à l'aide d'un nom DNS, d'une adresse IP ou d'un CNAME. Les utilisateurs envoient plutôt des demandes à la distribution principale (de production) et CloudFront acheminent certaines de ces demandes vers la distribution intermédiaire en fonction des paramètres de configuration du trafic définis dans la politique de déploiement continu. Il existe deux types de configurations du trafic :

Basée sur le poids

Une configuration basée sur le poids achemine le pourcentage spécifié de demandes des utilisateurs vers la distribution intermédiaire. Lorsque vous utilisez une configuration basée sur le poids, vous pouvez également activer le maintien des sessions, ce qui permet de s'assurer que CloudFront les demandes provenant du même utilisateur sont traitées dans le cadre d'une seule session. Pour plus d'informations, consultez the section called “Permanence des sessions pour les configurations basées sur le poids”.

Basée sur l'en-tête

Une configuration basée sur l'en-tête achemine les demandes vers la distribution intermédiaire lorsque la demande de l'utilisateur contient un en-tête HTTP spécifique (vous spécifiez l'en-tête et la valeur). Les demandes qui ne contiennent pas l'en-tête et la valeur spécifiés sont acheminées vers la distribution principale. Cette configuration est utile pour les tests locaux ou lorsque vous contrôlez les demandes des utilisateurs.

> **Note**
>
> Les en-têtes acheminés vers votre distribution intermédiaire doivent contenir le préfixe `aws-cf-cd-`.

Permanence des sessions pour les configurations basées sur le poids

Lorsque vous utilisez une configuration basée sur le poids pour acheminer le trafic vers une distribution intermédiaire, vous pouvez également activer la persistance des sessions, ce qui permet de garantir que CloudFront les demandes provenant du même visualiseur sont traitées comme une seule session. Lorsque vous activez le caractère permanent des sessions, CloudFront définit un cookie afin que toutes les demandes émanant d'un même utilisateur au cours d'une même session soient traitées par une seule distribution, principale ou intermédiaire.

Lorsque vous activez la permanence des sessions, vous pouvez également spécifier la durée d'inactivité. Si le visualiseur est inactif (n'envoie aucune demande) pendant cette durée, la session expire et CloudFront traite les futures demandes de ce visualiseur comme une nouvelle session. Vous spécifiez la durée d'inactivité en nombre de secondes, compris entre 300 (cinq minutes) et 3 600 (une heure).

Dans les cas suivants, CloudFront réinitialise toutes les sessions (même les sessions actives) et considère toutes les demandes comme une nouvelle session :

- Vous désactivez ou activez la politique de déploiement continu
- Vous désactivez ou activez le paramètre de permanence des sessions

Mettre à jour les distributions principales et intermédiaires

Lorsqu'une une politique de déploiement continu est attachée à une distribution principale, les changements de configuration suivants sont disponibles pour les distributions principale et intermédiaire :

- Tous les paramètres de comportement du cache, y compris le comportement du cache par défaut
- Tous les paramètres d'origine (origines et groupes d'origines)
- Réponses d'erreur personnalisées (pages d'erreur)
- Restrictions géographiques

- Objet racine par défaut
- Paramètres de journalisation
- Description (commentaire)

Vous pouvez également mettre à jour les ressources externes référencées dans la configuration d'une distribution, telles qu'une politique de cache, une politique d'en-têtes de réponse, une CloudFront fonction ou une fonction Lambda @Edge.

Les distributions principale et intermédiaire ne partagent pas de cache

Les distributions principale et intermédiaire ne partagent pas de cache. Lorsque CloudFront la première demande est envoyée à une distribution intermédiaire, son cache est vide. Il commence à mettre en cache les réponses (s'il est configuré pour le faire) au fur et à mesure que les demandes atteignent la distribution intermédiaire.

Quotas et autres considérations relatives au déploiement continu

CloudFront le déploiement continu est soumis aux quotas suivants et à d'autres considérations.

Quotas

- Nombre maximum de distributions intermédiaires par Compte AWS : 20
- Nombre maximum de politiques de déploiement continu par Compte AWS : 20
- Pourcentage maximal de trafic que vous pouvez envoyer vers une distribution intermédiaire dans une configuration basée sur le poids : 15 %
- Valeurs minimale et maximale pour la durée d'inactivité de la permanence des sessions : 300 à 3 600 secondes

Pour plus d'informations, consultez Quotas.

> **Note**
>
> Lorsque vous utilisez le déploiement continu et que votre distribution principale est définie avec OAC pour l'accès au compartiment S3, mettez à jour votre politique de compartiment S3 pour autoriser l'accès à la distribution intermédiaire. Par exemple, les politiques relatives aux compartiments S3, voirthe section called "Donnez à l'origine l'autorisation de contrôle d'accès d'accéder au compartiment S3".

AWS WAF ACL Web

Si vous activez la distribution continue pour votre distribution, les considérations suivantes s'appliquent AWS WAF :

- Vous ne pouvez pas associer une liste de contrôle d'accès AWS WAF Web (ACL) à la distribution pour la première fois.
- Vous ne pouvez pas dissocier une ACL AWS WAF Web de la distribution.

Avant de pouvoir effectuer les tâches précédentes, vous devez supprimer la politique de déploiement continu pour votre distribution de production. Cela supprime également la distribution intermédiaire. Pour plus d'informations, consultez Utilisez des AWS WAF protections.

Cas où toutes les demandes sont CloudFront envoyées à la distribution principale

Dans certains cas, tels que les périodes de forte utilisation des ressources, toutes les demandes CloudFront peuvent être envoyées à la distribution principale, indépendamment de ce qui est spécifié dans la politique de déploiement continu.

CloudFront envoie toutes les demandes à la distribution principale pendant les heures de pointe, indépendamment de ce qui est spécifié dans la politique de déploiement continu. Le pic de trafic fait référence au trafic du CloudFront service, et non au trafic de votre distribution.

HTTP/3

Vous ne pouvez pas utiliser le déploiement continu avec une distribution qui prend en charge le protocole HTTP/3.

Utilisez différentes origines avec les CloudFront distributions

Lorsque vous créez une distribution, vous spécifiez l'origine à laquelle les demandes de fichiers sont CloudFront envoyées. Vous pouvez utiliser différents types d'origines avec CloudFront. Par exemple, vous pouvez utiliser un compartiment Amazon S3, un MediaStore conteneur, un MediaPackage canal, un Application Load Balancer ou une URL de AWS Lambda fonction.

Rubriques

- Utiliser un compartiment Amazon S3
- Utiliser un MediaStore conteneur ou un MediaPackage canal

- Utiliser un Application Load Balancer
- Utiliser l'URL d'une fonction Lambda
- Utiliser Amazon EC2 (ou une autre origine personnalisée)
- Utiliser des groupes CloudFront d'origine

Utiliser un compartiment Amazon S3

Les rubriques suivantes décrivent les différentes manières d'utiliser un compartiment Amazon S3 comme origine d'une CloudFront distribution.

Rubriques

- Utiliser un compartiment Amazon S3 standard
- Utiliser Amazon S3 Object Lambda
- Utiliser le point d'accès Amazon S3
- Utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web
- Ajouter CloudFront à un compartiment Amazon S3 existant
- Déplacer un compartiment Amazon S3 vers un autre Région AWS

Utiliser un compartiment Amazon S3 standard

Lorsque vous utilisez Amazon S3 comme origine pour votre distribution, vous placez les objets que vous CloudFront souhaitez livrer dans un compartiment Amazon S3. Vous pouvez utiliser n’importe quelle méthode prise en charge par Amazon S3 pour accéder à vos objets dans Amazon S3. Par exemple, vous pouvez utiliser la console ou l'API Amazon S3, ou un outil tiers. Vous pouvez créer une hiérarchie dans votre compartiment pour stocker les objets, comme vous le feriez avec tout autre compartiment Amazon S3 standard.

L'utilisation d'un compartiment Amazon S3 existant comme serveur CloudFront d'origine ne modifie en rien le compartiment ; vous pouvez toujours l'utiliser comme vous le feriez normalement pour stocker et accéder à des objets Amazon S3 au prix standard d'Amazon S3. Le stockage d’objets dans le compartiment fait l’objet de frais Amazon S3 réguliers. Pour plus d'informations sur les frais d'utilisation CloudFront, consultez Amazon CloudFront Pricing. Pour plus d'informations sur l'utilisation CloudFront avec un compartiment S3 existant, consultezthe section called “Ajouter CloudFront à un compartiment Amazon S3 existant”.

> **Important**
>
> Pour que votre bucket fonctionne CloudFront, le nom doit être conforme aux exigences de dénomination du DNS. Pour plus d'informations, consultez la section Bucket naming rules dans le Guide de l'utilisateur Amazon Simple Storage Service.

Lorsque vous spécifiez un compartiment Amazon S3 comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

bucket-name.s3.*region*.amazonaws.com

Lorsque vous spécifiez le nom du bucket dans ce format, vous pouvez utiliser les CloudFront fonctionnalités suivantes :

- Configurez CloudFront pour communiquer avec votre compartiment Amazon S3 à l'aide du protocole SSL/TLS. Pour plus d'informations, consultez the section called "Utilisez le protocole HTTPS avec CloudFront".
- Utilisez un contrôle d'accès à l'origine pour obliger les spectateurs à accéder à votre contenu à l'aide d' CloudFrontURL, et non à l'aide d'URL Amazon S3. Pour plus d'informations, consultez the section called "Restreindre l'accès à une origine Amazon Simple Storage Service".
- Mettez à jour le contenu de votre bucket en le soumettant POST et en faisant PUT des demandes à CloudFront. Pour plus d'informations, consultez the section called "Méthodes HTTP" dans la rubrique the section called "Comment CloudFront traite et transmet les demandes à votre Amazon S3 d'origine".

Ne spécifiez pas le compartiment à l'aide des formats suivants :

- Le type de chemin d'accès Amazon S3 : s3.amazonaws.com/*bucket-name*
- Le CNAME Amazon S3

Utiliser Amazon S3 Object Lambda

Quand vous créez un point d'accès Object Lambda, Amazon S3 génère automatiquement un alias unique pour votre point d'accès Object Lambda. Vous pouvez utiliser cet alias au lieu d'un nom de compartiment Amazon S3 comme origine pour votre CloudFront distribution.

Lorsque vous utilisez un alias de point d'accès Object Lambda comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

alias.s3.*region*.amazonaws.com

Pour plus d'informations sur la manière de rechercher l'*alias*, consultez Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3 dans le Guide de l'utilisateur Amazon S3.

> **Important**
>
> Lorsque vous utilisez un point d'accès Object Lambda comme origine pour CloudFront, vous devez utiliser le contrôle d'accès à l'origine.

Pour un exemple de cas d'utilisation, consultez Utiliser Amazon S3 Object Lambda avec Amazon pour adapter CloudFront le contenu aux utilisateurs finaux.

CloudFront traite l'origine d'un point d'accès Object Lambda de la même manière que l'origine d'un compartiment Amazon S3 standard.

Si vous utilisez Amazon S3 Object Lambda comme origine pour votre distribution, vous devez configurer les quatre autorisations suivantes.

Object Lambda Access Point

Pour ajouter des autorisations pour le point d'accès Object Lambda

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès Lambda d'objet.
3. Choisissez le point d'accès Object Lambda que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès Lambda d'objet.
6. Collez la politique suivante dans le champ Politique.

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

```
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3-object-lambda:Get*",
            "Resource": "arn:aws:s3-object-lambda:region:AWS-account-
ID:accesspoint/Object-Lambda-Access-Point-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudfront::AWS-account-
ID:distribution/CloudFront-distribution-ID"
                }
            }
        }
    ]
}
```

7. Sélectionnez Enregistrer les modifications.

Amazon S3 Access Point

Pour ajouter des autorisations pour le point d'accès Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès.
3. Choisissez le point d'accès Amazon S3 que vous souhaitez utiliser.
4. Choisissez l’onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès.
6. Collez la politique suivante dans le champ Politique.

```
{
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
```

```
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-
name",
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-name/
object/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "s3-object-lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

7. Choisissez Enregistrer.

Amazon S3 bucket

Pour ajouter des autorisations au compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Politique de compartiment.
6. Collez la politique suivante dans le champ Politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
```

```
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
}
```

7. Sélectionnez Enregistrer les modifications.

AWS Lambda function

Pour ajouter des autorisations à la fonction Lambda

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation, choisissez Fonctions.
3. Choisissez la AWS Lambda fonction que vous souhaitez utiliser.
4. Choisissez l'onglet Configuration, puis choisisssez Autorisations.
5. Choisissez Ajouter des autorisations dans la section Déclarations de stratégie basées sur les ressources.
6. Sélectionnez Compte AWS.
7. Entrez un nom pour ID de déclaration.
8. Entrez `cloudfront.amazonaws.com` pour Principal.
9. Choisissez `lambda:InvokeFunction` dans le menu déroulant Action.
10. Choisissez Enregistrer.

Utiliser le point d'accès Amazon S3

Lorsque vous utilisez un point d'accès S3, Amazon S3 génère automatiquement un alias unique pour vous. Vous pouvez utiliser cet alias au lieu d'un nom de compartiment Amazon S3 comme origine pour votre CloudFront distribution.

Lorsque vous utilisez un alias de point d'accès Amazon S3 comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

alias.s3.*region*.amazonaws.com

Pour plus d'informations sur la manière de les trouver*alias*, consultez la section Utilisation d'un alias de type bucket pour le point d'accès à votre compartiment S3 dans le guide de l'utilisateur Amazon S3.

> **Important**
>
> Lorsque vous utilisez un point d'accès Amazon S3 comme point d'origine pour CloudFront, vous devez utiliser le contrôle d'accès à l'origine.

CloudFront traite l'origine d'un point d'accès Amazon S3 de la même manière qu'une origine de compartiment Amazon S3 standard.

Si vous utilisez Amazon S3 Object Lambda comme origine pour votre distribution, vous devez configurer les deux autorisations suivantes.

Amazon S3 Access Point

Pour ajouter des autorisations pour le point d'accès Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès.
3. Choisissez le point d'accès Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès.
6. Collez la politique suivante dans le champ Politique.

```
{
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
```

```
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-
name",
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-name/
object/*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceArn": "arn:aws:cloudfront::AWS-
account-ID:distribution/CloudFront-distribution-ID"}
            }
        }
    ]
}
```

7. Choisissez Enregistrer.

Amazon S3 bucket

Pour ajouter des autorisations au compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Politique de compartiment.
6. Collez la politique suivante dans le champ Politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": [
```

```
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
}
```

7. Sélectionnez Enregistrer les modifications.

Utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web

Vous pouvez utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web comme origine personnalisée avecCloudFront. Lorsque vous configurez votre CloudFront distribution, pour l'origine, entrez le point de terminaison d'hébergement de site Web statique Amazon S3 pour votre compartiment. La valeur s'affiche dans la console Amazon S3, sur l'onglet Properties (Propriétés), dans le volet Static website hosting (Hébergement de site Web statique). Par exemple :

`http://bucket-name.s3-website-region.amazonaws.com`

Pour de plus amples informations sur la spécification de points de terminaison web statiques Amazon S3, veuillez consulter Points de terminaison de sites web dans le Guide de l'utilisateur Amazon Simple Storage Service.

Lorsque vous spécifiez le nom du compartiment dans ce format comme votre origine, vous pouvez utiliser les redirections Amazon S3 et les documents d'erreur personnalisés Amazon S3. Pour de plus amples informations, veuillez consulter Configuration d'un document d'erreur personnalisé et Configuration d'une redirection dans le guide de l'utilisateur d'Amazon Simple Storage Service. (fournit CloudFront également des pages d'erreur personnalisées. Pour plus d'informations, voirthe section called "Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques".)

L'utilisation d'un compartiment Amazon S3 comme serveur CloudFront d'origine ne modifie en rien le compartiment. Vous pouvez continuer de l'utiliser normalement et des frais Amazon S3 réguliers s'appliquent. Pour plus d'informations sur les frais d'utilisation CloudFront, consultez Amazon CloudFront Pricing.

> **Note**
>
> Si vous utilisez l' CloudFront API pour créer votre distribution avec un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous devez le configurer en utilisant`CustomOriginConfig`, même si le site Web est hébergé dans un compartiment Amazon S3. Pour plus d'informations sur la création de distributions à l'aide de l'CloudFront API, consultez CreateDistributionle Amazon CloudFront API Reference.

Ajouter CloudFront à un compartiment Amazon S3 existant

Si vous stockez vos objets dans un compartiment Amazon S3, vous pouvez soit demander aux utilisateurs d'obtenir vos objets directement auprès de S3, soit configurer CloudFront pour obtenir vos objets depuis S3, puis les distribuer à vos utilisateurs. L'utilisation CloudFront peut être plus rentable si vos utilisateurs accèdent fréquemment à vos objets car, en cas d'utilisation élevée, le prix du transfert de CloudFront données est inférieur à celui du transfert de données Amazon S3. De plus, les téléchargements sont plus rapides avec CloudFront Amazon S3 uniquement, car vos objets sont stockés plus près de vos utilisateurs.

> **Note**
>
> Si vous CloudFront souhaitez respecter les paramètres de partage de ressources entre origines d'Amazon S3, configurez CloudFront pour transmettre l'`Origin`en-tête à Amazon S3. Pour plus d’informations, consultez the section called “Contenu du cache basé sur les en-têtes des demandes”.

Si vous distribuez actuellement du contenu directement depuis votre compartiment Amazon S3 en utilisant votre propre nom de domaine (tel que exemple.com) au lieu du nom de domaine de votre compartiment Amazon S3 (tel que DOC-EXAMPLE-BUCKET. s3.us-west-2.amazonaws.com), vous pouvez l'ajouter CloudFront sans interruption en suivant la procédure suivante.

À ajouter CloudFront lorsque vous distribuez déjà votre contenu depuis Amazon S3

1. Créez une CloudFront distribution. Pour plus d’informations, consultez the section called “Créer une distribution”.

Lors de la création de la distribution, indiquez le nom de votre compartiment Amazon S3 comme serveur d'origine.

> **Important**
>
> Pour que votre bucket fonctionne CloudFront, le nom doit être conforme aux exigences de dénomination du DNS. Pour plus d'informations, consultez la section Bucket naming rules dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous utilisez un CNAME avec Amazon S3, indiquez aussi le CNAME de votre distribution.

2. Créez une page web test qui contient des liens vers des objets accessibles au public dans votre compartiment Amazon S3 et testez les liens. Pour ce test initial, utilisez le nom de CloudFront domaine de votre distribution dans les URL des objets, par exemple,`https://d111111abcdef8.cloudfront.net/images/image.jpg`.

   Pour plus d'informations sur le format des CloudFront URL, consultezthe section called "Personnaliser les URL des fichiers".

3. Si vous utilisez des CNAME Amazon S3, votre application emploie votre nom de domaine (comme par exemple example.com) pour référencer les objets de votre compartiment Amazon S3 au lieu d'employer le nom de votre compartiment (comme par exemple DOC-EXAMPLE-BUCKET.s3.amazonaws.com). Pour continuer à utiliser votre nom de domaine pour référencer des objets au lieu d'utiliser le nom de CloudFront domaine de votre distribution (par exemple, d111111abcdef8.cloudfront.net), vous devez mettre à jour vos paramètres auprès de votre fournisseur de services DNS.

   Pour que les CNAME Amazon S3 fonctionnent, votre prestataire de services DNS doit disposer d'un jeu d'enregistrements de ressources CNAME pour votre domaine qui achemine actuellement les requêtes pour le domaine vers votre compartiment Amazon S3. Si un utilisateur demande, par exemple, cet objet :

   `https://example.com/images/image.jpg`

   La requête est automatiquement réacheminée et l'utilisateur voit cet objet :

   `https://DOC-EXAMPLE-BUCKET.s3.amazonaws.com/images/image.jpg`

Pour acheminer les requêtes vers votre CloudFront distribution plutôt que vers votre compartiment Amazon S3, vous devez utiliser la méthode fournie par votre fournisseur de services DNS pour mettre à jour l'enregistrement de ressources CNAME défini pour votre domaine. Cet enregistrement CNAME mis à jour redirige les requêtes DNS de votre domaine vers le nom de CloudFront domaine de votre distribution. Pour plus d'informations, consultez la documentation fournie par votre prestataire de services DNS.

> **Note**
>
> Si vous utilisez Route 53 comme service DNS, vous pouvez utiliser un jeu d'enregistrements de ressources d'alias ou CNAME. Pour de plus amples informations sur la modification des jeux d'enregistrements de ressources, veuillez consulter Modification des enregistrements. Pour de plus amples informations sur les jeux d'enregistrements de ressources d'alias, veuillez consulter Choix entre des enregistrements avec ou sans alias. Les deux rubriques se trouvent dans le Manuel du développeur Amazon Route 53.

Pour plus d'informations sur l'utilisation de CNames avec CloudFront, consultezthe section called "Utiliser des URL personnalisées".

Après avoir mis à jour le jeu d'enregistrements de ressources CNAME, un délai maximum de 72 heures peut être nécessaire pour que la modification se propage dans tout le système DNS, mais cela se produit en général plus vite. Pendant ce temps, certaines demandes concernant votre contenu continueront d'être acheminées vers votre compartiment Amazon S3, tandis que d'autres le seront. CloudFront

Déplacer un compartiment Amazon S3 vers un autre Région AWS

Si vous utilisez Amazon S3 comme origine pour une CloudFront distribution et que vous déplacez le compartiment vers une autre distribution Région AWS, la mise à jour de ses enregistrements afin d'utiliser la nouvelle région CloudFront peut prendre jusqu'à une heure lorsque les deux conditions suivantes sont remplies :

- Vous utilisez une identité CloudFront d'accès d'origine (OAI) pour restreindre l'accès au compartiment.

- vous déplacez le compartiment vers une région Amazon S3 qui exige Signature version 4 pour l'authentification.

Lorsque vous utilisez OAI, CloudFront utilise la région (entre autres valeurs) pour calculer la signature utilisée pour demander des objets à votre compartiment. Pour en savoir plus sur les OAI, consultez the section called "Utiliser une identité d'accès d'origine (ancienne, non recommandée)". Pour une liste de ceux Régions AWS qui prennent en charge la version 2 de Signature, voir le processus de signature de la version 2 de Signature dans le Référence générale d'Amazon Web Services.

Pour forcer une mise à CloudFront jour plus rapide des enregistrements, vous pouvez mettre à jour votre CloudFront distribution, par exemple en mettant à jour le champ Description dans l'onglet Général de la CloudFront console. Lorsque vous mettez à jour une distribution, vérifie CloudFront immédiatement la région dans laquelle se trouve votre compartiment. La propagation du changement à tous les emplacements périphériques ne doit prendre que quelques minutes.

Utiliser un MediaStore conteneur ou un MediaPackage canal

Pour diffuser des vidéos en streaming CloudFront, vous pouvez configurer un compartiment Amazon S3 configuré en tant que MediaStore conteneur, ou créer un canal et des points de terminaison avec MediaPackage. Ensuite, vous créez et configurez une distribution CloudFront pour diffuser la vidéo.

Pour plus d'informations et step-by-step d'instructions, consultez les rubriques suivantes :

- the section called "Diffusez la vidéo en utilisant AWS Elemental MediaStore comme origine"
- the section called "Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage"

Utiliser un Application Load Balancer

Si votre origine est un ou plusieurs serveurs HTTP (S) (serveurs Web) hébergés sur une ou plusieurs instances Amazon EC2, vous pouvez utiliser un Application Load Balancer connecté à Internet pour distribuer le trafic aux instances. Un équilibreur de charge connecté à Internet possède un nom DNS pouvant être résolu publiquement et achemine les demandes des clients vers des cibles via Internet.

Pour plus d'informations sur l'utilisation d'un Application Load Balancer comme point de départ CloudFront, notamment sur la manière de s'assurer que les utilisateurs ne peuvent accéder à vos serveurs Web que par le biais de l'équilibreur de charge CloudFront et non en accédant directement à l'équilibreur de charge, consultez. the section called "Restreindre l'accès aux équilibreurs de charge des applications"

Utiliser l'URL d'une fonction Lambda

L'URL d'une fonction Lambda est un point de terminaison HTTPS dédié à une fonction Lambda. Vous pouvez utiliser l'URL d'une fonction Lambda pour créer une application Web sans serveur entièrement dans Lambda. Vous pouvez appeler l'application Web Lambda directement via l'URL de fonction, sans avoir besoin de l'intégrer à API Gateway ou à un Application Load Balancer.

Si vous créez une application Web sans serveur en utilisant des fonctions Lambda avec des URL de fonction, vous pouvez en CloudFront ajouter pour bénéficier des avantages suivants :

- Accélérer votre application en mettant en cache le contenu plus près des utilisateurs
- Utiliser un nom de domaine personnalisé pour votre application Web
- Acheminez différents chemins d'URL vers différentes fonctions Lambda à l'aide CloudFront de comportements de cache
- Bloquer des demandes spécifiques en utilisant des restrictions CloudFront géographiques ou AWS WAF (ou les deux)
- AWS WAF À utiliser CloudFront pour protéger votre application contre les robots malveillants, empêcher les exploits courants des applications et améliorer la protection contre les attaques DDoS

Pour utiliser l'URL d'une fonction Lambda comme origine d'une CloudFront distribution, spécifiez le nom de domaine complet de l'URL de la fonction Lambda comme domaine d'origine. Un nom de domaine d'URL de fonction Lambda utilise le format suivant :

`function-URL-ID``.lambda-url.`*`AWS-Region`*`.on.aws`

Lorsque vous utilisez l'URL d'une fonction Lambda comme origine d'une CloudFront distribution, l'URL de la fonction doit être accessible au public. Pour ce faire, utilisez l'une des options suivantes :

- Si vous utilisez le contrôle d'accès à l'origine (OAC), le `AuthType` paramètre de l'URL de la fonction Lambda doit utiliser `AWS_IAM` la valeur et autoriser l'autorisation dans une politique `lambda:InvokeFunctionUrl` basée sur les ressources. Pour plus d'informations sur l'utilisation des URL des fonctions Lambda pour OAC, consultez. Restreindre l'accès à l'origine de l'URL d'une AWS Lambda fonction
- Si vous n'utilisez pas OAC, vous pouvez définir le `AuthType` paramètre de l'URL de la fonction sur `NONE` et autoriser l'`lambda:InvokeFunctionUrl`autorisation dans une politique basée sur les ressources.

Vous pouvez également ajouter un en-tête d'origine personnalisé aux demandes CloudFront envoyées à l'origine et écrire un code de fonction pour renvoyer une réponse d'erreur si l'en-tête n'est pas présent dans la demande. Cela permet de s'assurer que les utilisateurs ne peuvent accéder à votre application Web que par le biais de l'URL de la fonction Lambda CloudFront, et non directement à l'aide de celle-ci.

Pour plus d'informations sur les URL de fonction Lambda, consultez les rubriques suivantes dans le Guide du développeur AWS Lambda :

- URL de fonctions Lambda : présentation de la fonctionnalité d'URL de fonction Lambda
- Appel d'URL de fonctions Lambda : inclut des détails sur les charges utiles de demande et de réponse à utiliser pour coder votre application Web sans serveur
- Modèle de sécurité et d'authentification pour les URL des fonctions Lambda : inclut des détails sur les types d'authentification Lambda

Utiliser Amazon EC2 (ou une autre origine personnalisée)

Une origine personnalisée est un serveur Web HTTP (S) dont le nom DNS peut être résolu publiquement et qui achemine les demandes des clients vers des cibles via Internet. Le serveur HTTP (S) peut être hébergé sur une instance Amazon EC2, par AWS exemple, ou ailleurs. Une origine Amazon S3 configurée comme point de terminaison d'un site web est également considérée comme une origine personnalisée. Pour plus d'informations, consultez the section called "Utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web".

Lorsque vous utilisez votre propre serveur HTTP comme origine personnalisée, vous spécifiez le nom DNS du serveur, ainsi que les ports HTTP et HTTPS et le protocole que vous souhaitez utiliser CloudFront pour récupérer des objets depuis votre origine.

La plupart des CloudFront fonctionnalités sont prises en charge lorsque vous utilisez une origine personnalisée, à l'exception du contenu privé. Bien que vous puissiez utiliser une URL signée pour distribuer du contenu à partir d'une origine personnalisée, CloudFront pour accéder à l'origine personnalisée, celle-ci doit rester accessible au public. Pour plus d'informations, consultez the section called "Restreindre le contenu avec des URL signées et des cookies signés".

Suivez ces instructions pour utiliser des instances Amazon EC2 et d'autres origines personnalisées avec. CloudFront

- Hébergez et diffusez le même contenu sur tous les serveurs qui diffusent du contenu de même CloudFront origine. Pour plus d'informations, consultez the section called "Paramètres d'origine" dans la rubrique the section called "Paramètres de distribution".
- Enregistrez les entrées `X-Amz-Cf-Id` d'en-tête sur tous les serveurs au cas où vous en auriez besoin AWS Support ou CloudFront pour utiliser cette valeur pour le débogage.
- Limitez-les demandes d'accès aux ports HTTP et HTTPS sur lesquels votre origine personnalisée écoute.
- Synchronisez les horloges de tous les serveurs de votre implémentation. Notez que le temps universel coordonné (UTC) est CloudFront utilisé pour les URL signées et les cookies signés, pour les journaux et les rapports. En outre, si vous surveillez CloudFront l'activité à l'aide de CloudWatch métriques, notez que l'UTC est CloudWatch également utilisé.
- Utilisez des serveurs redondants pour gérer les défaillances.
- Pour plus d'informations sur l'utilisation d'une origine personnalisée pour servir un contenu privé consultez the section called "Restreindre l'accès aux fichiers dont l'origine est personnalisée".
- Pour plus d'informations sur le comportement de demande et de réponse, ainsi que sur les codes d'état HTTP pris en charge, consultez Comportement des demandes et des réponses.

Si vous utilisez Amazon EC2 pour une origine personnalisée, nous vous recommandons de procéder comme suit :

- Utilisez un Amazon Machine Image qui installe automatiquement le logiciel d'un serveur web. Pour de plus amples informations, consultez la documentation Amazon EC2.
- Utilisez un équilibreur de charge Elastic Load Balancing pour gérer le trafic entre plusieurs instances Amazon EC2 et isoler votre application des modifications apportées aux instances Amazon EC2. Par exemple, si vous utilisez un équilibreur de charge, vous pouvez ajouter et supprimer les instances Amazon EC2 sans modifier votre application. Pour de plus amples informations, veuillez consulter la documentation relative à Elastic Load Balancing.
- Lorsque vous créez votre CloudFront distribution, spécifiez l'URL de l'équilibreur de charge pour le nom de domaine de votre serveur d'origine. Pour plus d'informations, consultez the section called "Créer une distribution".

Utiliser des groupes CloudFront d'origine

Vous pouvez spécifier un groupe d'origine pour votre CloudFront origine si, par exemple, vous souhaitez configurer le basculement d'origine pour les scénarios nécessitant une haute disponibilité.

Utilisez le basculement d'origine pour désigner une origine principale et une CloudFront deuxième origine qui passe CloudFront automatiquement à une origine lorsque l'origine principale renvoie des réponses d'échec spécifiques au code d'état HTTP.

Pour de plus amples informations, notamment les étapes de configuration d'un groupe d'origine, veuillez consulter the section called "Améliorez la disponibilité grâce au basculement d'origine".

Utilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames)

Lorsque vous créez une distribution, CloudFront fournissez un nom de domaine pour celle-ci, tel que d111111abcdef8.cloudfront.net. Au lieu d'utiliser le nom de domaine fourni, vous pouvez utiliser un autre nom de domaine (également appelé CNAME).

Pour savoir comment utiliser votre propre nom de domaine, tel que www.example.com, consultez les rubriques suivantes :

Rubriques

Exigences relatives à l'utilisation de noms de domaines alternatifs

Lorsque vous ajoutez un autre nom de domaine, tel que www.example.com, à une CloudFront distribution, les conditions suivantes sont requises :

Les noms de domaines alternatifs doivent être en minuscules

Tous les noms de domaines alternatifs (CNAME) doivent être en minuscules.

Les noms de domaines alternatifs doivent être couverts par un certificat SSL/TLS valide

Pour ajouter un autre nom de domaine (CNAME) à une CloudFront distribution, vous devez joindre à votre distribution un certificat SSL/TLS valide et fiable qui couvre le nom de domaine

alternatif. Cela garantit que seules les personnes ayant accès au certificat de votre domaine peuvent s'associer à CloudFront un CNAME lié à votre domaine.

Un certificat sécurisé est un certificat émis par AWS Certificate Manager (ACM) ou par une autre autorité de certification (CA) valide. Vous pouvez utiliser un certificat auto-signé pour valider un CNAME existant, mais pas pour un nouveau CNAME. CloudFront prend en charge les mêmes autorités de certification que Mozilla. Pour obtenir la liste actuelle, consultez la Liste des certificats de CA inclus dans Mozilla.

Pour vérifier un autre nom de domaine à l'aide du certificat que vous joignez, y compris les noms de domaine alternatifs contenant des caractères génériques, CloudFront vérifiez le nom alternatif du sujet (SAN) sur le certificat. Le nom de domaine alternatif que vous ajoutez doit être couvert par le SAN.

> **Note**
>
> Un seul certificat peut être associé à une CloudFront distribution à la fois.

Vous prouvez que vous êtes autorisé à ajouter un nom de domaine alternatif spécifique à votre distribution en effectuant l'une des actions suivantes :

- Attacher un certificat qui inclut le nom de domaine alternatif, comme product-name.example.com.
- Attachement d'un certificat qui inclut un caractère générique * au début d'un nom de domaine, afin de couvrir plusieurs sous-domaines avec un même certificat. Lorsque vous spécifiez un caractère générique, vous pouvez y ajouter plusieurs sous-domaines en tant que noms de domaine alternatifs. CloudFront

Les exemples suivants illustrent le fonctionnement de l'utilisation de caractères génériques dans les noms de domaine d'un certificat pour vous autoriser à ajouter des noms de domaine alternatifs spécifiques. CloudFront

- Vous souhaitez ajouter marketing.example.com en tant que nom de domaine alternatif. Vous répertoriez dans votre certificat le nom de domaine suivant : *.example.com. Lorsque vous attachez ce certificat à CloudFront, vous pouvez ajouter n'importe quel autre nom de domaine pour votre distribution qui remplace le caractère générique à ce niveau, y compris marketing.example.com. Vous pouvez également, par exemple, ajouter les noms de domaines alternatifs suivants :

- product.example.com
- api.example.com

Toutefois, vous ne pouvez pas ajouter des noms de domaines alternatifs qui sont à un niveau supérieur ou inférieur au caractère générique. Par exemple, vous ne pouvez pas ajouter les noms de domaines alternatifs example.com ou marketing.product.example.com.

- Vous souhaitez ajouter example.com en tant que nom de domaine alternatif. Pour ce faire, vous devez répertorier le nom de domaine example.com lui-même sur le certificat que vous attachez à votre distribution.
- Vous souhaitez ajouter marketing.product.example.com en tant que nom de domaine alternatif. Pour ce faire, vous pouvez répertorier *.product.example.com sur le certificat, ou répertorier marketing.product.example.com lui-même sur le certificat.

Autorisation de modifier la configuration DNS

Lorsque vous ajoutez des noms de domaine alternatifs, vous devez créer des enregistrements CNAME pour acheminer les requêtes DNS relatives aux noms de domaine alternatifs vers votre CloudFront distribution. Pour ce faire, vous devez être autorisé à créer des enregistrements CNAME auprès du fournisseur de services DNS pour les noms de domaines alternatifs que vous utilisez. Cela signifie normalement que les domaines vous appartiennent, mais vous pouvez développer une application pour le propriétaire du domaine.

Noms de domaines alternatifs et HTTPS

Si vous souhaitez que les utilisateurs emploient HTTPS avec un nom de domaine alternatif, une configuration supplémentaire est nécessaire. Pour plus d'informations, consultez Utiliser des noms de domaine alternatifs et le protocole HTTPS.

Restrictions relatives à l'utilisation de noms de domaines alternatifs

Veuillez noter les restrictions suivantes relatives à l'utilisation de noms de domaines alternatifs :

Nombre maximum de noms de domaines alternatifs

Pour connaître le nombre maximum actuel de noms de domaine alternatifs que vous pouvez ajouter à une distribution ou demander un quota plus élevé (auparavant appelé limite), veuillez consulter Quotas généraux sur les distributions.

Duplication et chevauchement de noms de domaines alternatifs

Vous ne pouvez pas ajouter un autre nom de domaine à une CloudFront distribution si le même nom de domaine alternatif existe déjà dans une autre CloudFront distribution, même si l'autre distribution appartient à votre AWS compte.

Néanmoins, vous pouvez ajouter un nom de domaine alternatif à caractère générique, comme *.example.com, qui comporte (ou qui chevauche) un nom de domaine alternatif sans caractère générique, tel que www.example.com. Si vous avez des noms de domaine alternatifs qui se chevauchent dans deux distributions, CloudFront envoie la demande à la distribution dont le nom correspond le plus précisément, quelle que soit la distribution vers laquelle pointe l'enregistrement DNS. Par exemple, marketing.domain.com est plus spécifique que *. domain.com.

Domain fronting

CloudFront inclut une protection contre le fronting de domaine sur différents AWS comptes. Le fronting de domaine est un scénario dans lequel un client non standard crée une connexion TLS/SSL vers un nom de domaine dans un AWS compte, puis effectue une requête HTTPS pour un nom non lié dans un autre compte. AWS Par exemple, la connexion TLS peut se connecter à www.example.com, puis envoyer une demande pour www.example.org.

Pour éviter les cas où le fronting de domaine croise différents AWS comptes, CloudFront assurez-vous que le AWS compte propriétaire du certificat qu'il sert pour une connexion spécifique correspond toujours au AWS compte propriétaire de la demande traitée sur cette même connexion.

Si les deux numéros de AWS compte ne correspondent pas, CloudFront répond par une réponse HTTP 421 Misdirected Request pour donner au client la possibilité de se connecter en utilisant le bon domaine.

Ajout d’un nom de domaine alternatif sur le nœud supérieur (zone apex) pour un domaine

Lorsque vous ajoutez un autre nom de domaine à une distribution, vous créez généralement un enregistrement CNAME dans votre configuration DNS pour acheminer les requêtes DNS relatives au nom de domaine vers votre CloudFront distribution. Cependant, il n’est pas possible de créer un enregistrement CNAME pour le nœud supérieur d’un espace de nom DNS, également appelé zone apex. Le protocole DNS ne le permet pas. Par exemple, si vous enregistrez le nom DNS example.com, la zone apex est example.com. Vous ne pouvez pas créer un enregistrement CNAME pour example.com, mais vous pouvez créer des enregistrements CNAME pour www.example.com, newproduct.example.com, etc.

Si vous utilisez Route 53 comme service DNS, vous pouvez créer un jeu d'enregistrements de ressources d'alias, qui présente deux avantages par rapport aux enregistrements CNAME. Vous pouvez créer un jeu d'enregistrements de ressources d'alias pour un nom de domaine sur le nœud supérieur (example.com). De plus, lorsque vous utilisez un jeu d'enregistrements de ressources d'alias, vous ne payez pas pour les requêtes Route 53.

> **Note**
>
> Si vous activez IPv6, vous devez créer deux jeux d'enregistrements de ressources d'alias : un pour acheminer le trafic IPv4 (un enregistrement A) et l'autre pour acheminer le trafic IPv6 (un enregistrement AAAA). Pour plus d'informations, consultez Activation d'IPv6 dans la rubrique Référence des paramètres de distribution.

Pour plus d'informations, consultez la section Acheminer le trafic vers une distribution CloudFront Web Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

Ajouter un autre nom de domaine

La liste de tâches suivante décrit comment utiliser la CloudFront console pour ajouter un autre nom de domaine à votre distribution afin que vous puissiez utiliser votre propre nom de domaine dans vos liens au lieu du nom de CloudFront domaine. Pour plus d'informations sur la mise à jour de votre distribution à l'aide de l' CloudFront API, consultezConfiguration des distributions.

> **Note**
>
> Si vous souhaitez que les utilisateurs emploient HTTPS avec votre nom de domaine alternatif, consultez Utiliser des noms de domaine alternatifs et le protocole HTTPS.

Avant de commencer : Assurez-vous d'effectuer les opérations suivantes avant de mettre à jour votre distribution pour ajouter un nom de domaine alternatif :

- Enregistrez le nom de domaine auprès de Route 53 ou d'un autre registre de domaine.
- Obtenez un certificat SSL/TLS auprès d'une autorité de certification (CA) autorisée qui couvre le nom de domaine. Ajoutez le certificat à votre distribution pour vous assurer que vous êtes autorisé à utiliser le domaine. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs.

Ajouter un autre nom de domaine

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l’ID de la distribution que vous souhaitez mettre à jour.
3. Sous l’onglet General, choisissez Edit.
4. Mettez à jour les valeurs suivantes :

   Noms de domaine alternatifs (CNAME)

   Ajoutez vos noms de domaines alternatifs. Séparez les noms de domaines par des virgules ou saisissez chaque nom de domaine sur une nouvelle ligne.

   Certificat SSL

   Choisissez le paramètre suivant :

   - Use HTTPS (Utiliser HTTPS) – Choisissez Custom SSL Certificate (Certificat SSL personnalisé) et choisissez un certificat dans la liste. La liste inclut les certificats fournis par AWS Certificate Manager (ACM), les certificats que vous avez achetés auprès d'une autre autorité de certification et téléchargés vers ACM, ainsi que les certificats que vous avez achetés auprès d'une autre autorité de certification et téléchargés vers le magasin de certificats IAM.

     Si vous avez chargé un certificat dans le magasin de certificats IAM mais qu’il n’apparaît pas dans la liste, consultez la procédure Importer un certificat SSL/TLS afin de vérifier si vous avez correctement chargé le certificat.

     Si vous choisissez cette valeur, il est recommandé de n’utiliser qu’un nom de domaine alternatif dans vos URL d’objets (https://www.example.com/logo.jpg). Si vous utilisez votre nom de domaine de CloudFront distribution (https://d111111abcdef8.cloudfront.net.cloudfront.net/logo.jpg), un lecteur peut se comporter comme suit, en fonction de la valeur que vous avez choisie pour Clients Supported :

     - Tous les clients : si le lecteur ne prend pas en charge le SNI, il affiche un avertissement car le nom de CloudFront domaine ne correspond pas au nom de domaine de votre certificat TLS/SSL.
     - Uniquement les clients qui supportent l'indication du nom du serveur (SNI) : CloudFront abandonne la connexion avec le visualiseur sans renvoyer l'objet.

Clients pris en charge

Choisir une option :

- Tous les clients : CloudFront diffuse votre contenu HTTPS à l'aide d'adresses IP dédiées. Si vous sélectionnez cette option, des frais supplémentaires s'appliqueront lors de l'association de votre certificat SSL/TLS à une distribution activée. Pour en savoir plus, consultez Tarification Amazon CloudFront.
- Seuls les clients qui prennent en charge Server Name Indication (SNI) (recommandé) : les navigateurs plus anciens ou les autres clients qui ne prennent pas en charge l'extension SNI doivent utiliser une autre méthode pour accéder à votre contenu.

Pour plus d'informations, consultez Choisissez le mode de CloudFront traitement des requêtes HTTPS.

5. Choisissez Oui, Modifier.
6. Sous l'onglet Questions d'ordre général de la distribution, vérifiez que la valeur du champ Statut de distribution a été remplacée par Déployé. Si vous essayez d'utiliser un autre nom de domaine avant le déploiement des mises à jour de votre distribution, les liens que vous allez créer lors des étapes suivantes risquent de ne pas fonctionner.
7. Configurez le service DNS pour le nom de domaine alternatif (tel que www.example.com) afin d'acheminer le trafic vers le nom de CloudFront domaine de votre distribution (par exemple d111111abcdef8.cloudfront.net). La méthode utilisée varie selon que vous utilisiez ou non Route 53 comme fournisseur de services DNS pour le domaine.

> **Note**
>
> Si votre enregistrement DNS pointe déjà vers une distribution qui n'est pas celle que vous mettez à jour, alors vous ajoutez uniquement le nom de domaine alternatif à votre distribution après avoir mis à jour votre DNS. Pour plus d'informations, consultez Restrictions relatives à l'utilisation de noms de domaines alternatifs.

Route 53

Créez un jeu d'enregistrements de ressources d'alias. Avec un jeu d'enregistrements de ressources d'alias, vous ne payez pas pour les requêtes Route 53. De plus, vous pouvez créer un jeu d'enregistrements de ressources d'alias pour le nom de domaine racine (example.com), ce que DNS n'autorise pas pour les CNAME. Pour plus d'informations,

consultez la section Acheminer le trafic vers une distribution CloudFront Web Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

Autre fournisseur de services DNS

Utilisez la méthode fournie par votre fournisseur de services DNS pour ajouter un enregistrement CNAME à votre domaine. Ce nouvel enregistrement CNAME redirigera les requêtes DNS de votre nom de domaine alternatif (par exemple, www.exemple.com) vers le nom de CloudFront domaine de votre distribution (par exemple, d111111abcdef8.cloudfront.net). Pour plus d'informations, consultez la documentation fournie par votre prestataire de services DNS.

> **Important**
>
> Si vous possédez déjà un enregistrement CNAME pour votre autre nom de domaine, mettez-le à jour ou remplacez-le par un nouveau qui pointe vers le nom de CloudFront domaine de votre distribution.

8. Utilisez `dig` ou un outil DNS similaire pour vérifier que la configuration DNS créée à l'étape précédente pointe bien vers le nom de domaine de votre distribution.

   L'exemple suivant illustre une requête `dig` sur le domaine images.example.com ainsi que la partie pertinente de la réponse.

```
PROMPT> dig www.example.com

; <<> DiG 9.3.3rc2 <<> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15917
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.     IN    A

;; ANSWER SECTION:
www.example.com. 10800 IN CNAME d111111abcdef8.cloudfront.net.
...
```

   La section des réponses affiche un enregistrement CNAME qui achemine les requêtes pour www.example.com vers le nom de domaine de CloudFront distribution

d111111abcdef8.cloudfront.net. Si le nom sur le côté droit de CNAME est le nom de domaine de votre CloudFront distribution, l'enregistrement CNAME est correctement configuré. Si cette valeur est différente (s'il s'agit, par exemple, du nom de domaine de votre compartiment Amazon S3), l'enregistrement CNAME n'est pas configuré correctement. Vous devez alors retourner à l'étape 7 et corriger l'enregistrement CNAME pour qu'il pointe vers le nom de domaine de votre distribution.

9. Testez le nom de domaine alternatif en accédant aux URL contenant votre nom de domaine au lieu du nom de CloudFront domaine de votre distribution.
10. Dans votre application, modifiez les URL de vos objets afin d'utiliser votre nom de domaine alternatif au lieu du nom de domaine de votre CloudFront distribution.

Déplacer un autre nom de domaine vers une autre distribution

Lorsque vous essayez d'ajouter un nom de domaine alternatif à une distribution mais que ce nom alternatif est déjà utilisé sur une autre distribution, vous recevez une erreur `CNAMEAlreadyExists` (Un ou plusieurs des CNAME que vous avez fournis sont déjà associés à une autre ressource). Par exemple, vous recevez cette erreur lorsque vous tentez d'ajouter www.example.com à une distribution, mais que www.example.com est déjà associé à une autre distribution.

Dans ce cas, vous pouvez déplacer le nom de domaine alternatif existant d'une distribution (distribution source) vers une autre (distribution cible). Les étapes suivantes offrent un présentation du processus. Pour plus d'informations, suivez le lien à chaque étape de la présentation.

Pour déplacer un nom de domaine alternatif

1. Configurez la distribution cible. Cette distribution doit être accompagnée d'un certificat SSL/TLS qui couvre le nom de domaine alternatif que vous déplacez. Pour plus d'informations, consultez Configurer la distribution cible.
2. Recherchez la distribution source. Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour rechercher la distribution à laquelle le nom de domaine alternatif est associé. Pour plus d'informations, consultez Trouver la distribution source.
3. Déplacez le nom de domaine alternatif. La manière de procéder dépend du fait que les distributions source et cible se trouvent dans le même AWS compte. Pour plus d'informations, consultez the section called "Déplacer le nom de domaine alternatif".

Configurer la distribution cible

Avant de déplacer un nom de domaine alternatif, vous devez configurer la distribution cible (à savoir la distribution vers laquelle vous déplacez le nom de domaine alternatif).

Pour configurer la distribution cible

1. Obtenez un certificat SSL/TLS qui inclut le nom de domaine alternatif que vous déplacez. À défaut, vous pouvez en faire la demande à AWS Certificate Manager (ACM) ou en obtenir un auprès d'une autre autorité de certification (CA) et l'importer dans ACM. Assurez-vous que vous demandez ou importez le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).
2. Si vous n'avez pas encore créé la distribution cible, faites-le dès à présent. Dans le cadre de la création de la distribution cible, associez votre certificat (obtenu à l'étape précédente) à la distribution. Pour plus d'informations, consultez Créer une distribution.

   Si vous disposez déjà d'une distribution cible, associez votre certificat (de l'étape précédente) à cete distribution cible. Pour plus d'informations, consultez Mettre à jour une distribution.
3. Créez un enregistrement TXT DNS qui associe le nom de domaine alternatif au nom de domaine de distribution de la distribution cible. Créez l'enregistrement TXT avec un trait de soulignement (_) devant le nom de domaine alternatif. Voici un exemple d'enregistrement TXT dans DNS :

   ```
   _www.example.com TXT d111111abcdef8.cloudfront.net
   ```

   CloudFront utilise cet enregistrement TXT pour valider que vous êtes propriétaire du nom de domaine alternatif.

Trouver la distribution source

Avant de déplacer un nom de domaine alternatif d'une distribution à une autre, vous devez trouver la distribution source (distribution dans laquelle le nom de domaine alternatif est actuellement utilisé). Lorsque vous connaissez l'ID de compte AWS des distributions source et cible, vous pouvez déterminer le mode de déplacement du nom de domaine alternatif.

Pour rechercher la distribution source pour le nom de domaine alternatif

1. Utilisez la CloudFront list-conflicting-aliasescommande dans le AWS Command Line Interface (AWS CLI) comme indiqué dans l'exemple suivant. Remplacez *`www.example.com`* par le nom de domaine alternatif et *`EDFDVBD6EXAMPLE`* par l'ID de la distribution cible que vous avez précédemment configurée. Exécutez cette commande à l'aide des informations d'identification

enregistrées dans le même AWS compte que celui de la distribution cible. Pour utiliser cette commande, vous devez disposer des autorisations `cloudfront:GetDistribution` et `cloudfront:ListConflictingAlias` sur la distribution cible.

```
aws cloudfront list-conflicting-aliases --alias www.example.com --distribution-
id EDFDVBD6EXAMPLE
```

La sortie de la commande affiche la liste de tous les noms de domaines alternatifs présentant un conflit ou un chevauchement avec le nom fourni. Exemples :

- Si vous fournissez www.example.com à la commande, la sortie de cette dernière inclut www.example.com et le nom de domaine alternatif (*.example.com) avec chevauchement du caractère générique, s'il existe.
- Si vous fournissez *.example.com à la commande, la sortie de cette dernière inclut *.example.com et tout autre nom de domaine alternatif couvert par ce caractère générique (par exemple, www.example.com, test.example.com, dev.example.com, etc.).

Pour chaque autre nom de domaine alternatif dans la sortie de la commande, vous pouvez voir l'ID de la distribution à laquelle il est associé, ainsi que l'ID du compte AWS propriétaire de cette distribution. Les ID de distribution et de compte sont partiellement masqués, ce qui vous permet d'identifier les distributions et comptes que vous possédez, tout en protégeant les informations des distributions et comptes dont vous n'êtes pas propriétaire.

2. Dans le résultat de la commande, recherchez la distribution du nom de domaine alternatif que vous déplacez et notez l'ID de AWS compte de la distribution source. Comparez l'ID de compte de la distribution source avec l'ID du compte sur lequel vous avez créé la distribution cible, et déterminez si ces deux distributions se trouvent dans le même AWS compte. Vous pouvez ainsi déterminer le mode de déplacement du nom de domaine alternatif.

   Pour déplacer le nom de domaine alternatif, reportez-vous à la rubrique suivante.

Déplacer le nom de domaine alternatif

Selon le cas, choisissez parmi les méthodes suivantes pour déplacer le nom de domaine alternatif :

Si les distributions source et cible se trouvent dans la même compte AWS

Utilisez la associate-alias commande du AWS CLI pour déplacer le nom de domaine alternatif. Cette méthode fonctionne pour tous les déplacements de mêmes comptes, y compris lorsque le nom de domaine alternatif correspond à un domaine apex (également appelé domaine racine, comme exemple.com). Pour plus d'informations, consultez the section called "`associate-alias`À utiliser pour déplacer un autre nom de domaine".

Si les distributions source et cible se trouvent dans des comptes AWS différents

Si vous avez accès à la distribution source, le nom de domaine alternatif ne correspond pas à un domaine apex (également appelé domaine racine, comme `example.com`), et que vous n'utilisez pas de caractère générique qui chevauche ce nom de domaine alternatif, utilisez un caractère générique pour déplacer le nom de domaine alternatif. Pour plus d'informations, consultez the section called "Utilisation d'un caractère générique pour déplacer un nom de domaine alternatif".

Si vous n'avez pas accès au AWS compte de la distribution source, vous pouvez essayer d'utiliser la associate-alias commande dans le AWS CLI pour déplacer le nom de domaine alternatif. Si la distribution source est désactivée, vous pouvez déplacer le nom de domaine alternatif. Pour plus d'informations, consultez the section called "`associate-alias`À utiliser pour déplacer un autre nom de domaine". Si la commande associate-alias ne fonctionne pas, contactez AWS Support. Pour plus d'informations, consultez the section called "Contacter AWS Support pour déplacer un autre nom de domaine".

`associate-alias`À utiliser pour déplacer un autre nom de domaine

Si la distribution source se trouve dans le même AWS compte que la distribution cible, ou si elle se trouve dans un autre compte mais qu'elle est désactivée, vous pouvez utiliser la CloudFront associate-aliascommande du AWS CLI pour déplacer le nom de domaine alternatif.

Pour utiliser un alias associé pour déplacer un nom de domaine alternatif

1. Utilisez le AWS CLI pour exécuter la CloudFront associate-alias commande, comme indiqué dans l'exemple suivant. Remplacez *`www.exemple.com`* par le nom de domaine alternatif et *`EDFDVBD6EXAMPLE`* par l'ID de la distribution cible. Exécutez cette commande à l'aide des informations d'identification enregistrées dans le même AWS compte que celui de la distribution cible. Notez les restrictions suivantes liées à l'utilisation de cette commande :

   - Vous devez disposer des autorisations `cloudfront:AssociateAlias` et `cloudfront:UpdateDistribution` sur la distribution cible.

- Si les distributions source et cible se trouvent dans la même compte AWS , vous devez disposer de l'autorisation `cloudfront:UpdateDistribution` sur la distribution source.
- Si les distributions source et cible se trouvent dans des comptes AWS différents, la distribution source doit être désactivée.
- La distribution cible doit être configurée comme décrit dans the section called "Configurer la distribution cible".

```
aws cloudfront associate-alias --alias www.example.com --target-distribution-
id EDFDVBD6EXAMPLE
```

Cette commande met à jour les deux distributions en supprimant le nom de domaine alternatif de la distribution source et en l'ajoutant à la distribution cible.

2. Une fois la distribution cible entièrement déployée, mettez à jour votre configuration DNS afin de pointer l'enregistrement DNS du nom de domaine alternatif vers le nom de domaine de distribution de la distribution cible.

Utilisation d'un caractère générique pour déplacer un nom de domaine alternatif

Si la distribution source se trouve dans un AWS compte différent de celui de la distribution cible et que la distribution source est activée, vous pouvez utiliser un caractère générique pour déplacer le nom de domaine secondaire.

> **Note**
>
> Vous pouvez utiliser un caractère générique pour déplacer un domaine apex (comme example.com). Pour déplacer un domaine apex lorsque les distributions source et cible se trouvent dans des comptes AWS différents, contactez AWS Support. Pour plus d'informations, consultez the section called "Contacter AWS Support pour déplacer un autre nom de domaine".

Pour utiliser un caractère générique pour déplacer un nom de domaine alternatif

> **Note**
>
> Ce processus implique plusieurs mises à jour de vos distributions. Attendez que chaque distribution déploie entièrement la dernière modification avant de passer à l'étape suivante.

1. Mettez à jour la distribution cible pour ajouter un nom de domaine alternatif couvrant le nom de domaine alternatif que vous déplacez. Si le nom de domaine alternatif que vous déplacez correspond à www.example.com, ajoutez le nom de domaine alternatif *.example.com à la distribution cible. Pour ce faire, le certificat SSL/TLS de la distribution cible doit inclure le nom de domaine avec caractère générique. Pour plus d'informations, consultez the section called "Mettre à jour une distribution".
2. Mettez à jour les paramètres DNS du nom de domaine alternatif de manière à ce qu'il pointe vers le nom de domaine de la distribution cible. Par exemple, si le nom de domaine alternatif que vous déplacez correspond à www.example.com, mettez à jour l'enregistrement DNS correspondant à www.example.com de manière à acheminer le trafic vers le nom de domaine de la distribution cible (par exemple d111111abcdef8.cloudfront.net).

   > **Note**
   >
   > Même une fois les paramètres DNS mis à jour, le nom de domaine alternatif est toujours servi par la distribution source puisque c'est là que le nom de domaine alternatif est actuellement configuré.

3. Mettez à jour la distribution source pour supprimer le nom de domaine de remplacement. Pour plus d'informations, consultez Mettre à jour une distribution.
4. Mettez à jour la distribution cible pour ajouter le nom de domaine alternatif. Pour plus d'informations, consultez Mettre à jour une distribution.
5. Utilisez dig (ou un outil de requête DNS similaire) pour vérifier que l'enregistrement DNS du le nom de domaine alternatif est résolu avec le nom de domaine de la distribution cible.
6. (Facultatif) Mettez à jour la distribution cible pour supprimer le nom de domaine alternatif avec caractère générique.

Contacter AWS Support pour déplacer un autre nom de domaine

Si les distributions source et cible se trouvent dans AWS des comptes différents et que vous n'avez pas accès au AWS compte de la distribution source ou que vous ne pouvez pas désactiver la distribution source, vous pouvez contacter AWS Support pour déplacer le nom de domaine alternatif.

À contacter AWS Support pour déplacer un autre nom de domaine

1. Configurez une distribution cible, y compris l'enregistrement TXT DNS qui pointe vers la distribution cible. Pour plus d'informations, consultez Configurer la distribution cible.
2. Contactez-nous AWS Support pour leur demander de vérifier que vous êtes bien le propriétaire du domaine et de le déplacer vers la nouvelle CloudFront distribution pour vous.
3. Une fois la distribution cible entièrement déployée, mettez à jour votre configuration DNS afin de pointer l'enregistrement DNS du nom de domaine alternatif vers le nom de domaine de distribution de la distribution cible.

Supprimer un autre nom de domaine

Si vous souhaitez arrêter le routage du trafic d'un domaine ou d'un sous-domaine vers une CloudFront distribution, suivez les étapes décrites dans cette section pour mettre à jour à la fois la configuration DNS et la CloudFront distribution.

Il est important que vous supprimiez les noms de domaine alternatifs de la distribution et que vous mettiez à jour votre configuration DNS. Cela permet d'éviter des problèmes ultérieurs si vous souhaitez associer le nom de domaine à une autre CloudFront distribution. Si un nom de domaine alternatif est déjà associé à une distribution, il ne peut pas être configuré avec une autre.

> **Note**
>
> Si vous souhaitez supprimer le nom de domaine alternatif de cette distribution afin de pouvoir l'ajouter à une autre, suivez les étapes indiquées dans Déplacer un autre nom de domaine vers une autre distribution. Si vous suivez plutôt les étapes décrites ici (pour supprimer un domaine) puis que vous ajoutez le domaine à une autre distribution, il y aura une période pendant laquelle le domaine ne sera pas lié à la nouvelle distribution car il CloudFront se propage aux mises à jour vers les emplacements périphériques.

Pour supprimer un autre nom de domaine d'une distribution

1. Pour commencer, acheminez le trafic Internet de votre domaine vers une autre ressource qui n'est pas votre CloudFront distribution, comme un équilibreur de charge Elastic Load Balancing. Vous pouvez également supprimer l'enregistrement DNS vers lequel le trafic est acheminé CloudFront.

   Effectuez l'une des opérations suivantes, en fonction du service DNS pour votre domaine :

   - Si vous utilisez Route 53, mettez à jour ou supprimez les enregistrements d'alias ou les enregistrements CNAME. Pour de plus amples informations, veuillez consulter Modification des enregistrements ou Suppression des enregistrements.
   - Si vous utilisez un autre fournisseur de services DNS, utilisez la méthode fournie par celui-ci pour mettre à jour ou supprimer l'enregistrement CNAME vers CloudFront lequel le trafic est dirigé. Pour plus d'informations, consultez la documentation fournie par votre prestataire de services DNS.
2. Après avoir mis à jour les enregistrements DNS de votre domaine, attendez que les modifications se soient propagées et que les résolveurs DNS acheminent le trafic vers la nouvelle ressource. Vous pouvez vérifier si cette opération est terminée en créant des liens de test utilisant votre domaine dans l'URL.
3. Connectez-vous au AWS Management Console et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home, puis mettez à jour votre CloudFront distribution pour supprimer le nom de domaine en procédant comme suit :

   a. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
   b. Sous l'onglet General, choisissez Edit.
   c. Dans Autres noms de domaine (CNAME), supprimez le nom de domaine alternatif (ou les noms de domaine) que vous ne souhaitez plus utiliser pour votre distribution.
   d. Choisissez Oui, Modifier.

Utiliser des caractères génériques dans les noms de domaine alternatifs

Lorsque vous ajoutez des noms de domaine alternatifs, vous pouvez utiliser le caractère générique * au début d'un nom de domaine au lieu d'ajouter individuellement les sous-domaines. Par exemple, avec comme nom de domaine alternatif *.example.com, vous pouvez par exemple utiliser n'importe quel nom de domaine qui se termine par example.com dans vos URL, comme www.example.com,

product-name.example.com, marketing.product-name.example.com, etc. Le chemin vers l'objet est identique, quel que soit le nom de domaine, par exemple :

- www.example.com/images/image.jpg
- product-name.example.com/images/image.jpg
- marketing.product-name.example.com/images/image.jpg

Suivez ces exigences pour les noms de domaine alternatifs qui incluent des caractères génériques :

- Le nom de domaine alternatif doit commencer par un astérisque et un point (*.).
- Vous ne pouvez pas utiliser un caractère générique pour remplacer une partie d'un nom de sous-domaine, comme cela : *domain.example.com.
- Vous ne pouvez pas remplacer un sous-domaine au milieu d'un nom de domaine, comme cela : subdomain.*.example.com.
- Tous les noms de domaines alternatifs, y compris les noms de domaines alternatifs qui utilisent des caractères génériques, doivent être couverts par le nom SAN (Subject Alternative Name) sur le certificat.

Un nom de domaine alternatif avec caractère générique, comme *.example.com, peut comporter un autre nom de domaine en cours d'utilisation, comme example.com.

Utilisation WebSockets avec les CloudFront distributions

Amazon CloudFront prend en charge l'utilisation WebSocket d'un protocole TCP utile lorsque vous avez besoin de connexions bidirectionnelles de longue durée entre les clients et les serveurs. Une connexion persistante est souvent une exigence avec des applications en temps réel. Les scénarios que vous pouvez utiliser WebSockets incluent les plateformes de chat social, les espaces de travail collaboratifs en ligne, les jeux multijoueurs et les services fournissant des flux de données en temps réel, tels que les plateformes de trading financier. Les données via une WebSocket connexion peuvent circuler dans les deux sens pour une communication en duplex intégral.

WebSocket la fonctionnalité est automatiquement activée pour fonctionner avec n'importe quelle distribution. Pour l'utiliser WebSockets, configurez l'une des options suivantes dans le comportement du cache associé à votre distribution :

- Transférez tous les en-têtes des demandes des visiteurs vers votre source. (Vous pouvez utiliser la politique de AllViewer gestion des demandes d'origine.)
- Transférez spécifiquement les en-têtes de `Sec-WebSocket-Version` demande `Sec-WebSocket-Key` et dans votre politique de demande d'origine.

Comment fonctionne le WebSocket protocole

Le WebSocket protocole est un protocole TCP indépendant qui vous permet d'éviter une partie de la surcharge (voire une latence accrue) du protocole HTTP.

Pour établir une WebSocket connexion, le client envoie une requête HTTP normale qui utilise la sémantique de mise à niveau du protocole HTTP pour modifier le protocole. Le serveur peut ensuite terminer la liaison. La WebSocket connexion reste ouverte et le client ou le serveur peuvent s'envoyer des trames de données sans avoir à établir de nouvelles connexions à chaque fois.

Par défaut, le WebSocket protocole utilise le port 80 pour les WebSocket connexions régulières et le port 443 pour les WebSocket connexions via TLS/SSL. Les options que vous choisissez pour votre CloudFront Viewer Protocol Policy et que vous Protocole (origines personnalisées uniquement) appliquez aux WebSocket connexions ainsi qu'au trafic HTTP.

WebSocketexigences

WebSocket les demandes doivent être conformes à la RFC 6455 dans les formats standard suivants.

Exemple de requête du client :

```
GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHNhbXBsZSBub25jZQ==
Origin: https://example.com
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13
```

Exemple de réponse du serveur :

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
```

```
Connection: Upgrade
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+xOo=
Sec-WebSocket-Protocol: chat
```

Si la WebSocket connexion est déconnectée par le client ou le serveur, ou en raison d'une interruption du réseau, les applications clientes sont censées rétablir la connexion avec le serveur.

WebSocket En-têtes recommandés

Afin d'éviter des problèmes inattendus liés à la compression lors de l'utilisation WebSockets, nous vous recommandons d'inclure les en-têtes suivants dans une politique de demande d'origine :

- `Sec-WebSocket-Key`
- `Sec-WebSocket-Version`
- `Sec-WebSocket-Protocol`
- `Sec-WebSocket-Accept`
- `Sec-WebSocket-Extensions`

Mise en cache et disponibilité

Vous pouvez l'utiliser CloudFront pour réduire le nombre de demandes auxquelles votre serveur d'origine doit répondre directement. Grâce à CloudFront la mise en cache, un plus grand nombre d'objets sont servis depuis des emplacements CloudFront périphériques, plus proches de vos utilisateurs. Cela réduit la charge sur votre serveur d'origine et la latence.

Plus le nombre de demandes CloudFront pouvant être traitées à partir des caches périphériques est élevé, moins il y a de demandes des utilisateurs qui CloudFront doivent être transmises à votre source pour obtenir la dernière version ou une version unique d'un objet. Pour optimiser votre CloudFront système afin d'envoyer le moins de demandes possible à votre origine, pensez à utiliser un CloudFront Origin Shield. Pour plus d’informations, consultez Utilisation d'Amazon CloudFront Origin Shield.

La proportion de demandes traitées directement depuis le CloudFront cache par rapport à l'ensemble des demandes est appelée taux de réussite du cache. Vous pouvez consulter le pourcentage de demandes des utilisateurs qui sont des réponses positives, manquées ou erronées dans la CloudFront console. Pour plus d’informations, consultez Afficher les rapports statistiques du CloudFront cache.

Un certain nombre de facteurs influencent le taux d'accès au cache. Vous pouvez ajuster CloudFront la configuration de votre distribution pour améliorer le taux de réussite du cache en suivant les instructions fournies dansAugmenter la proportion de demandes traitées directement à partir des CloudFront caches (taux de réussite du cache).

Pour en savoir plus sur l'ajout et la suppression du contenu que vous CloudFront souhaitez diffuser, consultezAjouter, supprimer ou remplacer du contenu CloudFront diffusé.

Rubriques

Augmenter la proportion de demandes traitées directement à partir des CloudFront caches (taux de réussite du cache)

Vous pouvez améliorer les performances en augmentant la proportion de demandes de vos visiteurs qui sont traitées directement depuis le CloudFront cache au lieu d'être transmises à vos serveurs d'origine pour le contenu. Ce processus est appelé « amélioration du taux d'accès au cache ».

Les sections suivantes expliquent comment améliorer votre taux d'accès au cache.

Rubriques

Spécifiez la durée de mise CloudFront en cache de vos objets

Pour augmenter votre taux d'accès au cache, vous pouvez configurer votre origine de sorte qu'une directive Cache-Control max-age soit ajoutée à vos objets et spécifier la valeur pratique la plus longue pour `max-age`. Plus la durée du cache est courte, plus il CloudFront envoie fréquemment des demandes à votre origine pour déterminer si un objet a changé et pour obtenir la dernière version. Vous pouvez compléter `max-age` avec les directives `stale-while-revalidate` et `stale-if-error` pour améliorer davantage le taux d'accès au cache sous certaines conditions. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Utiliser Origin Shield

CloudFront Origin Shield peut contribuer à améliorer le taux de réussite du cache de votre CloudFront distribution, car il fournit une couche de mise en cache supplémentaire devant votre source d'origine. Lorsque vous utilisez Origin Shield, toutes les demandes de toutes les couches CloudFront de mise en cache envoyées à votre origine proviennent d'un seul endroit. CloudFront peut récupérer chaque objet à l'aide d'une seule demande d'origine provenant d'Origin Shield, et toutes les autres couches

du CloudFront cache (emplacements périphériques et caches périphériques régionaux) peuvent récupérer l'objet depuis Origin Shield.

Pour plus d'informations, consultez Utilisation d'Amazon CloudFront Origin Shield.

Mise en cache basée sur les paramètres de chaîne de requête

Si vous configurez CloudFront la mise en cache en fonction des paramètres de chaîne de requête, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour transmettre uniquement les paramètres de chaîne de requête pour lesquels votre origine renverra des objets uniques.
- Utilisez la même casse (majuscules ou minuscules) pour toutes les instances du même paramètre. Par exemple, si une demande contient `parameter1=A` et qu'une autre contient`parameter1=a`, CloudFront transfère des demandes distinctes à votre origine lorsqu'une demande contient `parameter1=A` et lorsqu'une demande contient`parameter1=a`. CloudFront met ensuite en cache séparément les objets correspondants renvoyés par votre origine séparément, même s'ils sont identiques. Si vous utilisez just `A` ora, CloudFront vous transférez moins de demandes à votre source.
- Listez les paramètres dans le même ordre. Comme dans le cas des différences de cas, si une demande pour un objet contient la chaîne de requête `parameter1=a&parameter2=b` et qu'une autre demande pour le même objet contient`parameter2=b&parameter1=a`, CloudFront transmet les deux demandes à votre origine et met en cache séparément les objets correspondants, même s'ils sont identiques. Si vous utilisez toujours le même ordre pour les paramètres, CloudFront vous transférez moins de demandes à votre source.

Pour plus d'informations, consultez Contenu du cache basé sur les paramètres de chaîne de requête. Si vous souhaitez consulter les chaînes de requête qui CloudFront sont transmises à votre origine, consultez les valeurs dans la `cs-uri-query` colonne de vos fichiers CloudFront journaux. Pour plus d'informations, consultez Configuration et utilisation des journaux standard (journaux d'accès).

Mise en cache basée sur des valeurs de cookie

Si vous configurez CloudFront la mise en cache en fonction des valeurs des cookies, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour transférer uniquement les cookies spécifiés au lieu de transférer tous les cookies. Pour les cookies que vous configurez CloudFront pour rediriger vers votre origine,

CloudFront transmet chaque combinaison de nom et de valeur du cookie. Il met ensuite en cache séparément les objets renvoyés par votre origine, même s'ils sont tous identiques.

Supposons, par exemple, que les utilisateurs incluent deux cookies dans chaque demande, que chaque cookie possède trois valeurs possibles et que toutes les combinaisons de valeurs de cookies soient possibles. CloudFront transmet jusqu'à six demandes différentes à votre origine pour chaque objet. Si votre origine renvoie différentes versions d'un objet en fonction d'un seul des cookies, cela signifie qu' CloudFront il transmet plus de demandes à votre origine que nécessaire et met inutilement en cache plusieurs versions identiques de l'objet.

- Créez des comportements de cache distincts pour le contenu statique et dynamique, et configurez CloudFront pour transférer les cookies vers votre origine uniquement pour le contenu dynamique.

  Supposons, par exemple, que vous n'ayez qu'un seul comportement de cache pour votre distribution et que vous utilisiez la distribution à la fois pour du contenu dynamique, tel que `.js` des fichiers, et pour `.css` des fichiers qui changent rarement. CloudFront met en cache des versions distinctes de vos `.css` fichiers en fonction des valeurs des cookies, de sorte que chaque emplacement CloudFront périphérique transmet une demande à votre origine pour chaque nouvelle valeur de cookie ou combinaison de valeurs de cookie.

  Si vous créez un comportement de cache qui suit le modèle de chemin `*.css` et qui CloudFront ne met pas en cache en fonction des valeurs des cookies, CloudFront vous transférez les demandes de `.css` fichiers à votre origine uniquement pour la première demande reçue par un emplacement périphérique pour un `.css` fichier donné et pour la première demande après l'expiration d'un `.css` fichier.
- Si possible, créez des comportements de cache distincts pour les contenus dynamiques pour lesquels les valeurs de cookie sont uniques pour chaque utilisateur (comme un ID utilisateur) et les contenus dynamiques qui varient selon un plus petit nombre de valeurs uniques.

Pour plus d’informations, consultez Contenu du cache basé sur les cookies. Si vous souhaitez consulter les cookies qui sont CloudFront transférés vers votre source, consultez les valeurs dans la `cs(Cookie)` colonne de vos fichiers CloudFront journaux. Pour plus d’informations, consultez Configuration et utilisation des journaux standard (journaux d’accès).

Mise en cache basée sur des valeurs d'en-tête

Si vous configurez CloudFront la mise en cache en fonction des en-têtes de demande, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour transférer et mettre en cache en fonction uniquement des en-têtes spécifiés au lieu du transfert et de la mise en cache en fonction de tous les en-têtes. Pour les en-têtes que vous spécifiez, CloudFront transfère chaque combinaison de nom et de valeur d'en-tête. Il met ensuite en cache séparément les objets que votre origine renvoie, même s'ils sont tous identiques.

  > **Note**
  >
  > CloudFront transmet toujours à votre origine les en-têtes spécifiés dans les rubriques suivantes :
  >
  > - Comment CloudFront traite et transmet les demandes à votre serveur d'origine Amazon S3 > En-têtes de requête HTTP qui CloudFront suppriment ou mettent à jour
  > - Comment CloudFront traite et transmet les demandes à votre serveur d'origine personnalisé > En-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3)

  Lorsque vous configurez la mise CloudFront en cache en fonction des en-têtes de demande, vous ne modifiez pas les en-têtes qui CloudFront sont transférés, mais uniquement si les objets sont mis en CloudFront cache en fonction des valeurs des en-têtes.

- Essayez d'éviter d'effectuer la mise en cache en fonction d'en-têtes de demande qui ont des nombres importants de valeurs uniques.

  Par exemple, si vous souhaitez diffuser différentes tailles d'image en fonction de l'appareil de l'utilisateur, ne configurez CloudFront pas le cache en fonction de l'`User-Agent`en-tête, qui comporte un très grand nombre de valeurs possibles. Configurez plutôt CloudFront pour mettre en cache en fonction des en-têtes CloudFront de type de périphérique`CloudFront-Is-Desktop-Viewer`,`CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer` et. `CloudFront-Is-Tablet-Viewer` De plus, si vous renvoyez la même version de l'image pour des tablettes et des ordinateurs de bureau, transmettez uniquement l'en-tête `CloudFront-Is-Tablet-Viewer`, pas l'en-tête `CloudFront-Is-Desktop-Viewer`.

Pour plus d’informations, consultez Contenu du cache basé sur les en-têtes des demandes.

Supprimer l'en-tête **`Accept-Encoding`** lorsqu'une compression n'est pas nécessaire

Si la compression n'est pas activée, parce que l'origine ne la prend pas en charge, CloudFront ne la prend pas en charge ou parce que le contenu n'est pas compressible, vous pouvez augmenter le taux de réussite du cache en associant un comportement de cache dans votre distribution à une origine qui définit les paramètres suivants : Custom Origin Header

- Header name (Nom de l'en-tête: `Accept-Encoding`
- Header value (Valeur de l'en-tête) : (laisser vide)

Lorsque vous utilisez cette configuration, elle CloudFront supprime l'`Accept-Encoding`en-tête de la clé de cache et ne l'inclut pas dans les demandes d'origine. Cette configuration s'applique à tous les contenus fournis CloudFront par la distribution à partir de cette origine.

Diffusez du contenu multimédia via HTTP

Pour plus d'informations sur l'optimisation du contenu vidéo à la demande (VOD) et en streaming, consultez Vidéo à la demande et diffusion vidéo en direct avec CloudFront.

Utilisation d'Amazon CloudFront Origin Shield

CloudFront Origin Shield est une couche supplémentaire de l'infrastructure de mise en CloudFront cache qui permet de minimiser la charge de votre origine, d'améliorer sa disponibilité et de réduire ses coûts d'exploitation. Avec CloudFront Origin Shield, vous bénéficiez des avantages suivants :

Un meilleur taux d'accès au cache

Origin Shield peut contribuer à améliorer le taux de réussite du cache de votre CloudFront distribution, car il fournit une couche de mise en cache supplémentaire devant votre source d'origine. Lorsque vous utilisez Origin Shield, toutes les requêtes envoyées par toutes les couches CloudFront de mise en cache à votre origine passent par Origin Shield, ce qui augmente le risque d'accès au cache. CloudFrontpeut récupérer chaque objet avec une seule demande d'origine envoyée par Origin Shield à votre origine, et toutes les autres couches du CloudFront cache (emplacements périphériques et caches périphériques régionaux) peuvent récupérer l'objet depuis Origin Shield.

Une charge d'origine réduite

La couche Origin Shield peut réduire davantage le nombre de demandes simultanées envoyées à votre origine pour le même objet. Les demandes de contenu ne se trouvant pas dans le cache d'Origin Shield sont consolidées avec d'autres demandes liées au même objet, ce qui permet qu'une seule demande soit envoyée à votre origine. Le fait de traiter moins de demandes à l'origine peut préserver la disponibilité de votre site d'origine en cas de pic de charge ou de pic de trafic imprévu, et peut réduire les coûts liés à des éléments tels que l' just-in-timeemballage, les transformations d'images et le transfert de données sortantes (DTO).

De meilleures performances réseau

Lorsque vous activez Origin Shield dans la AWS région où la latence par rapport à votre origine est la plus faible, vous pouvez obtenir de meilleures performances réseau. Pour les origines situées dans une AWS région, le trafic CloudFront réseau reste sur le CloudFront réseau à haut débit jusqu'à votre point d'origine. Pour les origines extérieures AWS, le trafic CloudFront réseau reste sur le CloudFront réseau jusqu'à Origin Shield, qui dispose d'une connexion à faible latence avec votre point d'origine.

Vous encourez des frais supplémentaires pour l'utilisation d'Origin Shield. Pour plus d'informations, consultez la section CloudFront Tarification.

Rubriques

Cas d'utilisation pour Origin Shield

CloudFront Origin Shield peut être utile dans de nombreux cas d'utilisation, notamment les suivants :

- Utilisateurs répartis dans différentes régions géographiques
- Origines qui fournissent des just-in-time emballages pour la diffusion en direct ou le traitement on-the-fly d'images

- Origines sur site avec des contraintes de capacité ou de bande passante
- Charges de travail utilisant plusieurs réseaux de diffusion de contenu

Il est possible qu'Origin Shield ne soit pas adapté dans certains cas, par exemple pour du contenu dynamique transmis par proxy à l'origine, du contenu avec une mise en cache faible ou du contenu rarement demandé.

Les sections suivantes expliquent les avantages d'Origin Shield pour les cas d'utilisation suivants.

Cas d'utilisation

- Utilisateurs dans des régions géographiques différentes
- Réseaux de diffusion de contenu multiples

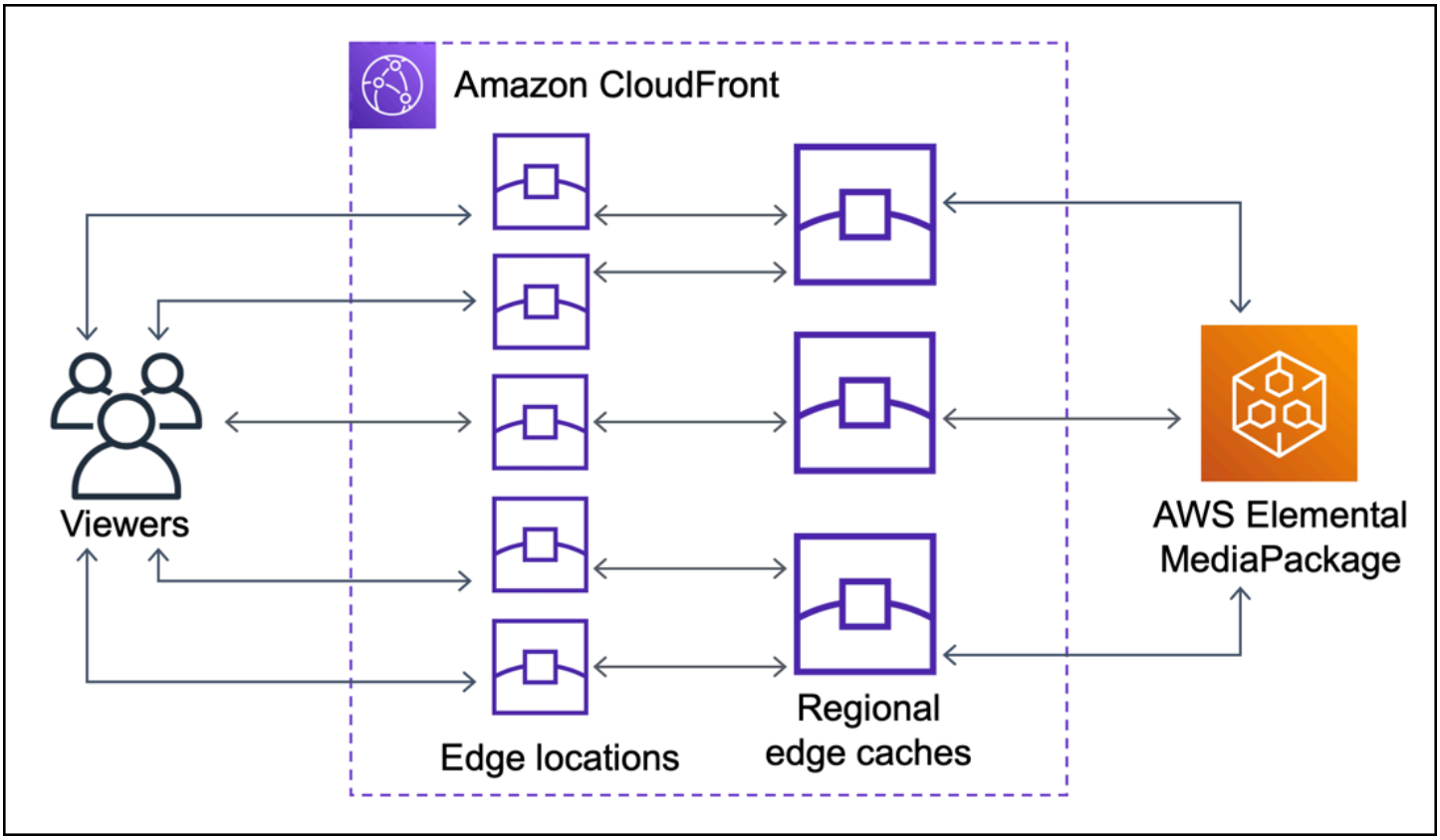
Utilisateurs dans des régions géographiques différentes

Avec Amazon CloudFront, vous bénéficiez par nature d'une charge réduite sur votre source, car les demandes qui CloudFront peuvent être envoyées depuis le cache ne sont pas transmises à votre origine. Outre le réseau mondial CloudFront d'emplacements périphériques, les caches périphériques régionaux servent de couche de mise en cache de niveau intermédiaire pour fournir des accès au cache et consolider les demandes d'origine pour les utilisateurs des régions géographiques voisines. Les demandes du spectateur sont d'abord acheminées vers un emplacement CloudFront périphérique proche, et si l'objet n'est pas mis en cache à cet emplacement, la demande est envoyée vers un cache périphérique régional.

Lorsque les utilisateurs se trouvent dans des régions géographiques différentes, les demandes peuvent être acheminées via différents caches périphériques régionaux, chacun pouvant envoyer une demande à votre origine pour le même contenu. Avec Origin Shield, vous disposez d'une couche supplémentaire de mise en cache entre les caches périphériques régionaux et votre origine. Toutes les demandes provenant de tous les caches périphériques régionaux passent par Origin Shield, réduisant encore la charge sur votre origine. Les diagrammes suivants illustrent ce concept. Dans les diagrammes suivants, l'origine est AWS Elemental MediaPackage.

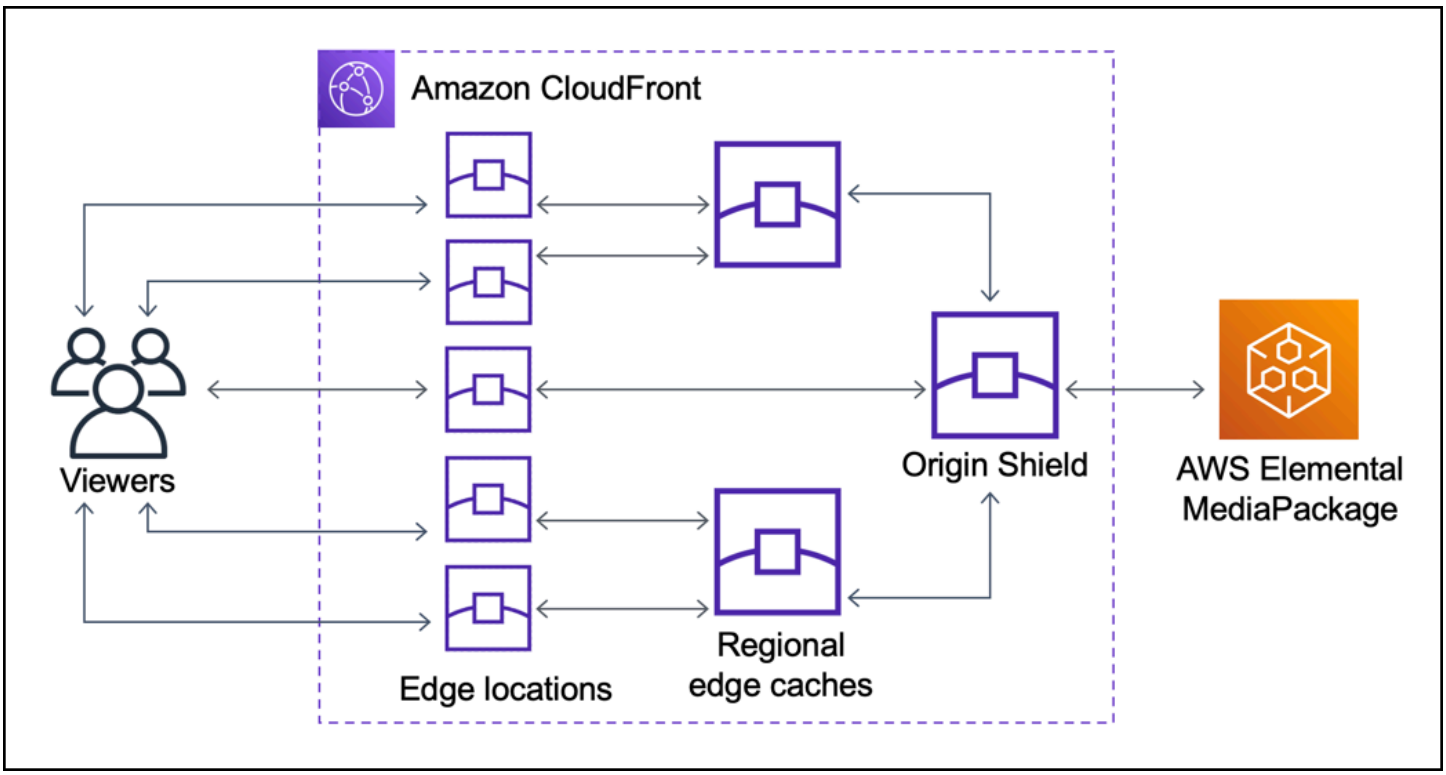
Sans Origin Shield

Sans Origin Shield, votre origine peut recevoir des demandes en double pour le même contenu, comme le montre le diagramme suivant.



Avec Origin Shield

L'utilisation d'Origin Shield permet de réduire la charge sur votre origine, comme le montre le diagramme suivant.



Réseaux de diffusion de contenu multiples

Pour diffuser des événements vidéo en direct ou du contenu populaire à la demande, vous pouvez utiliser plusieurs réseaux de diffusion de contenu. L'utilisation de plusieurs réseaux de diffusion de contenu peut offrir certains avantages, mais cela signifie également que votre origine peut recevoir de nombreuses demandes en double pour le même contenu, chacune provenant de réseaux différents ou d'emplacements différents au sein du même réseau de diffusion de contenu. Ces demandes redondantes peuvent nuire à la disponibilité de votre origine ou entraîner des coûts d'exploitation supplémentaires pour des processus tels que le just-in-time conditionnement ou le transfert de données (DTO) vers Internet.

Lorsque vous associez Origin Shield à l'utilisation de votre CloudFront distribution comme point d'origine pour d'autres CDN, vous pouvez bénéficier des avantages suivants :

- Un nombre moins important de demandes redondantes reçues par votre origine, ce qui contribue à réduire les effets négatifs de l'utilisation de plusieurs réseaux de diffusion de contenu.
- Une clé de cache commune sur les réseaux de diffusion de contenu et une gestion centralisée des fonctions liées à l'origine.
- Amélioration des performances réseau Le trafic réseau provenant d'autres CDN est interrompu à un emplacement CloudFront périphérique proche, ce qui peut provoquer un accès depuis le cache

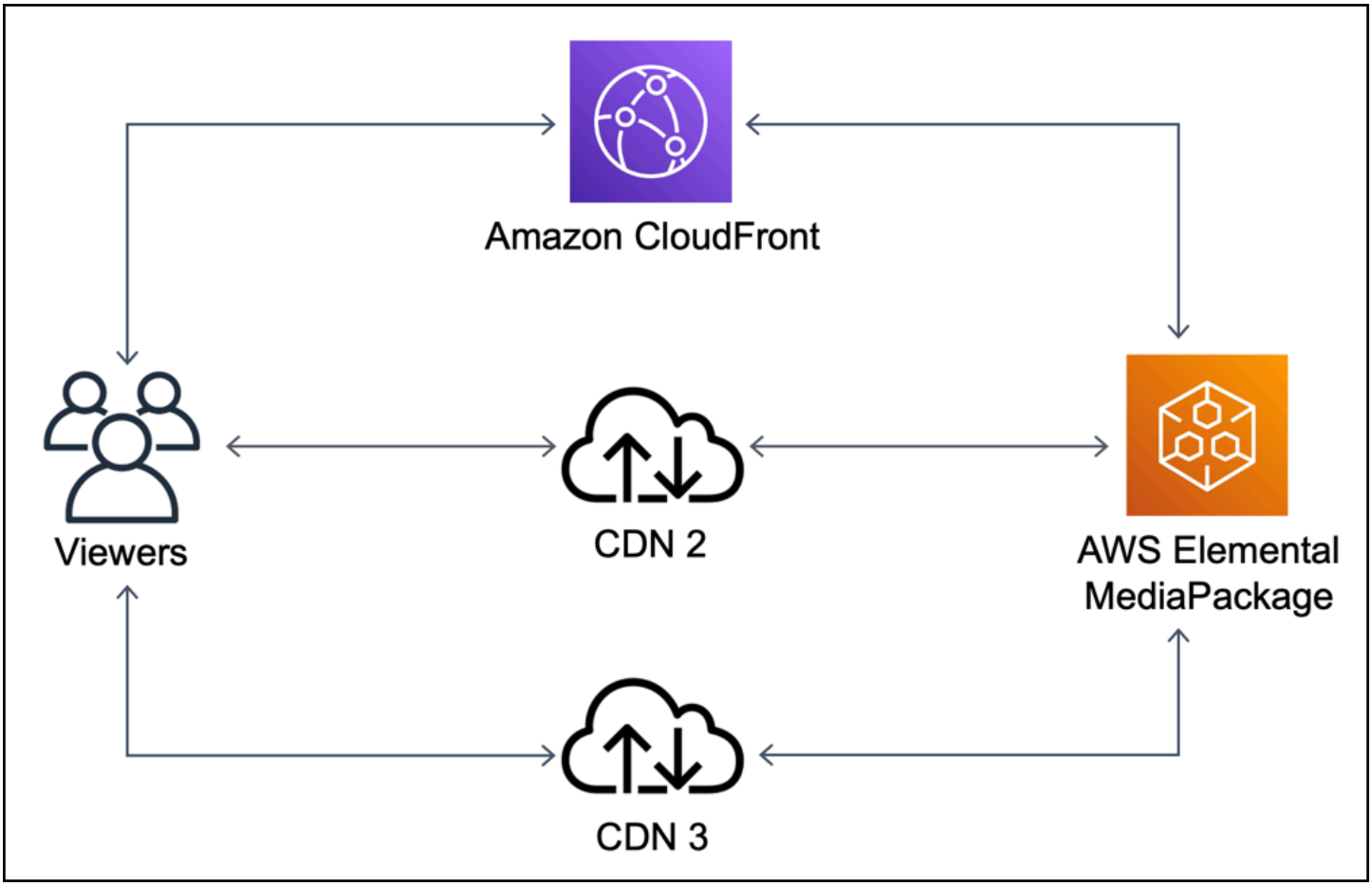
local. Si l'objet demandé ne se trouve pas dans le cache de localisation périphérique, la demande envoyée à l'origine reste sur le CloudFront réseau jusqu'à Origin Shield, qui fournit un débit élevé et une faible latence à l'origine. Si l'objet demandé se trouve dans le cache d'Origin Shield, la demande à votre origine est entièrement évitée.

> **Important**
>
> Si vous souhaitez utiliser Origin Shield dans une architecture multi-CDN et bénéficier de tarifs réduits, contactez-nous ou contactez votre représentant AWS commercial pour plus d'informations. Des frais supplémentaires peuvent être facturés.

Les diagrammes suivants montrent comment cette configuration peut aider à réduire la charge sur votre origine lorsque vous diffusez des événements vidéo populaires en direct avec plusieurs réseaux de diffusion de contenu. Dans les diagrammes suivants, l'origine est AWS Elemental MediaPackage.

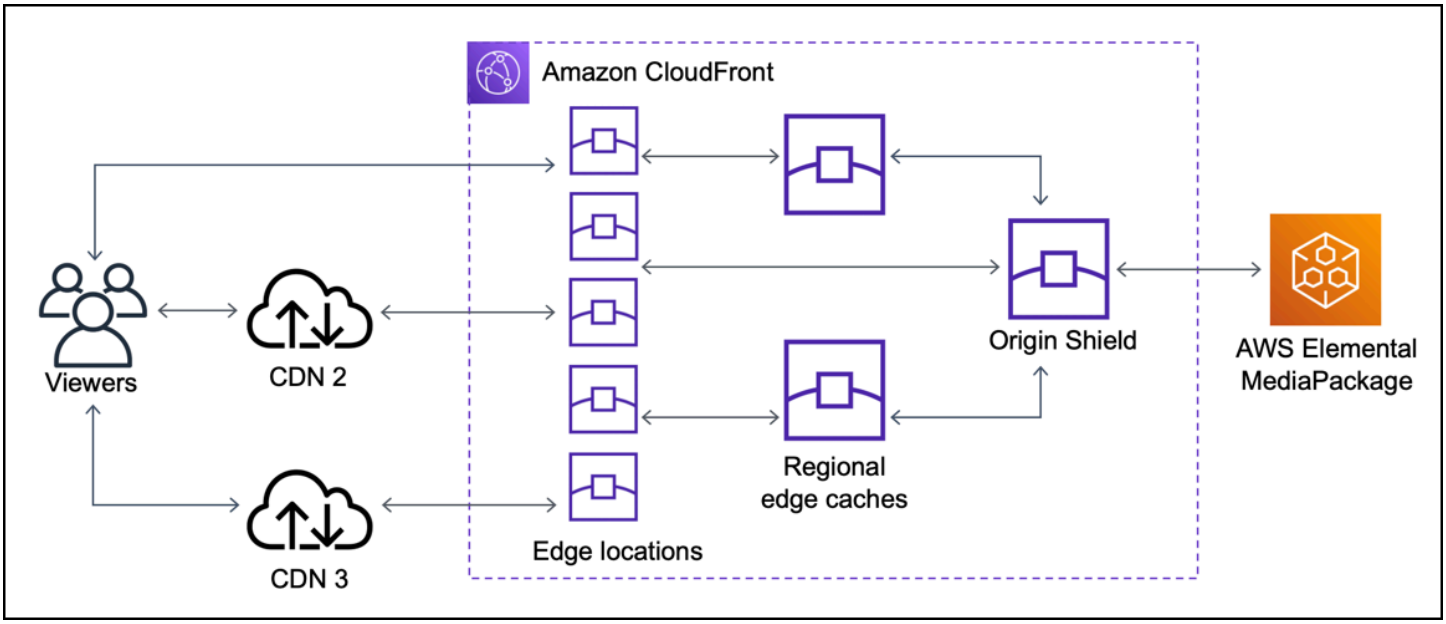
Sans Origin Shield (plusieurs réseaux de diffusion de contenu)

Sans Origin Shield, votre origine peut recevoir de nombreuses demandes en double pour le même contenu, chacune provenant d'un réseau de diffusion de contenu différent, comme indiqué dans le diagramme suivant.



Avec Origin Shield (plusieurs réseaux de diffusion de contenu)

L'utilisation d'Origin Shield, CloudFront comme origine pour vos autres CDN, peut contribuer à réduire la charge sur votre origine, comme le montre le schéma suivant.



Choisir la AWS région pour Origin Shield

Amazon CloudFront propose Origin Shield dans AWS les régions CloudFront disposant d'un cache périphérique régional. Lorsque vous activez Origin Shield, vous choisissez la AWS région pour Origin Shield. Vous devez choisir la région AWS dont la latence vers votre origine est la plus faible. Vous pouvez utiliser Origin Shield avec des origines situées dans une AWS région ou non AWS.

Pour les origines dans une région AWS

Si votre origine se trouve dans une AWS région, déterminez d'abord si votre origine se trouve dans une région dans laquelle Origin CloudFront Shield est proposé. CloudFront propose Origin Shield dans les AWS régions suivantes.

- US East (Ohio) – `us-east-2`
- US East (N. Virginia) – `us-east-1`
- US West (Oregon) – `us-west-2`
- Asia Pacific (Mumbai) – `ap-south-1`
- Asie-Pacifique (Séoul) – `ap-northeast-2`
- Asia Pacific (Singapore) – `ap-southeast-1`
- Asie-Pacifique (Sydney) – `ap-southeast-2`
- Asie-Pacifique (Tokyo) – `ap-northeast-1`
- Europe (Frankfurt) – `eu-central-1`

- Europe (Ireland) – `eu-west-1`
- Europe (London) – `eu-west-2`
- South America (São Paulo) – `sa-east-1`

Si votre origine se trouve dans une AWS région CloudFront proposant Origin Shield

Si votre origine se trouve dans une AWS région qui CloudFront propose Origin Shield (voir la liste précédente), activez Origin Shield dans la même région que votre origine.

Si votre origine ne se trouve pas dans une AWS région CloudFront proposant Origin Shield

Si votre origine ne se trouve pas dans une AWS région CloudFront proposant Origin Shield, consultez le tableau suivant pour déterminer dans quelle région activer Origin Shield.

Si votre origine est dans...	Activer Origin Shield dans ...
US West (N. California) – `us-west-1`	US West (Oregon) – `us-west-2`
Africa (Cape Town) – `af-south-1`	Europe (Ireland) – `eu-west-1`
Asia Pacific (Hong Kong) – `ap-east-1`	Asia Pacific (Singapore) – `ap-southeast-1`
Canada (Central) – `ca-central-1`	US East (N. Virginia) – `us-east-1`
Europe (Milan) – `eu-south-1`	Europe (Frankfurt) – `eu-central-1`
Europe (Paris) – `eu-west-3`	Europe (London) – `eu-west-2`
Europe (Stockholm) – `eu-north-1`	Europe (London) – `eu-west-2`
Middle East (Bahrain) – `me-south-1`	Asia Pacific (Mumbai) – `ap-south-1`

Pour les origines en dehors de AWS

Vous pouvez utiliser Origin Shield avec une origine sur site ou ne se trouvant pas dans une région AWS . Dans ce cas, activez Origin Shield dans la AWS région où la latence par rapport à votre origine est la plus faible. Si vous ne savez pas quelle AWS région présente la latence la plus faible par rapport à votre point d'origine, vous pouvez utiliser les suggestions suivantes pour vous aider à prendre une décision.

- Vous pouvez consulter le tableau précédent pour avoir une idée de la région AWS pouvant présenter la latence la plus faible vers votre origine, en fonction de l'emplacement géographique de votre origine.
- Vous pouvez lancer des instances Amazon EC2 dans différentes AWS régions géographiquement proches de votre origine et effectuer des tests `ping` pour mesurer les latences réseau typiques entre ces régions et votre origine.

Activation d'Origin Shield

Vous pouvez activer Origin Shield pour améliorer votre taux d'accès au cache, réduire la charge sur votre origine et améliorer les performances. Pour activer Origin Shield, modifiez les paramètres d'origine dans une CloudFront distribution. Origin Shield est une propriété de l'origine. Pour chaque origine de vos CloudFront distributions, vous pouvez activer Origin Shield séparément dans AWS la région offrant les meilleures performances pour cette origine.

Vous pouvez activer Origin Shield dans la CloudFront console AWS CloudFormation, avec ou avec l' CloudFrontAPI.

Console

Pour activer Origin Shield pour une origine existante (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution contenant l'origine à mettre à jour.
3. Choisissez l'onglet Origins and Origin Groups (Origines et groupes d'origine).
4. Choisissez l'origine à mettre à jour, puis choisissez Edit (Modifier).
5. Pour Enable Origin Shield (Activer Origin Shield), choisissez Yes (Oui).
6. Pour Origin Shield Region, choisissez la AWS région dans laquelle vous souhaitez activer Origin Shield. Pour obtenir de l'aide sur le choix d'une région, veuillez consulter Choisir la AWS région pour Origin Shield.
7. Au bas de la page, choisissez Oui, modifier.

Lorsque le statut de votre distribution est Deployed (Déployée), Origin Shield est prêt. Cela prend quelques minutes.

Pour activer Origin Shield pour une nouvelle origine (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Pour créer la nouvelle origine dans une distribution existante, procédez comme suit :

   1. Choisissez la distribution dans laquelle vous souhaitez créer l'origine.
   2. Choisissez Créer une origine, puis passez à l'étape 3.

   Pour créer la nouvelle origine dans une nouvelle distribution, procédez comme suit :

   1. Choisissez Create Distribution.
   2. Dans la section Web choisissez Mise en route. Dans la section Paramètres d'origine procédez comme suit, en commençant par l'étape 3.
3. Pour Enable Origin Shield (Activer Origin Shield), choisissez Yes (Oui).
4. Pour Origin Shield Region, choisissez la AWS région dans laquelle vous souhaitez activer Origin Shield. Pour obtenir de l'aide sur le choix d'une région, veuillez consulter Choisir la AWS région pour Origin Shield.

   Si vous créez une nouvelle distribution, continuez à configurer votre distribution en utilisant les autres paramètres de la page. Pour de plus amples informations, veuillez consulter Référence des paramètres de distribution.
5. N'oubliez pas d'enregistrer vos modifications en choisissant Créer (pour une nouvelle origine dans une distribution existante) ou Créer une distribution (pour une nouvelle origine dans une nouvelle distribution).

Lorsque le statut de votre distribution est Deployed (Déployée), Origin Shield est prêt. Cela prend quelques minutes.

AWS CloudFormation

Pour activer Origin Shield avec AWS CloudFormation, utilisez la `OriginShield` propriété dans le type de `Origin` propriété d'une `AWS::CloudFront::Distribution` ressource. Vous pouvez ajouter la propriété `OriginShield` à un type de propriété `Origin` existant, ou l'inclure lorsque vous créez un nouveau type de propriété `Origin`.

L'exemple suivant présente la syntaxe, au format YAML, pour l'activation d'`OriginShield` dans la région USA Ouest (Oregon) (`us-west-2`). Pour obtenir de l'aide sur le choix d'une

région, veuillez consulter the section called “Choisir la AWS région pour Origin Shield”. Cet exemple montre uniquement le type de propriété `Origin`, et non l'ensemble de la ressource `AWS::CloudFront::Distribution`.

```
Origins:
- DomainName: 3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com
  Id: Example-EMP-3ae97e9482b0d011
  OriginShield:
    Enabled: true
    OriginShieldRegion: us-west-2
  CustomOriginConfig:
    OriginProtocolPolicy: match-viewer
    OriginSSLProtocols: TLSv1
```

Pour plus d'informations, consultez AWS::CloudFront::Distribution Origin dans la section de référence des ressources et des propriétés du Guide de AWS CloudFormation l'utilisateur.

API

Pour activer Origin Shield avec l' CloudFront API à l'aide AWS des SDK ou AWS Command Line Interface (AWS CLI), utilisez le `OriginShield` type. Vous spécifiez `OriginShield` dans un type `Origin`, dans un type`DistributionConfig`. Pour plus d'informations sur le `OriginShield` type, consultez les informations suivantes dans le Amazon CloudFront API Reference.

- OriginShield(type)
- Origin (type)
- DistributionConfig(type)
- UpdateDistribution(opération)
- CreateDistribution(opération)

La syntaxe spécifique pour l'utilisation de ces types et opérations varie en fonction du client SDK, CLI ou de l'API. Pour de plus amples informations, veuillez consulter la documentation de référence de votre kit SDK, CLI ou client.

Estimation des frais liés à Origin Shield

Les frais liés à Origin Shield augmentent en fonction du nombre de demandes adressées à Origin Shield en tant que couche incrémentielle.

Pour les demandes dynamiques (ne pouvant pas être mises en cache) qui sont transmises par proxy à l'origine, Origin Shield est toujours une couche incrémentielle. Les requêtes dynamiques utilisent les méthodes HTTP `PUT`,`POST`,`PATCH`, et`DELETE`.

`GET`et les `HEAD` demandes dont le paramètre de durée de vie (TTL) est inférieur à 3 600 secondes sont considérées comme des demandes dynamiques. En outre, `GET` les `HEAD` demandes dont la mise en cache est désactivée sont également considérées comme des demandes dynamiques.

Pour estimer vos frais liés à Origin Shield pour les demandes dynamiques, utilisez la formule suivante :

Nombre total de demandes dynamiques x frais Origin Shield pour 10 000 demandes / 10 000

Pour les requêtes non dynamiques utilisant les méthodes HTTP, et `GET` `HEAD`, `OPTIONS`, Origin Shield est parfois une couche incrémentielle. Lorsque vous activez Origin Shield, vous choisissez Origin Shield. Région AWS Pour les demandes qui sont naturellement dirigées vers le cache périphérique régional de la même région qu'Origin Shield, Origin Shield n'est pas une couche incrémentielle. Ces demandes ne vous sont pas facturées par Origin Shield. Pour les demandes qui sont envoyées vers un cache périphérique régional dans une région différente de celle d'Origin Shield, puis vers Origin Shield, Origin Shield est une couche incrémentielle. Des frais Origin Shield supplémentaires seront facturés pour ces demandes.

Pour estimer vos frais liés à Origin Shield pour les demandes pouvant être mises en cache, utilisez la formule suivante :

Nombre total de demandes pouvant être mises en cache x (1 – taux d'accès au cache) x pourcentage de demandes allant à Origin Shield à partir d'un cache périphérique régional dans une autre région x frais Origin Shield pour 10 000 demandes / 10 000

Pour plus d'informations sur le tarif pour 10 000 demandes pour Origin Shield, consultez la section CloudFront Tarification.

Haute disponibilité d'Origin Shield

Origin Shield tire parti de la fonctionnalité de caches périphériques CloudFront régionaux. Chacun de ces caches périphériques est créé dans une AWS région utilisant au moins trois zones de

disponibilité avec des flottes d'instances Amazon EC2 auto-scalables. Les connexions entre les CloudFront sites et Origin Shield utilisent également le suivi actif des erreurs pour chaque demande afin d'acheminer automatiquement la demande vers un site Origin Shield secondaire si le site Origin Shield principal n'est pas disponible.

Comment Origin Shield interagit avec les autres fonctionnalités CloudFront

Les sections suivantes expliquent comment Origin Shield interagit avec les autres CloudFront fonctionnalités.

Origin Shield et CloudFront journalisation

Pour connaître le moment où Origin Shield a traité une demande, vous devez activer l'une des options suivantes :

- CloudFront journaux standard (journaux d'accès). Les journaux standard sont fournis gratuitement.
- CloudFront journaux en temps réel. Des frais supplémentaires sont liés à l'utilisation des journaux en temps réel. Consultez les CloudFront tarifs Amazon.

Les accès au cache provenant d'Origin Shield apparaissent comme `OriginShieldHit` `x-edge-detailed-result-type` sur le terrain dans CloudFront les journaux. Origin Shield exploite les CloudFront caches périphériques régionaux d'Amazon. Si une demande est acheminée depuis un emplacement CloudFront périphérique vers le cache périphérique régional qui agit en tant qu'Origin Shield, elle est signalée comme un `Hit` dans les journaux, et non comme un`OriginShieldHit`.

Origin Shield et groupes d'origines

Origin Shield est compatible avec les groupes CloudFront d'origine. Origin Shield étant une propriété de l'origine, les demandes passent toujours par Origin Shield pour chaque origine, même lorsque l'origine fait partie d'un groupe d'origines. Pour une demande donnée, CloudFront achemine la demande vers l'origine principale du groupe d'origine via le Origin Shield de l'origine principale. Si cette demande échoue (selon les critères de basculement du groupe d'origine), CloudFront achemine la demande vers l'origine secondaire via le Origin Shield de l'origine secondaire.

Origin Shield et Lambda@Edge

Origin Shield n'a pas d'impact sur l'exécution des fonctions de Lambda@Edge, mais peut affecter la région AWS dans laquelle ces fonctions s'exécutent.

Lorsque vous utilisez Origin Shield avec Lambda @Edge, les déclencheurs orientés vers l'origine (demande d'origine et réponse d'origine) s'exécutent dans la région AWS où Origin Shield est activé. Si l'emplacement Origin Shield principal n'est pas disponible et CloudFront achemine les demandes vers un emplacement Origin Shield secondaire, les déclencheurs Lambda @Edge orientés vers l'origine seront également déplacés pour utiliser l'emplacement secondaire d'Origin Shield.

Les déclencheurs liés à l'utilisateur ne sont pas affectés.

Optimisez la haute disponibilité grâce au basculement CloudFront d'origine

Vous pouvez configurer le basculement CloudFront d'origine pour les scénarios nécessitant une haute disponibilité. Pour commencer, vous créez un groupe d'origine avec deux origines : une principale et une secondaire. Si l'origine principale n'est pas disponible ou renvoie des codes d'état de réponse HTTP spécifiques indiquant un échec, passe CloudFront automatiquement à l'origine secondaire.

Pour configurer le basculement d'origine, vous devez avoir une distribution avec au moins deux origines. Ensuite, vous créez un groupe d'origine pour votre distribution incluant deux origines, en en définissant une comme la principale. Enfin, vous créez ou mettez à jour un comportement de cache pour utiliser le groupe d'origine.

Pour voir les étapes de configuration des groupes d'origine et des options de basculement pour une origine spécifique, veuillez consulter Création d'un groupe d'origine.

Après avoir configuré le basculement d'origine pour un comportement de cache, CloudFront procédez comme suit pour les demandes des utilisateurs :

- En cas d'accès au cache, CloudFront renvoie l'objet demandé.
- En cas de perte de cache, CloudFront achemine la demande vers l'origine principale du groupe d'origine.
- Lorsque l'origine principale renvoie un code d'état qui n'est pas configuré pour le basculement, tel qu'un code d'état HTTP 2xx ou 3xx, envoie l'objet CloudFront demandé au visualiseur.
- Lorsque l'une des situations suivantes se produit :
  - L'origine principale renvoie un code d'état HTTP que vous avez configuré pour le basculement
  - CloudFront ne parvient pas à se connecter à l'origine principale
  - La réponse de l'origine principale met trop de temps à arriver (temps d'attente)

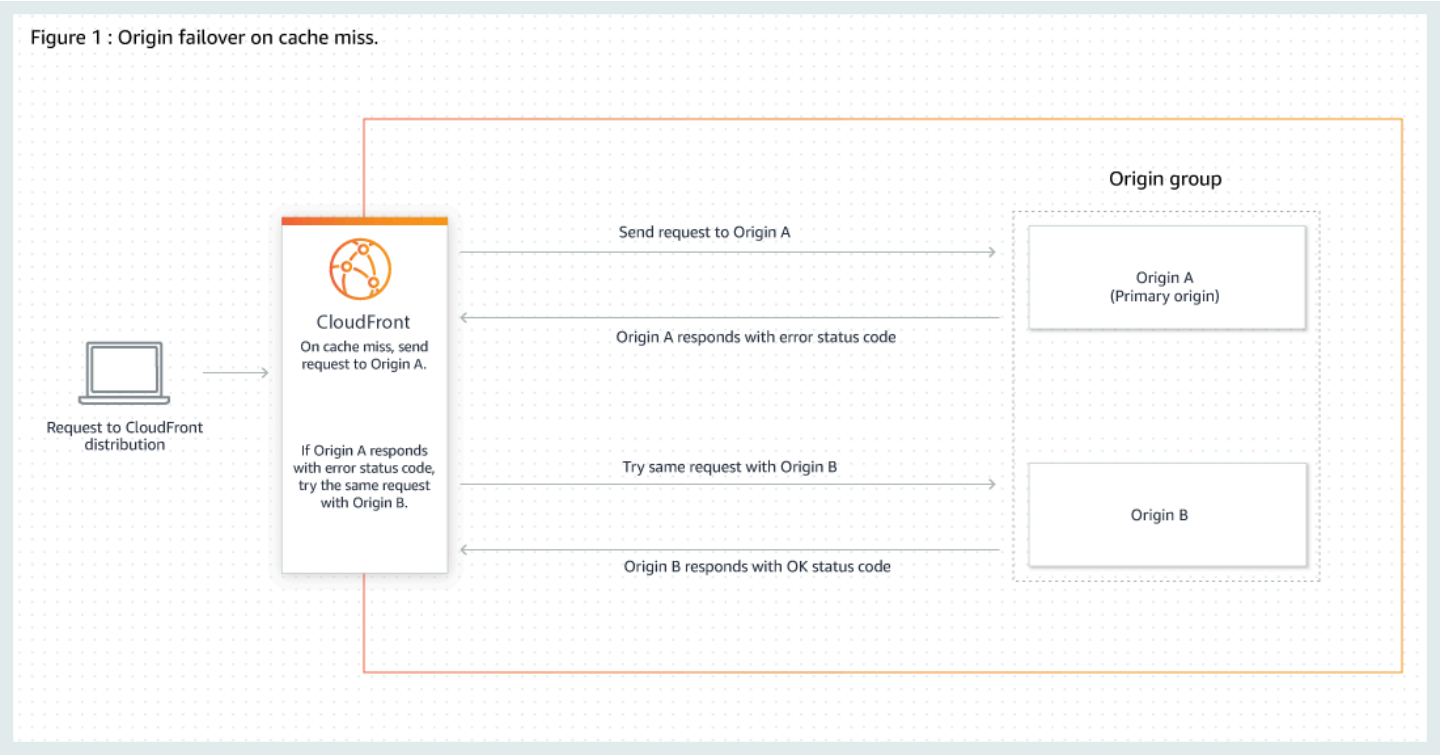
CloudFront Route ensuite la demande vers l'origine secondaire du groupe d'origine.

> **Note**
>
> Dans certains cas d'utilisation, tels que le streaming de contenu vidéo, vous CloudFront souhaiterez peut-être passer rapidement à l'origine secondaire. Pour régler la rapidité CloudFront du basculement vers l'origine secondaire, voirContrôlez les délais et les tentatives d'origine.

CloudFront achemine toutes les demandes entrantes vers l'origine principale, même lorsqu'une demande précédente a échoué vers l'origine secondaire. CloudFront envoie des demandes à l'origine secondaire uniquement après l'échec d'une demande à l'origine principale.

CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du spectateur est `GET`, `HEAD`, ou`OPTIONS`. CloudFront ne bascule pas lorsque le visualiseur envoie une autre méthode HTTP (par exemple `POST`,`PUT`, etc.).

Le graphique suivant illustre le fonctionnement du basculement d'origine



Rubriques

Création d'un groupe d'origine

Pour créer un groupe d'origine

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution pour laquelle vous souhaitez créer le groupe d'origine.
3. Choisissez l'onglet Origines.
4. Assurez-vous qu'il existe plusieurs origines pour la distribution. Si ce n'est pas le cas, ajoutez une deuxième origine.
5. Sous l'onglet Origins (Origines) du volet Origin groups (Groupes d'origines), choisissez Create origin group (Créer un groupe d'origines).
6. Choisissez les origines du groupe d'origine. Après avoir ajouté des origines, utilisez les flèches pour définir la priorité, c'est-à-dire l'origine principale et l'origine secondaire.
7. Saisissez un nom pour le groupe d'origines.
8. Choisissez les codes d'état HTTP à utiliser comme critères de basculement. Vous pouvez choisir n'importe quelle combinaison des codes d'état suivants : 400, 403, 404, 416, 500, 502, 503 ou 504. Lorsqu'il CloudFront reçoit une réponse avec l'un des codes d'état que vous spécifiez, il bascule vers l'origine secondaire.

   > **Note**
   >
   > CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du spectateur est `GET`, `HEAD`, ou`OPTIONS`. CloudFront ne bascule pas lorsque le visualiseur envoie une autre méthode HTTP (par exemple `POST`,`PUT`, etc.).

9. Choisissez Create origin group (Créer un groupe d'origines).

Assurez-vous d'attribuer votre groupe d'origine comme origine du comportement du cache de votre distribution. Pour plus d'informations, consultez Nom.

Contrôlez les délais et les tentatives d'origine

Par défaut, CloudFront essaie de se connecter à l'origine principale dans un groupe d'origine pendant 30 secondes maximum (3 tentatives de connexion de 10 secondes chacune) avant de basculer vers l'origine secondaire. Dans certains cas d'utilisation, tels que le streaming de contenu vidéo, vous CloudFront souhaiterez peut-être passer plus rapidement à l'origine secondaire. Vous pouvez ajuster les paramètres suivants pour déterminer la rapidité avec laquelle vous CloudFront basculez vers l'origine secondaire. Si l'origine est une origine secondaire ou une origine ne faisant pas partie d'un groupe d'origine, ces paramètres affectent la rapidité CloudFront avec laquelle une réponse HTTP 504 est renvoyée au lecteur.

Pour basculer plus rapidement, spécifiez un délai d'expiration de connexion plus court, moins de tentatives de connexion, ou les deux. Pour les origines personnalisées (y compris les origines de compartiment Amazon S3 qui sont configurées avec un hébergement de site web statique), vous pouvez également ajuster le délai d'expiration de la réponse d'origine.

Délai d'expiration de la connexion d'origine

Le paramètre de délai d'expiration de la connexion d'origine affecte le temps d' CloudFront attente lors de la tentative d'établissement d'une connexion avec l'origine. Par défaut, CloudFront attend 10 secondes pour établir une connexion, mais vous pouvez spécifier 1 à 10 secondes (inclus). Pour plus d’informations, consultez Délai de connexion.

Tentatives de connexion de l'origine

Le paramètre Tentatives de connexion d'origine affecte le nombre de CloudFront tentatives de connexion à l'origine. Par défaut, CloudFront essaie 3 fois de se connecter, mais vous pouvez spécifier 1 à 3 (inclus). Pour plus d’informations, consultez Tentatives de connexion.

Pour une origine personnalisée (y compris un compartiment Amazon S3 configuré avec un hébergement de site Web statique), ce paramètre affecte également le nombre de CloudFront tentatives d'obtention d'une réponse de la part de l'origine en cas d'expiration du délai de réponse d'origine.

Délai de réponse de l'origine

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

Le paramètre de délai d'expiration de la réponse d'origine affecte le temps d' CloudFront attente pour recevoir une réponse (ou pour recevoir la réponse complète) de la part de l'origine. Par défaut, CloudFront attend 30 secondes, mais vous pouvez spécifier 1 à 60 secondes (incluses). Pour plus d'informations, consultez Délai de réponse (origines personnalisées uniquement).

Comment modifier ces paramètres

Pour modifier ces paramètres dans la CloudFront console

- Pour une nouvelle origine ou une nouvelle distribution, vous spécifiez ces valeurs lorsque vous créez la ressource.
- Pour une origine existante dans une distribution existante, vous spécifiez ces valeurs lorsque vous modifiez l'origine.

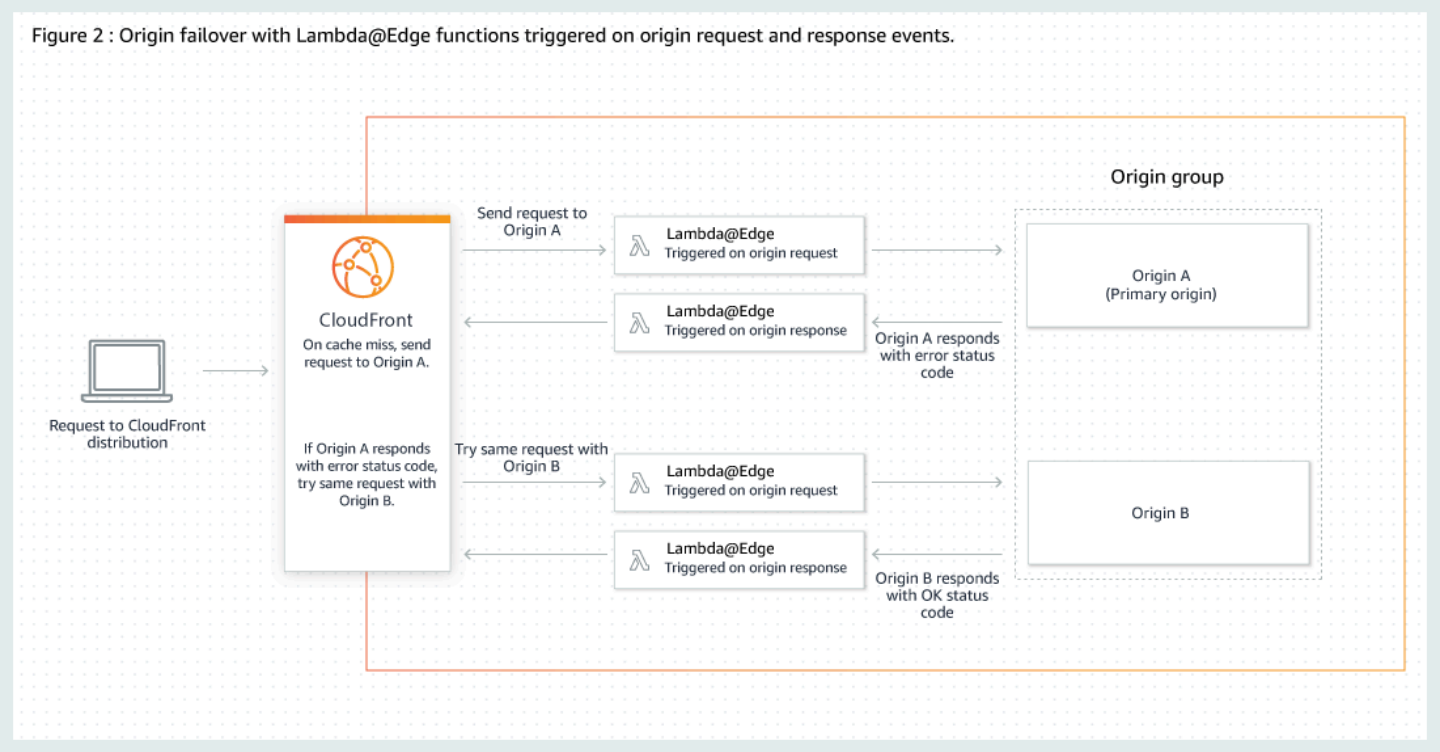
Pour de plus amples informations, veuillez consulter Référence des paramètres de distribution.

Utilisation du basculement d'origine avec les fonctions Lambda@Edge

Vous pouvez utiliser les fonctions Lambda @Edge avec des CloudFront distributions que vous avez configurées avec des groupes d'origine. Pour utiliser une fonction Lambda, spécifiez-la dans une demande d'origine ou un déclencheur de réponse de l'origine pour un groupe d'origine lorsque vous créez le comportement de cache. Lorsque vous utilisez une fonction Lambda@Edge avec un groupe d'origine, la fonction peut être déclenchée deux fois pour une seule demande d'utilisateur. Par exemple, envisagez le scénario suivant :

1. Vous créez une fonction Lambda@Edge avec un déclencheur de demande d'origine.
2. La fonction Lambda est déclenchée une fois lors de l' CloudFront envoi d'une demande à l'origine principale (en cas d'échec du cache).
3. L'origine principale répond avec un code d'état HTTP configuré pour le basculement.
4. La fonction Lambda est à nouveau déclenchée lorsqu'elle CloudFront envoie la même demande à l'origine secondaire.

Le schéma suivant illustre la façon dont le basculement d'origine fonctionne lorsque vous incluez une fonction Lambda@Edge dans une requête d'origine ou un déclencheur de réponse.



Pour plus d'informations sur l'utilisation des déclencheurs Lambda@Edge, consultez the section called “Ajouter des déclencheurs pour une fonction Lambda @Edge”.

Pour plus d'informations sur la gestion du basculement DNS, consultez la section Configuration du basculement DNS dans le manuel Amazon Route 53 Developer Guide.

Utilisation des pages d'erreur personnalisées avec le basculement d'origine

Vous pouvez utiliser des pages d'erreur personnalisées avec des groupes d'origine de la même façon dont vous les utiliseriez avec des origines qui ne sont pas configurées pour le basculement d'origine.

Lorsque vous utilisez le basculement d'origine, vous pouvez configurer CloudFront pour renvoyer une page d'erreur personnalisée pour l'origine principale ou secondaire (ou les deux) :

- Renvoyer une page d'erreur personnalisée pour l'origine principale : si l'origine principale renvoie un code d'état HTTP qui n'est pas configuré pour le basculement, CloudFront renvoie la page d'erreur personnalisée aux lecteurs.
- Renvoie une page d'erreur personnalisée pour l'origine secondaire : si CloudFront l'origine secondaire envoie un code d'état de défaillance, CloudFront renvoie la page d'erreur personnalisée.

Pour plus d'informations sur l'utilisation de pages d'erreur personnalisées avec CloudFront, consultezGénérez des réponses d'erreur personnalisées.

Gérer la durée pendant laquelle le contenu reste dans le cache (expiration)

Vous pouvez contrôler la durée pendant laquelle vos fichiers restent dans le CloudFront cache avant de CloudFront transmettre une autre demande à votre source. Réduire la durée vous permet de servir des contenus dynamiques. Augmenter la durée signifie que vos utilisateurs obtiennent de meilleures performances parce que vos fichiers sont plus susceptibles d'être servis directement à partir du cache périphérique. Une durée plus longue réduit également la charge sur votre origine.

Généralement, CloudFront diffuse un fichier à partir d'un emplacement périphérique jusqu'à ce que la durée de cache que vous avez spécifiée soit atteinte, c'est-à-dire jusqu'à ce que le fichier expire. Après son expiration, la prochaine fois que l'emplacement périphérique reçoit une demande pour le fichier, CloudFront transmet la demande à l'origine pour vérifier que le cache contient la dernière version du fichier. La réponse de l'origine varie selon que le fichier a changé ou non :

- Si le CloudFront cache possède déjà la dernière version, l'origine renvoie un code d'état`304 Not Modified`.
- Si le CloudFront cache ne possède pas la dernière version, l'origine renvoie un code d'état `200 OK` et la dernière version du fichier.

Si un fichier situé dans un emplacement périphérique n'est pas fréquemment demandé, CloudFront vous pouvez l'expulser (supprimer le fichier avant sa date d'expiration) pour faire de la place aux fichiers demandés plus récemment.

Par défaut, chaque fichier expire automatiquement au bout de 24 heures, mais vous pouvez modifier le comportement par défaut de deux manières :

- Pour modifier la durée du cache pour tous les fichiers qui correspondent au même schéma de chemin, vous pouvez modifier les CloudFront paramètres TTL minimum, TTL maximum et TTL par défaut pour un comportement de cache. Pour plus d'informations sur les différents paramètres, consultez Durée de vie minimale, Durée de vie maximale et Durée de vie par défaut dans the section called “Paramètres de distribution”.
- Pour changer la durée de conservation en cache pour un fichier individuel, vous pouvez configurer votre origine de sorte à ajouter un en-tête `Cache-Control` avec la directive `max-age` ou `s-`

`maxage`, ou un en-tête `Expires` au fichier. Pour plus d'informations, consultez Utiliser des en-têtes pour contrôler la durée du cache pour des objets individuels.

Pour de plus amples informations sur la manière dont la durée de vie minimale, la durée de vie par défaut et la durée de vie maximale interagissent avec les directives `max-age` et `s-maxage`, ainsi que le champ d'en-tête `Expires`, veuillez consulter the section called "Spécifiez la durée de mise en CloudFront cache des objets".

Vous pouvez également contrôler la durée pendant laquelle les erreurs (par exemple`404 Not Found`) restent dans un CloudFront cache avant de CloudFront réessayer d'obtenir l'objet demandé en transférant une autre demande à votre origine. Pour plus d'informations, consultez the section called "Comment CloudFront traite les codes d'état HTTP 4xx et 5xx de votre origine".

Rubriques

- Utiliser des en-têtes pour contrôler la durée du cache pour des objets individuels
- Servir du contenu périmé (expiré)
- Spécifiez la durée de mise en CloudFront cache des objets
- Ajoutez des en-têtes à vos objets à l'aide de la console Amazon S3

Utiliser des en-têtes pour contrôler la durée du cache pour des objets individuels

Vous pouvez utiliser les en-têtes `Cache-Control` et `Expires` pour contrôler pendant combien de temps des objets restent dans le cache. Les valeurs de Durée de vie minimale, Durée de vie par défaut et Durée de vie maximale affectent également la durée de conservation en cache, mais voici un aperçu de l'incidence de ces en-têtes sur cette durée :

- La `Cache-Control max-age` directive vous permet de spécifier la durée (en secondes) pendant laquelle vous souhaitez qu'un objet reste dans le cache CloudFront avant de le récupérer depuis le serveur d'origine. Le délai d'expiration minimum pris CloudFront en charge est de 0 seconde. La valeur maximale est 100 ans. Spécifiez la valeur au format suivant :

  ```
  Cache-Control: max-age=secondes
  ```

  Par exemple, la directive suivante indique CloudFront de conserver l'objet associé dans le cache pendant 3 600 secondes (une heure) :

```
Cache-Control: max-age=3600
```

Si vous souhaitez que les objets restent dans les caches CloudFront périphériques pendant une durée différente de celle dans les caches du navigateur, vous pouvez utiliser les `Cache-Control s-maxage` directives `Cache-Control max-age` et conjointement. Pour plus d'informations, consultez Spécifiez la durée de mise en CloudFront cache des objets.

- Le champ d'en-tête `Expires` vous permet de spécifier une date et une heure d'expiration au format spécifié dans RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1 Section 3.3.1, Full Date, par exemple :

```
Sat, 27 Jun 2015 23:59:59 GMT
```

Nous vous recommandons d'utiliser la directive `Cache-Control max-age` plutôt que le champ d'en-tête `Expires` pour contrôler la mise en cache des objets. Si vous spécifiez des valeurs à la fois pour `Cache-Control max-age` et pour`Expires`, CloudFront utilise uniquement la valeur de`Cache-Control max-age`.

Pour plus d'informations, consultez Spécifiez la durée de mise en CloudFront cache des objets.

Vous ne pouvez pas utiliser les champs HTTP `Cache-Control` ou d'`Pragma`en-tête dans une `GET` demande d'un visualiseur CloudFront pour forcer le retour de l'objet sur le serveur d'origine. CloudFront ignore ces champs d'en-tête dans les demandes des utilisateurs.

Pour plus d'informations sur les champs d'en-tête `Cache-Control` et `Expires`, consultez les sections suivantes de RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1:

- Section 14.9 Cache Control
- Section 14.21 Expires

Servir du contenu périmé (expiré)

CloudFront prend en charge `Stale-While-Revalidate` les directives de contrôle du `Stale-If-Error` cache et.

- La `stale-while-revalidate` directive permet CloudFront de diffuser du contenu périmé depuis le cache tout en récupérant de manière asynchrone une nouvelle version depuis l'origine. Cela améliore la latence, car les utilisateurs reçoivent des réponses immédiatement depuis CloudFront

les emplacements périphériques sans avoir à attendre la récupération en arrière-plan, et le nouveau contenu est chargé en arrière-plan pour les demandes futures.

Dans l'exemple suivant, met en CloudFront cache la réponse pendant une heure (`max-age=3600`). Si une demande est faite après cette période, CloudFront diffuse le contenu périmé tout en envoyant simultanément une demande à l'origine pour revalider et actualiser le contenu mis en cache. Le contenu obsolète est diffusé pendant 10 minutes au maximum (`stale-while-revalidate=600`) pendant la revalidation du contenu.

```
Cache-Control: max-age=3600, stale-while-revalidate=600
```

- La `stale-if-error` directive permet CloudFront de diffuser du contenu périmé depuis le cache si l'origine est inaccessible ou renvoie un code d'erreur compris entre 500 et 600. Cela garantit que les utilisateurs peuvent accéder au contenu même en cas de panne de l'origine.

  Dans l'exemple suivant, met en CloudFront cache la réponse pendant une heure (`max-age=3600`). Si l'origine est en panne ou renvoie une erreur après cette période, le contenu périmé CloudFront continue à être diffusé pendant 24 heures au maximum (`stale-if-error=86400`).

  ```
  Cache-Control: max-age=3600, stale-if-error=86400
  ```

  > **Note**
  >
  > Lorsque des réponses d'erreur personnalisées `stale-if-error` et à la fois sont configurées, essayez d' CloudFront abord de diffuser le contenu périmé si une erreur est détectée dans le délai spécifié`stale-if-error`. Si le contenu périmé n'est pas disponible ou si la `stale-if-error` durée du contenu est dépassée, CloudFront les réponses d'erreur personnalisées configurées pour le code d'état d'erreur correspondant sont envoyées.

Utilisez les deux ensemble

`stale-while-revalidate` et `stale-if-error` sont des directives de contrôle du cache indépendantes qui peuvent être utilisées ensemble pour réduire la latence et ajouter une mémoire tampon permettant à votre origine de répondre ou de récupérer.

Dans l'exemple suivant, met en CloudFront cache la réponse pendant une heure (`max-age=3600`). Si une demande est faite après cette période, CloudFront diffuse le contenu périmé pendant 10 minutes maximum (`stale-while-revalidate=600`) pendant la revalidation du contenu. Si le serveur d'origine renvoie une erreur alors qu'il CloudFront tente de revalider le contenu, il CloudFront continue à diffuser le contenu périmé pendant 24 heures au maximum ()`stale-if-error=86400`.

```
Cache-Control: max-age=3600, stale-while-revalidate=600, stale-if-error=86400
```

> **Tip**
>
> La mise en cache est un équilibre entre performance et actualisation. L'utilisation de directives telles que `stale-while-revalidate` et `stale-if-error` peut améliorer les performances et l'expérience utilisateur, mais vérifiez que les configurations correspondent à l'actualisation souhaitée pour votre contenu. Les directives de contenu obsolètes conviennent mieux aux cas d'utilisation où le contenu doit être actualisé, mais où il n'est pas essentiel de disposer de la dernière version. De plus, si votre contenu ne change pas ou change rarement, `stale-while-revalidate` peut ajouter des demandes réseau inutiles. Envisagez plutôt de définir une durée de cache longue.

Spécifiez la durée de mise en CloudFront cache des objets

Pour contrôler la durée pendant laquelle un objet CloudFront est conservé dans le cache avant d'envoyer une autre demande à l'origine, vous pouvez :

- Définissez les valeurs TTL minimale, maximale et par défaut dans le comportement du cache d'une CloudFront distribution. Vous pouvez définir ces valeurs dans une politique de cache associée au comportement de cache (recommandé) ou dans les paramètres de cache hérités.
- inclure l'en-tête `Cache-Control` ou `Expires` dans les réponses de l'origine. Ces en-têtes permettent également de déterminer la durée pendant laquelle un navigateur conserve un objet dans le cache du navigateur avant d'envoyer une autre demande à CloudFront.

Le tableau suivant explique comment les en-têtes `Cache-Control` et `Expires` envoyés à partir de l'origine fonctionnent avec les paramètres TTL dans un comportement de cache pour affecter la mise en cache.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute une directive **`Cache-Control: max-age`** à l'objet	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur la plus faible entre la valeur de la `Cache-Control: max-age` directive ou la valeur TTL CloudFront maximale. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la directive `Cache-Control: max-age`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de la directive : `Cache-Control max-age` • Si le TTL minimum est `max-age` < le TTL maximum, l'objet est mis en CloudFront cache pour la valeur de la directive. `Cache-Control: max-age` • Si le TTL est `max-age` inférieur au minimum, l'objet est mis en CloudFront cache pour la valeur du TTL CloudFront minimum. • Si `max-age` > TTL maximal, met en CloudFront cache l'objet pour la valeur du TTL CloudFront maximal. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
		directive `Cache-Control: max-age`.
L'origine n'ajoute pas de directive **`Cache-Control: max-age`** à l'objet	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur du TTL CloudFront par défaut. Conservation en cache par les navigateurs Dépend du navigateur.	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur la plus élevée entre le TTL CloudFront minimum ou le TTL par défaut. Conservation en cache par les navigateurs Dépend du navigateur.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute les directive s **`Cache-Control: max-age`** et **`Cache-Control: s-maxage`** à l'objet	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur la plus faible entre la valeur de la `Cache-Control: s-maxage` directive ou la valeur TTL CloudFront maximale. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la directive `Cache-Control max-age`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de la directive : `Cache-Control: s-maxage` • Si le TTL minimum est `s-maxage` < le TTL maximum, l'objet est mis en CloudFront cache pour la valeur de la directive. `Cache-Control: s-maxage` • Si le TTL est `s-maxage` inférieur au minimum, l'objet est mis en CloudFront cache pour la valeur du TTL CloudFront minimum. • Si `s-maxage` > TTL maximal, met en CloudFront cache l'objet pour la valeur du TTL CloudFront maximal. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
		directive `Cache-Control: max-age`.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute un en-tête **`Expires`**à l'objet	CloudFront mise en cache CloudFront met en cache l'objet jusqu'à la date indiquée dans l'`Expires`en-tête ou jusqu'à la valeur du TTL CloudFront maximal, selon la première de ces deux dates. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache jusqu'à la date indiquée dans l'en-tête `Expires`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de l'en-tête : `Expires` • Si le TTL minimum est `Expires` < le TTL maximum, l'objet est mis en CloudFront cache jusqu'à la date et à l'heure indiquées dans l'en-tête. `Expires` • Si le TTL est `Expires` inférieur au minimum, l'objet est mis en CloudFront cache pour la valeur du TTL CloudFront minimum. • Si `Expires` > TTL maximal, met en CloudFront cache l'objet pour la valeur du TTL CloudFront maximal. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache jusqu'à la date et l'heure indiquées dans l'en-tête `Expires`.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute les directive s **`Cache-Control: no-cache`**, **`no-store`** et/ou **`private`** à l'objet	CloudFront et les navigateurs respectent les en-têtes.	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur TTL CloudFront minimale. Voir l'avertissement en dessous de ce tableau. Conservation en cache par les navigateurs Les navigateurs respectent les en-têtes.

Warning

Si votre TTL minimum est supérieur à 0, CloudFront utilise le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cache` `no-store`, et/ou sont présentes dans les en-têtes d'origine.
Si l'origine est accessible, CloudFront récupère l'objet depuis l'origine et le renvoie au visualiseur.
Si l'origine est inaccessible et que la valeur TTL minimale ou maximale est supérieure à 0, CloudFront servira l'objet obtenu précédemment par l'origine.
Pour éviter ce comportement, incluez la directive `Cache-Control: stale-if-error=0` avec l'objet renvoyé de l'origine. Cela CloudFront entraîne le renvoi d'une erreur en réponse aux futures demandes si l'origine est inaccessible, plutôt que de renvoyer l'objet obtenu précédemment.

Pour plus d'informations sur la façon de modifier les paramètres des distributions à l'aide de la CloudFront console, consultezMettre à jour une distribution. Pour plus d'informations sur la modification des paramètres des distributions à l'aide de l' CloudFront API, consultez UpdateDistribution.

Ajoutez des en-têtes à vos objets à l'aide de la console Amazon S3

Pour ajouter un champ d'en-tête **`Cache-Control`** ou **`Expires`** aux objets Amazon S3 à l'aide de la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste des compartiments, sélectionnez le nom du compartiment contenant les fichiers auxquels vous ajoutez des en-têtes.
3. Sélectionnez la case à cocher située à côté du nom du fichier ou du dossier auquel vous ajoutez des en-têtes. L'ajout d'en-têtes sur un dossier impacte tous les fichiers contenus dans ce dossier.
4. Sélectionnez Actions, puis Edit metadata (Modifier les métadonnées).
5. Dans le panneau Add metadata (Ajouter des métadonnées), procédez comme suit :
   a. Sélectionnez Add metadata (Ajouter des métadonnées).
   b. DansType, choisissez System defined (Défini par le système).
   c. Dans Key (Clé), choisissez le nom de l'en-tête que vous ajoutez (Cache-Control ou Expires).
   d. Dans Value (Valeur), entrez une valeur d'en-tête. Par exemple, pour une en-tête `Cache-Control`, vous pouvez entrer `max-age=86400`. Pour `Expires`, vous pouvez entrer une date et une heure d'expiration comme `Wed, 30 Jun 2021 09:28:00 GMT`.
6. Au bas de la page, sélectionnez Edit metadata (Modifier les métadonnées).

Contenu du cache basé sur les paramètres de chaîne de requête

Certaines applications web utilisent des chaînes de requête pour envoyer des informations à l'origine. Une chaîne de requête est la partie d'une requête web qui s'affiche après un caractère ? ; la chaîne peut contenir un ou plusieurs paramètres séparés par des caractères &. Dans l'exemple suivant, la chaîne de requête comprend deux paramètres, *`color=red`* et *`size=large`* :

`https://d111111abcdef8.cloudfront.net/images/image.jpg?`*`color=red&size=large`*

Pour les distributions, vous pouvez choisir de transférer les chaînes de requête CloudFront vers votre origine et de mettre en cache votre contenu en fonction de tous les paramètres ou des paramètres sélectionnés. Pourquoi est-ce utile ? Prenez l'exemple de code suivant.

Supposons que votre site web soit disponible en cinq langues. La structure du répertoire et les noms de fichier des cinq versions du site web sont identiques. Lorsqu'un utilisateur consulte votre site

Web, les demandes sont transmises pour CloudFront inclure un paramètre de chaîne de requête de langue basé sur la langue choisie par l'utilisateur. Vous pouvez configurer CloudFront pour transférer les chaînes de requête vers l'origine et vers le cache en fonction du paramètre de langue. Si vous configurez votre serveur Web pour renvoyer la version d'une page donnée correspondant à la langue sélectionnée, met en CloudFront cache chaque version de langue séparément, en fonction de la valeur du paramètre de chaîne de requête de langue.

Dans cet exemple, si la page principale de votre site Web est`main.html`, les cinq requêtes suivantes sont mises en CloudFront cache `main.html` cinq fois, une fois pour chaque valeur du paramètre de chaîne de requête de langue :

- `https://d111111abcdef8.cloudfront.net/main.html?language=de`
- `https://d111111abcdef8.cloudfront.net/main.html?language=en`
- `https://d111111abcdef8.cloudfront.net/main.html?language=es`
- `https://d111111abcdef8.cloudfront.net/main.html?language=fr`
- `https://d111111abcdef8.cloudfront.net/main.html?language=jp`

Notez ce qui suit :

- Certains serveurs HTTP ne traitent pas les paramètres des chaînes de requête et ne renvoient donc pas de versions différentes d'un objet basé sur les valeurs des paramètres. Pour ces origines, si vous configurez pour CloudFront transférer les paramètres de chaîne de requête vers l'origine, les mises en cache CloudFront restent basées sur les valeurs des paramètres, même si l'origine renvoie des versions identiques de l'objet CloudFront pour chaque valeur de paramètre.
- Pour que les paramètres de chaîne de requête fonctionnent comme décrit dans l'exemple ci-dessus avec les langues, vous devez utiliser le caractère & comme délimiteur entre les paramètres de chaîne de requête. Si vous utilisez un autre délimiteur, vous risquez d'obtenir des résultats inattendus, en fonction des paramètres que vous spécifiez comme base de mise en cache et de l'ordre dans lequel les paramètres apparaissent dans la chaîne de requête. CloudFront

  Les exemples suivants montrent ce qui se passe si vous utilisez un autre délimiteur et que vous configurez CloudFront le cache uniquement en fonction du `color` paramètre :

  - Dans la requête suivante, met en CloudFront cache votre contenu en fonction de la valeur du `color` paramètre, mais CloudFront interprète la valeur comme *`rouge ;`* size=large :

    ```
    https://d111111abcdef8.cloudfront.net/images/
    image.jpg?color=red;size=large
    ```

- Dans la demande suivante, met en CloudFront cache votre contenu mais ne base pas la mise en cache sur les paramètres de la chaîne de requête. Cela est dû CloudFront au fait que vous avez configuré le cache en fonction du `color` paramètre, mais que CloudFront vous interprétez la chaîne suivante comme contenant uniquement un `size` paramètre dont la valeur est *`grande ; color=red`* :

  ```
  https://d111111abcdef8.cloudfront.net/images/
  image.jpg?size=large;color=red
  ```

Vous pouvez configurer CloudFront pour effectuer l'une des opérations suivantes :

- Ne réachemine pas du tout les chaînes de requête vers l'origine. Si vous ne transférez pas les chaînes de requête, CloudFront il n'est pas mis en cache en fonction des paramètres des chaînes de requête.
- Réachemine les chaînes de requête vers l'origine et mette en cache en fonction de tous les paramètres de la chaîne de requête.
- Réachemine les chaînes de requête vers l'origine et mette en cache en fonction des paramètres spécifiés de la chaîne de requête.

Pour plus d'informations, consultez the section called “Optimisation de la mise en cache”.

Rubriques

- Paramètres de console et d'API pour le réacheminement et la mise en cache des chaînes de requête
- Optimisation de la mise en cache
- Paramètres de chaîne de requête et journaux CloudFront standard (journaux d'accès)

Paramètres de console et d'API pour le réacheminement et la mise en cache des chaînes de requête

Pour configurer le transfert et la mise en cache des chaînes de requête dans la CloudFront console, consultez les paramètres suivants dans the section called “Paramètres de distribution” :

- the section called “Réacheminement et mise en cache des chaînes de requête”
- the section called “Liste d'autorisation des chaînes de requête”

Pour configurer le transfert et la mise en cache des chaînes de requête avec l' CloudFront API, consultez les paramètres suivants dans DistributionConfiget DistributionConfigWithTagsdans le Amazon CloudFront API Reference :

- `QueryString`
- `QueryStringCacheKeys`

Optimisation de la mise en cache

Lorsque vous configurez CloudFront le cache en fonction des paramètres de chaîne de requête, vous pouvez suivre les étapes suivantes pour réduire le nombre de demandes CloudFront transmises à votre origine. Lorsque les emplacements CloudFront périphériques desservent des objets, vous réduisez la charge sur votre serveur d'origine et la latence, car les objets sont servis depuis des emplacements plus proches de vos utilisateurs.

Mettre en cache uniquement sur des paramètres pour lesquels votre origine renvoie des versions différentes d'un objet

Pour chaque paramètre de chaîne de requête vers lequel votre application Web transmet CloudFront, CloudFront transmet les demandes à votre origine pour chaque valeur de paramètre et met en cache une version distincte de l'objet pour chaque valeur de paramètre. Ceci est le cas même si votre origine renvoie toujours le même objet quelle que soit la valeur du paramètre. Dans le cas de plusieurs paramètres, le nombre de requêtes et le nombre d'objets sont multipliés.

Nous vous recommandons de CloudFront configurer la mise en cache uniquement en fonction des paramètres de chaîne de requête pour lesquels votre origine renvoie différentes versions, et d'examiner attentivement les avantages de la mise en cache en fonction de chaque paramètre. Par exemple, supposons que vous ayez un site web de vente au détail. Vous présentez les photos d'une veste dans six couleurs différentes et cette veste est disponible dans 10 tailles. Les photos que vous affichez pour la veste montrent les différentes couleurs proposées, mais pas les différentes tailles. Pour optimiser la mise en cache, vous CloudFront devez configurer la mise en cache uniquement en fonction du paramètre de couleur, et non du paramètre de taille. Cela augmente la probabilité de CloudFront répondre à une demande depuis le cache, ce qui améliore les performances et réduit la charge sur votre origine.

Toujours répertorier les paramètres dans le même ordre

L'ordre des paramètres a de l'importance dans les chaînes de requête. Dans l'exemple suivant, les chaînes de requête sont identiques, mais les paramètres sont dans un ordre différent. Cela

CloudFront entraîne le transfert de deux requêtes distinctes pour image.jpg à votre origine et la mise en cache de deux versions distinctes de l'objet :

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red&size=large`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large&color=red`

Nous vous recommandons de toujours utiliser le même ordre pour la liste des noms de paramètres, par exemple l'ordre alphabétique.

Toujours utiliser la même casse pour les noms et les valeurs des paramètres

CloudFront prend en compte le cas des noms et des valeurs des paramètres lors de la mise en cache basée sur les paramètres des chaînes de requête. Dans l'exemple suivant, les chaînes de requête sont identiques sauf dans le cas des noms et des valeurs des paramètres. Cela CloudFront entraîne le transfert de quatre requêtes distinctes pour image.jpg à votre origine et la mise en cache de quatre versions distinctes de l'objet :

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=Red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?Color=red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?Color=Red`

Nous vous recommandons d'utiliser systématiquement la même casse pour les noms et valeurs des paramètres, par exemple des minuscules.

N'utilisez pas de noms de paramètres qui soient en conflit avec les URL signées

Si vous utilisez des URL signées pour restreindre l'accès à votre contenu (si vous avez ajouté des signataires de confiance à votre distribution), CloudFront supprimez les paramètres de chaîne de requête suivants avant de transférer le reste de l'URL vers votre source :

- `Expires`
- `Key-Pair-Id`
- `Policy`
- `Signature`

Si vous utilisez des URL signées et que vous souhaitez les configurer pour transférer les chaînes de requête CloudFront vers votre origine, les paramètres de vos propres chaînes de requête ne peuvent pas être nommés `Expires`,`Key-Pair-Id`,`Policy`, ou`Signature`.

Paramètres de chaîne de requête et journaux CloudFront standard (journaux d'accès)

Si vous activez la journalisation, CloudFront enregistre l'URL complète, y compris les paramètres de la chaîne de requête. Cela est vrai, que vous ayez ou non configuré pour CloudFront transmettre les chaînes de requête à l'origine. Pour plus d'informations sur la CloudFront journalisation, consultezthe section called “Utilisation des journaux standard (journaux d’accès)”.

Contenu du cache basé sur les cookies

Par défaut, les cookies CloudFront ne sont pas pris en compte lors du traitement des demandes et des réponses, ni lors de la mise en cache de vos objets dans des emplacements périphériques. S'il CloudFront reçoit deux demandes identiques à l'exception du contenu de l'`Cookie`en-tête, il CloudFront traite par défaut les demandes comme identiques et renvoie le même objet pour les deux demandes.

Vous pouvez configurer CloudFront pour transférer à votre origine une partie ou la totalité des cookies contenus dans les requêtes des utilisateurs, et pour mettre en cache des versions distinctes de vos objets en fonction des valeurs des cookies transférés. Dans ce cas, CloudFront utilise une partie ou la totalité des cookies contenus dans les demandes du lecteur, quels que soient ceux pour lesquels le transfert est configuré, afin d'identifier de manière unique un objet dans le cache.

Par exemple, supposons que des demandes pour `locations.html` contiennent un cookie `country` ayant la valeur uk ou `fr`. Lorsque vous configurez CloudFront la mise en cache de vos objets en fonction de la valeur du `country` cookie, que CloudFront vous transmettez les demandes `locations.html` à l'origine et que vous incluez le `country` cookie et sa valeur. Votre origine renvoie `locations.html` et met en CloudFront cache l'objet une fois pour les requêtes contenant la valeur du `country` cookie uk et une fois pour les requêtes contenant cette valeur. `fr`

> **Important**
>
> Amazon S3 et certains serveurs HTTP ne gèrent pas les cookies. Ne configurez pas CloudFront pour transférer les cookies vers une origine qui ne traite pas les cookies ou dont la réponse ne varie pas en fonction des cookies. Cela peut CloudFront entraîner le transfert d'un plus grand nombre de demandes vers l'origine pour le même objet, ce qui ralentit les performances et augmente la charge sur l'origine. Si, dans l'exemple précédent, votre origine ne traite pas le `country` cookie ou renvoie toujours la même version de `locations.html`

to, CloudFront quelle que soit la valeur du `country` cookie, ne configurez pas CloudFront pour transférer ce cookie.
À l'inverse, si votre origine personnalisée dépend d'un cookie en particulier ou envoie des réponses différentes en fonction d'un cookie, assurez-vous de configurer le transfert de ce cookie CloudFront vers l'origine. Dans le cas contraire, CloudFront supprimez le cookie avant de transmettre la demande à votre source.

Pour configurer la transmission des cookies, vous mettez à jour le comportement du cache de votre distribution. Pour de plus amples informations sur les comportements de cache, consultez Paramètres de comportement du cache, en particulier les sections Réacheminer les cookies et Cookies de la liste d'autorisation.

Vous pouvez configurer chaque comportement de cache pour effectuer l'une des opérations suivantes :

- Transférer tous les cookies vers votre source : CloudFront inclut tous les cookies envoyés par le spectateur lorsqu'il transmet des demandes à l'origine. Lorsque votre origine renvoie une réponse, elle la met en CloudFront cache en utilisant les noms et les valeurs des cookies figurant dans la demande du lecteur. Si la réponse d'origine inclut `Set-Cookie` des en-têtes, elle les CloudFront renvoie au visualiseur avec l'objet demandé. CloudFront met également en cache `Set-Cookie` les en-têtes avec l'objet renvoyé par l'origine et envoie ces `Set-Cookie` en-têtes aux spectateurs à chaque accès au cache.
- Transférer un ensemble de cookies que vous spécifiez : CloudFront supprime tous les cookies envoyés par le spectateur qui ne figurent pas sur la liste d'autorisation avant de transmettre une demande à l'origine. CloudFront met en cache la réponse en utilisant les noms et les valeurs des cookies répertoriés dans la demande du visualiseur. Si la réponse d'origine inclut `Set-Cookie` des en-têtes, elle les CloudFront renvoie au visualiseur avec l'objet demandé. CloudFront met également en cache `Set-Cookie` les en-têtes avec l'objet renvoyé par l'origine et envoie ces `Set-Cookie` en-têtes aux spectateurs à chaque accès au cache.

  Pour plus d'informations sur la spécification de caractères génériques dans des noms des cookies, consultez Cookies de la liste d'autorisation.

  Pour déterminer le quota actuel concernant le nombre de noms de cookies que vous pouvez transférer pour chaque comportement de cache ou pour demander un quota supérieur, consultez la section Quotas sur les chaînes de requêtes (paramètres de cache hérités).

- Ne transférez pas les cookies vers votre source : CloudFront ne met pas en cache vos objets en fonction du cookie envoyé par le spectateur. En outre, CloudFront supprime les cookies avant de transférer les demandes à votre source et supprime les `Set-Cookie` en-têtes des réponses avant de renvoyer les réponses à vos spectateurs. Comme il ne s'agit pas d'une manière optimale d'utiliser vos ressources d'origine, lorsque vous sélectionnez ce comportement de cache, vous devez vous assurer que votre origine n'inclut pas de cookies dans les réponses d'origine par défaut.

Remarque à propos de la spécification des cookies que vous ne souhaitez pas transmettre :

Journaux d'accès

Si vous configurez CloudFront pour enregistrer les demandes et pour enregistrer les cookies, CloudFront enregistre tous les cookies et tous les attributs des cookies, même si vous configurez pour CloudFront ne pas transférer les cookies vers votre origine ou si vous configurez CloudFront pour ne transférer que des cookies spécifiques. Pour plus d'informations sur la CloudFront journalisation, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

Sensibilité à la casse

Les noms et valeurs de cookie sont sensibles à la casse. Par exemple, s'il CloudFront est configuré pour transférer tous les cookies et que deux demandes d'affichage pour le même objet contiennent des cookies identiques, sauf majuscules, CloudFront met l'objet en cache deux fois.

CloudFront trie les biscuits

S'il CloudFront est configuré pour transférer les cookies (tous ou un sous-ensemble), CloudFront trie les cookies dans l'ordre naturel par nom de cookie avant de transmettre la demande à votre origine.

`If-Modified-Since` et `If-None-Match`

`If-Modified-Since`et les demandes `If-None-Match` conditionnelles ne sont pas prises en charge lorsqu'elle CloudFront est configurée pour transférer les cookies (tous ou un sous-ensemble).

Un format standard de paire nom-valeur est requis

CloudFront transmet un en-tête de cookie uniquement si la valeur est conforme au format standard de paire nom-valeur, par exemple : `"Cookie: cookie1=value1; cookie2=value2"`

Désactiver la mise en cache des en-têtes **`Set-Cookie`**

S'il CloudFront est configuré pour transférer les cookies vers l'origine (qu'il s'agisse de tous les cookies ou de cookies spécifiques), il met également en cache `Set-Cookie` les en-têtes reçus dans la réponse d'origine. CloudFront inclut ces `Set-Cookie` en-têtes dans sa réponse au visualiseur d'origine, et les inclut également dans les réponses suivantes diffusées depuis le CloudFront cache.

Si vous souhaitez recevoir des cookies à l'origine, mais que vous ne voulez pas CloudFront mettre en cache `Set-Cookie` les en-têtes dans les réponses de votre origine, configurez votre origine pour ajouter un `Cache-Control` en-tête avec une `no-cache` directive spécifiant un `Set-Cookie` nom de champ. Par exemple: `Cache-Control: no-cache="Set-Cookie"`. Pour de plus amples informations, consultez Response Cache-Control Directives dans le standard Hypertext Transfer Protocol (HTTP/1.1): mise en cache.

Longueur maximum des noms de cookie

Si vous configurez CloudFront pour transférer des cookies spécifiques vers votre origine, le nombre total d'octets de tous les noms de cookies que vous configurez CloudFront pour le transfert ne peut pas dépasser 512 moins le nombre de cookies que vous transférez. Par exemple, si vous configurez CloudFront pour transférer 10 cookies vers votre origine, la longueur combinée des noms des 10 cookies ne peut pas dépasser 502 octets (512 à 10).

Si vous configurez CloudFront pour transférer tous les cookies vers votre origine, la longueur des noms des cookies n'a pas d'importance.

Pour plus d'informations sur l'utilisation de la CloudFront console pour mettre à jour une distribution CloudFront afin de transférer les cookies à l'origine, consultezMettre à jour une distribution. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

Contenu du cache basé sur les en-têtes des demandes

CloudFront vous permet de choisir si vous souhaitez transférer les en-têtes CloudFront vers votre origine et mettre en cache des versions distinctes d'un objet spécifique en fonction des valeurs d'en-tête figurant dans les demandes des utilisateurs. Cela vous permet de servir des versions différentes de votre contenu selon l'appareil employé par l'utilisateur, l'emplacement de l'utilisateur, la langue utilisée par l'utilisateur et différents autres critères.

Rubriques

En-têtes et distributions web : présentation

Par défaut, les en-têtes CloudFront ne sont pas pris en compte lors de la mise en cache de vos objets dans des emplacements périphériques. Si votre origine renvoie deux objets et qu'ils ne diffèrent que par les valeurs des en-têtes de demande, met en CloudFront cache une seule version de l'objet.

Vous pouvez configurer CloudFront pour transférer les en-têtes vers l'origine, ce qui entraîne la mise CloudFront en cache de plusieurs versions d'un objet en fonction des valeurs d'un ou de plusieurs en-têtes de demande. CloudFront Pour configurer la mise en cache des objets en fonction des valeurs d'en-têtes spécifiques, vous devez spécifier les paramètres de comportement du cache pour votre distribution. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de requête sélectionnés.

Par exemple, supposons que des demandes d'utilisateur pour `logo.jpg` contiennent un en-tête `Product` personnalisé ayant la valeur `Acme` ou `Apex`. Lorsque vous configurez CloudFront pour mettre en cache vos objets en fonction de la valeur de l'`Product`en-tête, transférez CloudFront les demandes `logo.jpg` à l'origine et incluez les valeurs de l'`Product`en-tête et de l'en-tête. CloudFront met en cache `logo.jpg` une fois pour les demandes dans lesquelles se trouve la valeur de l'`Product`en-tête `Acme` et une fois pour les demandes dans lesquelles la valeur est`Apex`.

Vous pouvez configurer chaque comportement de cache d'une distribution pour exécuter l'une des opérations suivantes :

- Transmettre tous les en-têtes à votre origine

> **Note**
>
> Pour les anciens paramètres de cache : si vous configurez CloudFront pour transférer tous les en-têtes vers votre origine, les objets associés à ce comportement de cache CloudFront ne sont pas mis en cache. Par contre, il envoie chaque demande à l'origine.

- Transférez la liste des en-têtes que vous spécifiez. CloudFront met en cache vos objets en fonction des valeurs de tous les en-têtes spécifiés. CloudFront transmet également les en-têtes qu'il transmet par défaut, mais il met en cache vos objets uniquement en fonction des en-têtes que vous spécifiez.
- Transmettre uniquement les en-têtes par défaut. Dans cette configuration, vos objets CloudFront ne sont pas mis en cache en fonction des valeurs contenues dans les en-têtes de demande.

Pour obtenir le quota actuel relatif au nombre d'en-têtes que vous pouvez transférer pour chaque comportement de cache ou pour demander un quota supérieur, consultez la section Quotas sur les en-têtes.

Pour plus d'informations sur l'utilisation de la CloudFront console pour mettre à jour une distribution afin CloudFront de transférer les en-têtes à l'origine, consultezMettre à jour une distribution. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour une distribution existante, consultez Mettre à jour la distribution dans le manuel Amazon CloudFront API Reference.

Sélectionnez les en-têtes sur lesquels baser la mise en cache

Les en-têtes que vous pouvez transférer vers l'origine et sur lesquels CloudFront repose la mise en cache varient selon que votre origine est un compartiment Amazon S3 ou une origine personnalisée.

- Amazon S3 — Vous pouvez configurer CloudFront pour transférer et mettre en cache vos objets en fonction d'un certain nombre d'en-têtes spécifiques (voir la liste d'exceptions suivante). Toutefois, nous vous recommandons d'éviter de transférer des en-têtes avec une origine Amazon S3, sauf si vous devez implémenter le partage des ressources cross-origin (CORS) ou que vous souhaitez personnaliser du contenu en utilisant Lambda@Edge dans les événements axés sur l'origine.

  - Pour configurer CORS, vous devez transférer des en-têtes qui permettent CloudFront de distribuer du contenu pour les sites Web activés pour le partage de ressources entre origines (CORS). Pour plus d'informations, consultez Configurer CloudFront pour respecter les paramètres CORS.
  - Pour personnaliser le contenu en utilisant des en-têtes que vous transférez vers votre origine Amazon S3, vous écrivez et ajoutez des fonctions Lambda @Edge et vous les associez à CloudFront votre distribution pour qu'elles soient déclenchées par un événement lié à l'origine. Pour plus d'informations sur l'utilisation des en-têtes afin de personnaliser du contenu, consultez Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples.

    Nous vous recommandons d'éviter de transférer des en-têtes que vous n'utilisez pas pour personnaliser du contenu, car le transfert d'en-têtes supplémentaires peut réduire votre taux d'accès au cache. En d'autres termes, il ne CloudFront peut pas répondre à autant de demandes provenant des caches périphériques par rapport à l'ensemble des demandes.
- Origine personnalisée — Vous pouvez configurer le cache CloudFront en fonction de la valeur de n'importe quel en-tête de demande, à l'exception de ce qui suit :
  - `Connection`
  - `Cookie` – Si vous souhaitez effectuer la transmission et la mise en cache en fonction de cookies, vous utilisez un paramètre distinct dans votre distribution. Pour plus d'informations, consultez Contenu du cache basé sur les cookies.
  - `Host (for Amazon S3 origins)`
  - `Proxy-Authorization`
  - `TE`
  - `Upgrade`

  Vous pouvez configurer CloudFront pour mettre en cache des objets en fonction des valeurs `User-Agent` des en-têtes `Date` et, mais nous ne le recommandons pas. Ces en-têtes ont de nombreuses valeurs possibles, et la mise en cache basée sur leurs valeurs peut entraîner le transfert d'un plus grand nombre de demandes CloudFront vers votre origine.

Pour obtenir la liste complète des en-têtes de requête HTTP et leur mode CloudFront de traitement, consultezEn-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3).

Configurer CloudFront pour respecter les paramètres CORS

Si vous avez activé le partage des ressources cross-origin (CORS) dans un compartiment Amazon S3 ou une origine personnalisée, vous devez choisir des en-têtes spécifiques à transmettre pour respecter les paramètres CORS. Les en-têtes que vous devez transférer diffèrent en fonction de l'origine (Amazon S3 ou origine personnalisée) et selon que vous souhaitez ou non mettre en cache les réponses `OPTIONS`.

Amazon S3

- Si vous souhaitez que les réponses `OPTIONS` soient mises en cache, procédez comme suit :
  - Choisissez les options pour les paramètres de comportement de cache par défaut qui permettent la mise en cache pour les réponses `OPTIONS`.
  - Configurez CloudFront pour transférer les en-têtes suivants : `OriginAccess-Control-Request-Headers`, et`Access-Control-Request-Method`.
- Si vous ne souhaitez pas que `OPTIONS` les réponses soient mises en cache, configurez CloudFront pour transférer l'`Origin`en-tête, ainsi que tous les autres en-têtes requis par votre origine (par exemple, `Access-Control-Request-HeadersAccess-Control-Request-Method`, ou autres).

Origines personnalisées – Transmettez l'en-tête `Origin` en même temps que tous les autres en-têtes requis par votre origine.

CloudFront Pour configurer la mise en cache des réponses basées sur CORS, vous devez configurer CloudFront pour transférer les en-têtes à l'aide d'une politique de cache. Pour plus d'informations, consultez Contrôlez la clé de cache à l'aide d'une politique.

Pour plus d'informations sur CORS et Amazon S3, consultez la section Utilisation du partage des ressources cross-origin (CORS) du Guide de l'utilisateur Amazon Simple Storage Service.

Configuration de la mise en cache en fonction du type d'appareil

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de l'appareil utilisé par l'utilisateur pour afficher votre contenu, configurez CloudFront pour transférer les en-têtes applicables vers votre origine personnalisée :

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`

- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

Sur la base de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes `false` avant `true` ou avant le transfert de la demande à votre origine. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront vous pouvez définir les deux options `CloudFront-Is-Mobile-Viewer` et la valeur `CloudFront-Is-Tablet-Viewer` sur`true`.

Configurer la mise en cache en fonction de la langue du visualiseur

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de la langue spécifiée dans la demande, configurez CloudFront pour transmettre l'`Accept-Language`en-tête à votre origine.

Configurer la mise en cache en fonction de l'emplacement du visualiseur

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction du pays d'origine de la demande, configurez CloudFront pour transférer l'`CloudFront-Viewer-Country`en-tête à votre origine. CloudFront convertit automatiquement l'adresse IP d'où provient la demande en un code de pays à deux lettres. Pour une easy-to-use liste des codes de pays, triable par code et par nom de pays, voir l'entrée de Wikipédia ISO 3166-1 alpha-2.

Configurer la mise en cache en fonction du protocole de la demande

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction du protocole de la demande, HTTP ou HTTPS, configurez CloudFront pour transférer l'`CloudFront-Forwarded-Proto`en-tête à votre origine.

Configuration de la mise en cache pour les fichiers compressés

Si votre origine prend en charge la compression Brotli, vous pouvez effectuer une mise en cache en fonction de l'en-tête `Accept-Encoding`. Configurez la mise en cache en fonction de `Accept-Encoding` uniquement si votre origine traite différents contenus selon l'en-tête.

Incidence de la mise en cache basée sur les en-têtes sur les performances

Lorsque vous configurez CloudFront le cache en fonction d'un ou de plusieurs en-têtes et que les en-têtes ont plusieurs valeurs possibles, CloudFront transfère davantage de demandes à votre

serveur d'origine pour le même objet. Ceci ralentit les performances et augmente la charge sur votre serveur d'origine. Si votre serveur d'origine renvoie le même objet quelle que soit la valeur d'un en-tête donné, nous vous recommandons de ne pas CloudFront configurer le cache en fonction de cet en-tête.

Si vous configurez CloudFront pour transférer plusieurs en-têtes, l'ordre des en-têtes dans les demandes des utilisateurs n'affecte pas la mise en cache tant que les valeurs sont identiques. Par exemple, si une demande contient les en-têtes A:1, B:2 et qu'une autre demande contient B:2, A:1, une seule copie de l'objet est mise en CloudFront cache.

Impact de la casse des en-têtes et des valeurs d'en-tête sur la mise en cache

Lors de la CloudFront mise en cache basée sur les valeurs d'en-tête, il ne prend pas en compte le cas du nom de l'en-tête, mais le cas de la valeur de l'en-tête :

- Si les demandes de l'utilisateur incluent les deux`product:Acme`, `Product:Acme` et ne met en CloudFront cache un objet qu'une seule fois. La seule différence entre les deux est la casse du nom de l'en-tête qui n'a pas d'incidence sur la mise en cache.
- Si les demandes de l'utilisateur incluent les deux `Product:Acme` et`Product:acme`, met en CloudFront cache un objet deux fois, car la valeur se trouve `Acme` dans certaines demandes et `acme` dans d'autres.

En-têtes CloudFront renvoyés au visualiseur

La configuration CloudFront pour transférer et mettre en cache les en-têtes n'a aucune incidence sur les en-têtes CloudFront renvoyés au visualiseur. CloudFront renvoie tous les en-têtes qu'il obtient depuis l'origine, à quelques exceptions près. Pour plus d'informations, consultez la rubrique applicable :

- Origines Amazon S3 — Voir En-têtes de réponse HTTP qui CloudFront suppriment ou mettent à jour.
- Origines personnalisées – Voir En-têtes de réponse HTTP qui CloudFront suppriment ou remplacent.

Contrôlez la clé de cache à l'aide d'une politique

Avec une politique de CloudFront cache, vous pouvez spécifier les en-têtes HTTP, les cookies et les chaînes de requête CloudFront inclus dans la clé de cache pour les objets mis en cache à des emplacements CloudFront périphériques. La clé de cache est l'identifiant unique de chaque objet du cache et elle détermine si la requête HTTP d'un utilisateur entraîne un accès au cache.

Un accès au cache se produit lorsqu'une demande d'utilisateur génère la même clé de cache qu'une requête précédente et que l'objet de cette clé de cache est dans le cache de l'emplacement périphérique et valide. En cas d'accès au cache, l'objet est diffusé au spectateur depuis un emplacement CloudFront périphérique, ce qui présente les avantages suivants :

- Réduction de la charge sur votre serveur d'origine
- Latence réduite pour l'utilisateur

L’inclusion de moins de valeurs dans la clé de cache augmente la probabilité d'un accès au cache. Cela peut améliorer les performances de votre site Web ou de votre application, car le taux d'accès au cache est plus élevé (une plus grande proportion de demandes de visiteurs aboutissant à un accès au cache). Pour plus d’informations, consultez Comprendre la clé de cache.

Pour contrôler la clé de cache, vous devez utiliser une politique de CloudFront cache. Vous associez une politique de cache à un ou plusieurs comportements de cache dans une CloudFront distribution.

Vous pouvez également utiliser la politique de cache pour spécifier les paramètres de durée de vie (TTL) des objets du CloudFront cache et permettre de demander et de CloudFront mettre en cache des objets compressés.

Rubriques

- Comprendre les politiques de cache
- Création de politiques de cache
- Utiliser des politiques de cache gérées
- Comprendre la clé de cache

Comprendre les politiques de cache

Vous pouvez utiliser une politique de cache pour améliorer le taux de réussite du cache en contrôlant les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans la clé de cache. CloudFrontfournit des politiques de cache prédéfinies, appelées politiques gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces politiques gérées ou créer votre propre politique de cache adaptée à vos besoins. Pour de plus amples informations sur les politiques gérées, veuillez consulter Utiliser des politiques de cache gérées.

Une politique de cache contient les paramètres suivants, qui sont classés en informations de politique, paramètres time-to-live (TTL) et paramètres de clé de cache.

Informations sur les politiques

Nom

Nom permettant d'identifier la politique de cache. Dans la console, vous utilisez le nom pour attacher la politique de cache à un comportement de cache.

Description

Commentaire décrivant la politique de cache. Cette option est facultative, mais elle peut vous aider à identifier l'objectif de la politique de cache.

Paramètres time-to-live (TTL)

Les paramètres de durée de vie (TTL) fonctionnent conjointement avec les en-têtes `Cache-Control` et `Expires` HTTP (s'ils figurent dans la réponse d'origine) pour déterminer la durée de validité des objets du CloudFront cache.

Durée de vie minimale

Durée minimale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. Pour plus d’informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Durée de vie (TTL) maximale

Durée maximale, en secondes, pendant laquelle les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. CloudFront utilise ce

paramètre uniquement lorsque l'origine envoie `Cache-Control` ou met en `Expires` en-tête l'objet. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

TTL par défaut

Durée par défaut, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. CloudFront utilise la valeur de ce paramètre comme TTL de l'objet uniquement lorsque l'origine n'envoie pas *`Cache-Control`* ou ne contient pas d'`Expires`en-têtes avec l'objet. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

> **Note**
>
> Si les paramètres TTL minimum, TTL maximum et TTL par défaut sont tous définis sur 0, la mise en cache est désactivée. CloudFront

Paramètres de la clé de cache

Les paramètres de la clé de cache spécifient les valeurs figurant dans les demandes du lecteur CloudFront incluses dans la clé de cache. Les valeurs peuvent inclure des chaînes de requête URL, des en-têtes HTTP et des cookies. Les valeurs que vous incluez dans la clé de cache sont automatiquement incluses dans les demandes CloudFront envoyées à l'origine, appelées demandes d'origine. Pour de plus amples informations sur le contrôle des demandes d'origine sans affecter la clé de cache, veuillez consulter Contrôlez les demandes d'origine à l'aide d'une politique.

Les paramètres de clé de cache incluent :

- En-têtes
- Cookies
- Chaînes de requête
- Prise en charge de la compression

En-têtes

Les en-têtes HTTP dans les demandes du lecteur, CloudFront y compris dans la clé de cache et dans les demandes d'origine. Pour les en-têtes, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les en-têtes HTTP dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine.
- Include the following headers (Inclure les en-têtes suivants) – Vous spécifiez quels en-têtes HTTP des demandes de l'utilisateur sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.

Lorsque vous utilisez le paramètre Include the following headers (Inclure les en-têtes suivants), vous spécifiez les en-têtes HTTP par leur nom, et non par leur valeur. Par exemple, considérez l'en-tête HTTP suivant :

```
Accept-Language: en-US,en;q=0.5
```

Dans ce cas, vous spécifiez l'en-tête comme `Accept-Language`, pas comme `Accept-Language: en-US,en;q=0.5`. Cependant, CloudFront inclut l'en-tête complet, y compris sa valeur, dans la clé de cache et dans les demandes d'origine.

Vous pouvez également inclure certains en-têtes générés par CloudFront dans la clé de cache. Pour plus d'informations, consultez the section called “Ajouter des en-têtes de CloudFront demande”.

Cookies

Les cookies contenus dans les demandes du lecteur, CloudFront y compris dans la clé de cache, et dans les demandes d'origine. Pour les cookies, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les cookies dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine.
- Tous – Tous les cookies dans les demandes de l'utilisateur sont inclus dans la clé de cache et sont automatiquement inclus dans les demandes d'origine.
- Include specified cookies (Inclure les cookies spécifiés) – Vous spécifiez quels cookies dans les demandes de l'utilisateur sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.

- Include all cookies except (Inclure tous les cookies sauf) – Vous spécifiez quels cookies dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine. Tous les autres cookies, à l'exception de ceux que vous spécifiez, sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.

Lorsque vous utilisez le paramètre Include specified cookies (Inclure les cookies spécifiés) ou Include all cookies except (Inclure tous les cookies sauf), vous spécifiez les cookies par leur nom, et non par leur valeur. Prenons l'exemple de l'en-tête `Cookie` suivant :

```
Cookie: session_ID=abcd1234
```

Dans ce cas, vous spécifiez le cookie comme `session_ID`, pas comme `session_ID=abcd1234`. Cependant, CloudFront inclut le cookie complet, y compris sa valeur, dans la clé de cache et dans les requêtes d'origine.

Chaînes de requête

Les chaînes de requête d'URL contenues dans les demandes du lecteur CloudFront incluses dans la clé de cache et dans les demandes d'origine. Pour les chaînes de requête, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les chaînes de requête dans les demandes utilisateur ne sont pas incluses dans la clé de cache et ne sont pas automatiquement incluses dans les demandes d'origine.
- Toutes – Toutes les chaînes de requête dans les demandes de l'utilisateur sont incluses dans la clé de cache et sont également automatiquement incluses dans les demandes d'origine.
- Include specified query strings (Inclure les chaînes de requête spécifiées) – Vous spécifiez quelles chaînes de requête dans les demandes de l'utilisateur sont incluses dans la clé de cache et automatiquement incluses dans les demandes d'origine.
- Include all query strings except (Inclure toutes les chaînes de requête sauf) – Vous spécifiez quelles chaînes de requête dans les demandes de l'utilisateur ne sont pas incluses dans la clé de cache et ne sont pas automatiquement incluses dans les demandes d'origine. Toutes les autres chaînes de requête, à l'exception de celles que vous spécifiez, sont incluses dans la clé de cache et automatiquement incluses dans les demandes d'origine.

Lorsque vous utilisez le paramètres Include specified query strings (Inclure les chaînes de requête spécifiées) Include all query strings except (Inclure toutes les chaînes de requête sauf), vous

spécifiez les chaînes de requête par leur nom, et non par leur valeur. Prenons l'exemple du chemin d'URL suivant :

```
/content/stories/example-story.html?split-pages=false
```

Dans ce cas, vous spécifiez la chaîne de requête comme `split-pages`, pas comme `split-pages=false`. Cependant, CloudFront inclut la chaîne de requête complète, y compris sa valeur, dans la clé de cache et dans les demandes d'origine.

Prise en charge de la compression

Ces paramètres permettent CloudFront de demander et de mettre en cache des objets compressés aux formats de compression Gzip ou Brotli, lorsque le visualiseur les prend en charge. Ces paramètres permettent également à CloudFront la compression de fonctionner. Les utilisateurs indiquent leur prise en charge de ces formats de compression avec l'en-tête `Accept-Encoding` HTTP.

> **Note**
>
> Les navigateurs web Chrome et Firefox prennent en charge la compression Brotli uniquement lorsque la demande est envoyée en HTTPS. Ces navigateurs ne prennent pas en charge Brotli avec les demandes HTTP.

Activez ces paramètres lorsque l'une des conditions suivantes est vraie :

- Votre origine renvoie des objets compressés Gzip lorsque les utilisateurs les prennent en charge (les demandes contiennent l'en-tête `Accept-Encoding` HTTP avec `gzip` comme valeur). Dans ce cas, utilisez le paramètre activé par Gzip (défini `EnableAcceptEncodingGzip` sur `true` dans l' CloudFront API AWS CLI, AWS les SDK ou AWS CloudFormation).
- Votre origine renvoie des objets compressés Brotli lorsque les utilisateurs les prennent en charge (les demandes contiennent l'en-tête `Accept-Encoding` HTTP avec `br` comme valeur). Dans ce cas, utilisez le paramètre activé par Brotli (défini `EnableAcceptEncodingBrotli` sur `true` dans l' CloudFront API AWS CLI, AWS les SDK ou). AWS CloudFormation
- Le comportement du cache auquel cette politique de cache est attachée est configuré avec CloudFrontla compression. Dans ce cas, vous pouvez activer la mise en cache pour Gzip ou

Brotli, ou les deux. Lorsque CloudFront la compression est activée, l'activation de la mise en cache pour les deux formats peut contribuer à réduire les coûts de transfert de données vers Internet.

> **Note**
>
> Si vous activez la mise en cache pour l'un de ces formats de compression ou pour les deux, n'incluez pas l'`Accept-Encoding`en-tête dans une politique de demande d'origine associée au même comportement de cache. CloudFrontinclut toujours cet en-tête dans les demandes d'origine lorsque la mise en cache est activée pour l'un ou l'autre de ces formats. L'inclusion `Accept-Encoding` dans une politique de demande d'origine n'a donc aucun effet.

Si votre serveur d'origine ne renvoie pas d'objets compressés Gzip ou Brotli, ou si le comportement du cache n'est pas configuré avec la CloudFront compression, n'activez pas la mise en cache pour les objets compressés. Si vous le faites, cela peut entraîner une diminution du taux d'accès au cache.

Ce qui suit explique comment ces paramètres affectent une CloudFront distribution. Tous les scénarios suivants supposent que la demande de l'utilisateur inclut l'en-tête `Accept-Encoding`. Lorsque la demande du visualiseur n'inclut pas l'`Accept-Encoding`en-tête, CloudFront ne l'inclut pas dans la clé de cache et ne l'inclut pas dans la demande d'origine correspondante.

Lorsque la mise en cache des objets compressés est activée pour les deux formats de compression

Si le visualiseur prend en charge à la fois Gzip et Brotli, c'est-à-dire si les `br` valeurs `gzip` et figurent toutes deux dans l'`Accept-Encoding`en-tête de la demande du visualiseur, effectue les opérations suivantes : CloudFront

- Normalise l'en-tête sur `Accept-Encoding: br,gzip` et inclut l'en-tête normalisé dans la clé de cache. La clé de cache n'inclut pas d'autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.
- Si le cache contient un objet compressé Brotli ou Gzip qui correspond à la demande et n'a pas expiré, cet emplacement renvoie l'objet à l'utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Brotli ou Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: br,gzip`) dans la demande d'origine correspondante. La demande

d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Si le visualiseur prend en charge un format de compression mais pas l'autre (par exemple, s'il s'`gzip`agit d'une valeur dans l'`Accept-Encoding`en-tête de la demande du lecteur mais ne l'`br`est pas), CloudFront effectue les opérations suivantes :

- Normalise l'en-tête sur `Accept-Encoding: gzip` et inclut l'en-tête normalisé dans la clé de cache. La clé de cache n'inclut pas d'autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.
- Si le cache contient un objet compressé Gzip qui correspond à la demande et n'a pas expiré, l'emplacement périphérique renvoie l'objet à l'utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: gzip`) dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Pour comprendre ce qui CloudFront se passe si le lecteur prend en charge Brotli mais pas Gzip, remplacez les deux formats de compression dans l'exemple précédent.

Si le lecteur ne prend pas en charge Brotli ou GZIP, c'est-à-dire que l'`Accept-Encoding`en-tête de la demande du lecteur ne contient pas de valeurs ou ne contient `br` pas de valeurs : `gzip` CloudFront

- N'inclut pas l'en-tête `Accept-Encoding` dans la clé de cache.
- Inclut `Accept-Encoding: identity` dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Lorsque la mise en cache des objets compressés est activée pour un format de compression, mais pas pour l'autre

Si le visualiseur prend en charge le format pour lequel la mise en cache est activée, par exemple, si la mise en cache des objets compressés est activée pour Gzip et que le visualiseur prend en charge Gzip (`gzip`c'est l'une des valeurs de l'`Accept-Encoding`en-tête de la demande du lecteur), procède comme suit : CloudFront

- Normalise l'en-tête sur `Accept-Encoding: gzip` et inclut l'en-tête normalisé dans la clé de cache.

- Si le cache contient un objet compressé Gzip qui correspond à la demande et n'a pas expiré, l'emplacement périphérique renvoie l'objet à l'utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: gzip`) dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Ce comportement est le même lorsque l'utilisateur prend en charge Gzip et Brotli (l'en-tête `Accept-Encoding` de la demande de l'utilisateur inclut les deux `gzip` et `br` comme valeurs), car dans ce scénario, la mise en cache des objets compressés pour Brotli n'est pas activée.

Pour comprendre ce qui CloudFront se passe si la mise en cache des objets compressés est activée pour Brotli mais pas pour Gzip, remplacez les deux formats de compression dans l'exemple précédent.

Si le lecteur ne prend pas en charge le format de compression pour lequel la mise en cache est activée (l'`Accept-Encoding`en-tête de la demande du lecteur ne contient pas la valeur correspondant à ce format), CloudFront :

- N'inclut pas l'en-tête `Accept-Encoding` dans la clé de cache.
- Inclut `Accept-Encoding: identity` dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Lorsque la mise en cache des objets compressés est désactivée pour les deux formats de compression

Lorsque la mise en cache des objets compressés est désactivée pour les deux formats de compression, CloudFront traite l'`Accept-Encoding`en-tête de la même manière que tout autre en-tête HTTP dans la demande du visualiseur. Par défaut, il n'est pas inclus dans la clé de cache et il n'est pas inclus dans les demandes de l'origine. Vous pouvez l'inclure dans la liste d'autorisation des en-têtes dans une politique de cache ou une politique de demande d'origine comme tout autre en-tête HTTP.

Création de politiques de cache

Vous pouvez utiliser une politique de cache pour améliorer votre taux d'accès au cache en contrôlant les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans la clé de cache.

Vous pouvez créer une politique de cache dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Après avoir créé une politique de cache, vous l'associez à un ou plusieurs comportements de cache dans une CloudFront distribution.

Console

Pour créer une politique de cache (console)

1. Connectez-vous à la page Politiques AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Choisissez Créer une politique de cache.
3. Choisissez le paramètre souhaité pour cette politique de cache. Pour plus d'informations, consultez Comprendre les politiques de cache.
4. Lorsque vous avez terminé, choisissez Create (Créer).

Après avoir créé une politique de cache, vous pouvez l'attacher à un comportement de cache.

Pour attacher une politique de cache à une distribution existante (console)

1. Ouvrez la page Distributions dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Comportements.
3. Choisissez le comportement du cache à mettre à jour, puis choisissez Modifier.

   Ou, pour créer un nouveau comportement de cache, choisissez Create behavior (Créer un comportement).
4. Dans la section Cache key and origin requests (Clé de cache et demandes d'origine), assurez-vous que l'option Cache policy and origin request policy (Politique de cache et politique de demande d'origine) est sélectionnée.
5. Pour Cache policy (Politique de cache), choisissez la politique de cache à attacher à ce comportement de cache.
6. Choisissez Save changes (Enregistrer les modifications) en bas de la page.

Pour attacher une politique de cache à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Dans la section Cache key and origin requests (Clé de cache et demandes d'origine), assurez-vous que l'option Cache policy and origin request policy (Politique de cache et politique de demande d'origine) est sélectionnée.
4. Pour Cache policy (Politique de cache), choisissez la politique de cache à attacher au comportement de cache par défaut de cette distribution.
5. Choisissez les paramètres souhaités pour l'origine, le comportement de cache par défaut et les autres paramètres de distribution. Pour plus d'informations, consultez Référence des paramètres de distribution.
6. Lorsque vous avez terminé, choisissez Create distribution (Créer une distribution).

CLI

Pour créer une politique de cache avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-cache-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une politique de cache (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `cache-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-cache-policy.

```
aws cloudfront create-cache-policy --generate-cli-skeleton yaml-input > cache-policy.yaml
```

2. Ouvrez le fichier nommé `cache-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de politique de cache que vous souhaitez, puis enregistrez le fichier. Vous pouvez supprimer des champs facultatifs du fichier, mais ne supprimez pas les champs obligatoires.

   Pour de plus amples informations sur les paramètres de politique de cache, veuillez consulter Comprendre les politiques de cache.

3. Utilisez la commande suivante pour créer la politique de cache à l'aide des paramètres d'entrée du fichier `cache-policy.yaml`.

```
aws cloudfront create-cache-policy --cli-input-yaml file://cache-policy.yaml
```

   Notez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de politique de cache, dont vous avez besoin pour associer la politique de cache au comportement de cache d'une CloudFront distribution.

Pour attacher une politique de cache à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour pour utiliser une politique de cache.

   - Dans le comportement du cache, ajoutez un champ nommé `CachePolicyId`. Pour la valeur du champ, utilisez l'ID de politique de cache que vous avez noté après la création de la politique.
   - Supprimez les champs `MinTTL`, `MaxTTL`, `DefaultTTL` et `ForwardedValues` du comportement du cache. Ces paramètres sont spécifiés dans la politique de cache, de sorte que vous ne pouvez pas inclure ces champs et une politique de cache dans le même comportement de cache.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la politique de cache. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une politique de cache à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml` qui contient tous les paramètres d'entrée de la commande create-distribution.

   ```
   aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
    distribution.yaml
   ```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `CachePolicyId`, entrez l'ID de politique de cache que vous avez noté après la création de la politique. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

   Pour de plus amples informations sur les paramètres de distribution, veuillez consulter Référence des paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

   ```
   aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
   ```

API

Pour créer une politique de cache avec l' CloudFront API, utilisez CreateCachePolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez Comprendre les politiques de cache la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une politique de cache, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la politique de cache dans le champ `CachePolicyId`, à l'intérieur d'un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utiliser des politiques de cache gérées

CloudFront fournit un ensemble de politiques de cache gérées que vous pouvez associer à tous les comportements de cache de votre distribution. Avec une stratégie de cache gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre stratégie de cache. Les stratégies gérées utilisent des paramètres optimisés pour des cas d'utilisation spécifiques.

Pour utiliser une stratégie de cache gérée, vous l'attachez à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une stratégie de cache, mais au lieu d'en créer une nouvelle, vous n'avez qu'à attacher l'une des stratégies de cache gérées. Vous joignez la politique soit par son nom (avec la console), soit par son identifiant (avec le AWS CLI ou les SDK). Les noms et les identifiants sont répertoriés dans la section suivante.

Pour plus d’informations, consultez Création de politiques de cache.

Les rubriques suivantes décrivent les stratégies de cache gérées que vous pouvez utiliser.

Rubriques

- Amplify
- CachingDisabled
- CachingOptimized
- CachingOptimizedForUncompressedObjects
- Élémentaire- MediaPackage
- UseOriginCacheControlHeaders
- UseOriginCacheControlHeaders-QueryStrings

Amplify

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour être utilisée avec une origine qui est une appli web AWS Amplify.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`2e54312d-136d-493c-8eb9-b001f22f67d2`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 2 secondes
- Maximum TTL (Durée de vie maximale) : 600 secondes (10 minutes)
- Default TTL (Durée de vie par défaut) : 2 secondes
- En-têtes inclus dans la clé de cache :
  - `Authorization`
  - `CloudFront-Viewer-Country`
  - `Host`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).
- Cookies included in cache key (Cookies inclus dans la clé de cache) : tous les cookies sont inclus.
- Query strings included in cache key (Chaînes de requête incluses dans la clé de cache) : toutes les chaînes de requête sont incluses.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

CachingDisabled

Afficher cette politique dans la CloudFront console

Cette stratégie désactive la mise en cache. Cette stratégie est utile pour le contenu dynamique et pour les demandes qui ne peuvent pas être mises en cache.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`4135ea2d-6df8-44a3-9df3-4b5a84be39ad`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 0 seconde
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune
- Paramètre des objets compressés du cache : Désactivé

CachingOptimized

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour optimiser l'efficacité du cache en minimisant les valeurs CloudFront incluses dans la clé de cache. CloudFront n'inclut aucune chaîne de requête ni aucun cookie dans la clé de cache et inclut uniquement l'`Accept-Encoding`en-tête normalisé. Cela permet CloudFront de mettre en cache séparément les objets aux formats de compression Gzip et Brotli lorsque l'origine les renvoie ou lorsque la compression des CloudFront bords est activée.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`658327ea-f89d-4fab-a63d-7e88639e58f6`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 1 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours).
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures).
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun n'est explicitement inclus. L'en-tête `Accept-Encoding` normalisé est inclus car le paramètre des objets

compressés du cache est activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun.
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

CachingOptimizedForUncompressedObjects

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour optimiser l'efficacité du cache en minimisant les valeurs incluses dans la clé de cache. Aucune chaîne de requête, aucun en-tête ou cookie ne sont inclus. Cette stratégie est identique à la précédente, mais elle désactive le paramètre des objets compressés du cache.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`b2884449-e4de-46a7-ac36-70bc7f1ddd6d`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 1 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures)
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune
- Paramètre des objets compressés du cache : Désactivé

Élémentaire- MediaPackage

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour être utilisée avec une origine qui est un point de terminaison AWS Elemental MediaPackage .

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`08627262-05a9-4f76-9ded-b50ca2e3a84f`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures)
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Origin`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé pour Gzip. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) :
  - `aws.manifestfilter`
  - `start`
  - `end`
  - `m`
- Cache compressed objects setting (Paramètre des objets compressés du cache) : activé pour Gzip. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

UseOriginCacheControlHeaders

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour être utilisée avec une origine qui renvoie des en-têtes de réponse `Cache-Control` HTTP et ne diffuse pas de contenu différent en fonction des valeurs présentes dans la chaîne de requête. Si votre origine diffuse un contenu différent en fonction des valeurs présentes dans la chaîne de requête, pensez à utiliserUseOriginCacheControlHeaders-QueryStrings.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`83da9c7e-98b4-4e11-a168-04f0df8e2c65`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).
- Cookies inclus dans la clé de cache : tous les cookies sont inclus.
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

UseOriginCacheControlHeaders-QueryStrings

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour être utilisée avec une origine qui renvoie des en-têtes de réponse `Cache-Control` HTTP et diffuse un contenu différent en fonction des valeurs présentes dans la chaîne de requête. Si votre origine ne diffuse pas de contenu différent en fonction des valeurs présentes dans la chaîne de requête, pensez à utiliserUseOriginCacheControlHeaders.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`4cc15a8a-d715-48a4-82b8-cc0b614638fe`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).
- Cookies inclus dans la clé de cache : tous les cookies sont inclus.
- Chaînes de requête incluses dans la clé de cache : toutes les chaînes de requête sont incluses.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, veuillez consulter Compression support (Prise en charge de la compression).

Comprendre la clé de cache

La clé de cache détermine si une demande d'un utilisateur à un emplacement CloudFront périphérique entraîne un accès au cache. La clé de cache est l'identifiant unique d'un objet dans le cache. Chaque objet du cache possède une clé de cache unique.

Un accès au cache se produit lorsqu'une demande d'utilisateur génère la même clé de cache qu'une requête précédente, et que l'objet de cette clé de cache est dans le cache de l'emplacement périphérique et valide. En cas d'accès au cache, l'objet demandé est diffusé au spectateur depuis un emplacement CloudFront périphérique, ce qui présente les avantages suivants :

- Réduction de la charge sur votre serveur d'origine
- Latence réduite pour l'utilisateur

Vous pouvez obtenir de meilleures performances à partir de votre site Web ou de votre application lorsque vous avez un taux d'accès au cache plus élevé (une proportion plus élevée de requêtes de visionneuse entraînant un accès au cache). Une façon d'améliorer votre taux d'accès du cache est d'inclure uniquement les valeurs minimales nécessaires dans la clé de cache. Pour plus d'informations, consultez les sections suivantes.

Vous pouvez modifier les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) dans la clé de cache à l'aide d'une stratégie de cache. (Vous pouvez également modifier la clé de cache à l'aide d'une fonction Lambda @Edge.) Avant de modifier la clé de cache, il est important de comprendre comment votre application est conçue et quand et comment elle peut servir différentes réponses en fonction des caractéristiques de la requête de la visionneuse. Lorsqu'une valeur dans la demande de visionneuse détermine la réponse renvoyée par votre origine, vous devez inclure cette valeur dans la clé de cache. Mais si vous incluez une valeur dans la clé de cache qui n'affecte pas la réponse renvoyée par votre origine, vous risquez de mettre en cache des objets en double.

Clé de cache par défaut

Par défaut, la clé de cache d'une CloudFront distribution inclut les informations suivantes :

- Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net)
- Chemin d'URL de l'objet demandé (par exemple, `/content/stories/example-story.html`)

> **Note**
>
> La méthode `OPTIONS` est incluse dans la clé de cache pour les demandes `OPTIONS`. Cela signifie que les réponses aux demandes `OPTIONS` sont mises en cache séparément des réponses aux demandes `GET` et `HEAD`.

Les autres valeurs de la demande de visionneuse ne sont pas incluses dans la clé de cache, par défaut. Examinez la requête HTTP suivante provenant d'un navigateur Web.

```
            GET /content/stories/example-story.html?ref=0123abc&split-pages=false
HTTP/1.1
            Host: d111111abcdef8.cloudfront.net
            User-Agent: Mozilla/5.0 Gecko/20100101 Firefox/68.0
            Accept: text/html,*/*
```

```
Accept-Language: en-US,en
Cookie: session_id=01234abcd
Referer: https://news.example.com/
```

Lorsqu'une requête d'utilisateur comme dans cet exemple arrive à un emplacement CloudFront périphérique, CloudFront utilise la clé de cache pour déterminer s'il y a un accès au cache. Par défaut, seuls les composants suivants de la demande sont inclus dans la clé de cache : `/content/stories/example-story.html` et `d111111abcdef8.cloudfront.net`. Si l'objet demandé n'est pas dans le cache (erreur de cache), CloudFront envoie une demande à l'origine pour obtenir l'objet. Après avoir récupéré l'objet, il le CloudFront renvoie au visualiseur et le stocke dans le cache de l'emplacement périphérique.

Lorsqu'il CloudFront reçoit une autre demande pour le même objet, telle que déterminée par la clé de cache CloudFront , envoie immédiatement l'objet mis en cache au spectateur, sans envoyer de demande à l'origine. Prenons l'exemple de la demande HTTP suivante qui vient après la demande précédente.

```
GET /content/stories/example-story.html?ref=xyz987&split-pages=true
HTTP/1.1
Host: d111111abcdef8.cloudfront.net
User-Agent: Mozilla/5.0 AppleWebKit/537.36 Chrome/83.0.4103.116
Accept: text/html,*/*
Accept-Language: en-US,en
Cookie: session_id=wxyz9876
Referer: https://rss.news.example.net/
```

Cette demande concerne le même objet que la demande précédente, mais elle est différente de la demande précédente. Il a une chaîne de requête URL différente, différents en-têtes `User-Agent` et `Referer` et un cookie `session_id` différent. Cependant, aucune de ces valeurs ne fait partie de la clé de cache par défaut, de sorte que cette deuxième demande entraîne un accès au cache.

Personnaliser la clé de cache

Dans certains cas, vous pouvez inclure plus d'informations dans la clé de cache, même si cela peut entraîner moins de visites de cache. Vous spécifiez les éléments à inclure dans la clé de cache à l'aide d'une stratégie de cache.

Par exemple, si votre serveur d'origine utilise l'en-tête HTTP `Accept-Language` dans les demandes de l'utilisateur pour renvoyer un contenu différent en fonction de la langue de l'utilisateur, vous pouvez inclure cet en-tête dans la clé de cache. Lorsque vous le faites, CloudFront utilisez cet en-tête pour déterminer les accès au cache et incluez-le dans les demandes d'origine (demandes CloudFront envoyées à l'origine en cas de perte de cache).

L'inclusion de valeurs supplémentaires dans la clé de cache CloudFront peut avoir pour conséquence de mettre en cache des objets dupliqués en raison des variations qui peuvent survenir dans les demandes des utilisateurs. Par exemple, les utilisateurs peuvent envoyer l'une des valeurs suivantes pour l'en-tête `Accept-Language` :

- `en-US,en`
- `en,en-US`
- `en-US, en`
- `en-US`

Toutes ces différentes valeurs indiquent que la langue de l'utilisateur est l'anglais, mais la variation peut CloudFront entraîner la mise en cache du même objet plusieurs fois. Cela peut réduire les accès au cache et augmenter le nombre de demandes d'origine. Vous pouvez éviter cette duplication en n'incluant pas l'en-tête `Accept-Language` dans la clé de cache et en configurant votre site Web ou votre application de manière à utiliser différentes URL pour le contenu dans différentes langues (par exemple, `/en-US/content/stories/example-story.html`).

Pour toute valeur donnée que vous avez l'intention d'inclure dans la clé de cache, vous devez vous assurer de comprendre combien de variations différentes de cette valeur peuvent apparaître dans les demandes de l'utilisateur. Pour certaines valeurs de demande, il est rarement logique de les inclure dans la clé de cache. Par exemple, l'en-tête `User-Agent` peut avoir des milliers de variations uniques, de sorte que ce n'est généralement pas un bon candidat à inclure dans la clé de cache. Les cookies qui ont des valeurs spécifiques à l'utilisateur ou à la session et qui sont uniques sur des milliers (voire des millions) de demandes ne sont pas non plus de bons candidats pour l'inclusion dans la clé de cache. Si vous incluez ces valeurs dans la clé de cache, chaque variation unique entraîne une autre copie de l'objet dans le cache. Si ces copies de l'objet ne sont pas uniques, ou si vous vous retrouvez avec un nombre si important d'objets légèrement différents que chaque objet ne reçoit qu'un petit nombre de visites de cache, vous pouvez envisager une approche différente. Vous pouvez exclure ces valeurs hautement variables de la clé de cache ou marquer des objets comme ne pouvant pas être mis en cache.

Faites preuve de prudence lors de la personnalisation de la clé de cache. Parfois, c'est souhaitable, mais cela peut avoir des conséquences inattendues telles que la mise en cache des objets en double, la réduction du taux d'accès du cache et l'augmentation du nombre de demandes d'origine. Si votre site web ou votre application d'origine doit recevoir certaines valeurs provenant des demandes de l'utilisateur pour l'analyse, la télémétrie ou d'autres utilisations, mais que ces valeurs ne modifient pas l'objet renvoyé par l'origine, utilisez une stratégie de demande d'origine pour inclure ces valeurs dans les demandes d'origine, mais ne pas les inclure dans la clé de cache.

Contrôlez les demandes d'origine à l'aide d'une politique

Lorsqu'une demande d'affichage CloudFront entraîne un échec du cache (l'objet demandé n'est pas mis en cache à l'emplacement périphérique), CloudFront envoie une demande à l'origine pour récupérer l'objet. C'est ce qu'on appelle une demande d'origine. La demande d'origine inclut toujours les informations suivantes provenant de la demande de l'utilisateur :

- Le chemin d'URL (le chemin uniquement, sans les chaînes de requête d'URL ou le nom de domaine)
- Le corps de la requête (s'il y en a un)
- Les en-têtes HTTP qui CloudFront sont automatiquement inclus dans chaque demande d'origine, notamment `HostUser-Agent`, et `X-Amz-Cf-Id`

D'autres informations provenant de la demande de l'utilisateur, telles que les chaînes de requête URL, les en-têtes HTTP et les cookies, ne sont pas incluses dans la demande d'origine par défaut. (Exception : avec les anciens paramètres de cache CloudFront , les en-têtes sont transférés par défaut vers votre origine.) Toutefois, vous pouvez demander à recevoir certaines de ces autres informations à l’origine, par exemple pour collecter des données à des fins d’analyse ou de télémétrie. Vous pouvez utiliser une stratégie de demande d'origine pour contrôler les informations incluses dans une demande d'origine.

Les stratégies de demande d'origine sont séparées des stratégies de cache, qui contrôlent la clé de cache. De cette façon, vous pouvez recevoir des informations supplémentaires dès l'origine tout en conservant un bon taux d'accès au cache (la proportion de demandes des utilisateurs aboutissant à un accès au cache). Pour ce faire, contrôlez séparément quelles informations sont incluses dans les demandes d'origine (à l'aide de la stratégie de demande d'origine) et celles qui sont incluses dans la clé de cache (à l'aide de la stratégie de cache).

Bien que les deux types de stratégie soient distincts, elles sont liées. Toutes les chaînes de requête URL, les en-têtes HTTP et les cookies que vous incluez dans la clé de cache (à l'aide d'une stratégie de cache) sont automatiquement inclus dans les requêtes d'origine. Utilisez la stratégie de demande d'origine pour spécifier les informations que vous souhaitez inclure dans les demandes d'origine, mais pas dans la clé de cache. Tout comme une politique de cache, vous associez une politique de demande d'origine à un ou plusieurs comportements de cache dans une CloudFront distribution.

Vous pouvez également utiliser une stratégie de demande d'origine pour ajouter des en-têtes HTTP supplémentaires à une demande d'origine qui n'étaient pas inclus dans la demande de l'utilisateur.

Ces en-têtes supplémentaires sont ajoutés CloudFront avant l'envoi de la demande d'origine, avec des valeurs d'en-tête qui sont déterminées automatiquement en fonction de la demande du spectateur. Pour plus d'informations, consultez the section called "Ajouter des en-têtes de CloudFront demande".

Rubriques

- Comprendre les politiques relatives aux demandes d'origine
- Création de politiques de demande d'origine
- Utiliser des politiques de demande d'origine gérées
- Ajouter des en-têtes de CloudFront demande
- Découvrez comment les politiques de demande d'origine et les politiques de cache fonctionnent ensemble

Comprendre les politiques relatives aux demandes d'origine

CloudFront fournit des politiques de demande d'origine prédéfinies, appelées politiques gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces stratégies gérées ou créer votre propre stratégie de demande d'origine spécifique à vos besoins. Pour de plus amples informations sur les politiques gérées, veuillez consulter Utiliser des politiques de demande d'origine gérées.

Une stratégie de demande d'origine contient les paramètres suivants, qui sont classés en informations de stratégie et en paramètres de demande d'origine.

Informations sur les stratégies

Nom

Nom permettant d'identifier la stratégie de demande d'origine. Dans la console, vous utilisez le nom pour attacher la stratégie de demande d'origine à un comportement de cache.

Description

Commentaire décrivant la stratégie de demande de l'origine. Facultative.

Paramètres de la demande d'origine

Les paramètres de demande d'origine spécifient les valeurs des demandes du lecteur qui sont incluses dans les demandes CloudFront envoyées à l'origine (appelées demandes d'origine). Les

valeurs peuvent inclure des chaînes de requête URL, des en-têtes HTTP et des cookies. Les valeurs que vous spécifiez sont incluses dans les demandes d'origine, mais ne sont pas incluses dans la clé de cache. Pour de plus amples informations sur le contrôle de la clé cache, veuillez consulter Contrôlez la clé de cache à l'aide d'une politique.

En-têtes

Les en-têtes HTTP dans les demandes du lecteur, CloudFront y compris dans les demandes d'origine. Pour les en-têtes, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les en-têtes HTTP des demandes de l'utilisateur ne sont pas inclus dans les demandes d'origine.
- Tous les en-têtes de l'utilisateur : tous les en-têtes HTTP des demandes de l'utilisateur sont inclus dans les demandes d'origine.
- Tous les en-têtes du visualiseur et les CloudFront en-têtes suivants : tous les en-têtes HTTP des requêtes du visualiseur sont inclus dans les requêtes d'origine. En outre, vous spécifiez les CloudFront en-têtes que vous souhaitez ajouter aux demandes d'origine. Pour plus d'informations sur les CloudFront en-têtes, consultezthe section called “Ajouter des en-têtes de CloudFront demande”.
- Include the following headers (Inclure les en-têtes suivants) : vous spécifiez quels en-têtes HTTP sont inclus dans les demandes d'origine.

  > **Note**
  >
  > Ne spécifiez pas un en-tête déjà inclus dans vos paramètres En-têtes personnalisés de l'origine. Pour plus d’informations, consultez Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine.

- Tous les en-têtes de visionnage, à l'exception de – vous spécifiez les en-têtes HTTP qui ne sont pas inclus dans les demandes d'origine. Tous les autres en-têtes HTTP contenus dans les demandes de visionnage, à l'exception de ceux spécifiés, sont inclus.

Lorsque vous utilisez tous les en-têtes de visionneuse et les CloudFront en-têtes suivants, incluez les en-têtes suivants ou Tous les en-têtes de visionneuse sauf le paramètre, vous spécifiez les en-têtes HTTP uniquement par leur nom d'en-tête. CloudFront inclut l'en-tête complet, y compris sa valeur, dans les demandes d'origine.

> **Note**
>
> Lorsque vous utilisez le paramètre Tous les en-têtes du lecteur sauf pour supprimer l'`Host`en-tête du lecteur, vous ajoutez CloudFront un nouvel `Host` en-tête avec le nom de domaine de l'origine à la demande d'origine.

Cookies

Les cookies contenus dans les demandes des utilisateurs, CloudFront y compris dans les demandes d'origine. Pour les cookies, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les cookies dans les demandes de l'utilisateur ne sont pas inclus dans les demandes d'origine.
- Tous : tous les cookies dans les demandes de l'utilisateur sont inclus dans les demandes d'origine.
- Inclure les cookies suivants – vous spécifiez quels cookies figurant dans les demandes de visionnage sont inclus dans les demandes d'origine.
- Tous les cookies sauf – vous spécifiez quels cookies figurant dans les demandes de visionnage ne sont pas inclus dans les demandes d'origine. Tous les autres cookies figurant dans les demandes de visionnage sont inclus.

Lorsque vous utilisez le paramètre Inclure les cookies suivants ou Tous les cookies sauf, vous spécifiez les cookies uniquement par leur nom. CloudFront inclut le cookie complet, y compris sa valeur, dans les demandes d'origine.

Chaînes de requête

Les chaînes de requête d'URL contenues dans les demandes du visualiseur, CloudFront y compris dans les demandes d'origine. Pour les chaînes de requête, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les chaînes de requête dans les demandes de l'utilisateur ne sont pas incluses dans les demandes d'origine.
- Toutes : toutes les chaînes de requête dans les demandes de l'utilisateur sont incluses dans les demandes d'origine.
- Inclure les chaînes de requête suivantes – vous spécifiez quelles chaînes de requête figurant dans les demandes de visionnage sont incluses dans les demandes d'origine.

- Toutes les chaînes de requête sauf – vous spécifiez quelles chaînes de requête figurant dans les demandes de visionnage ne sont pas incluses dans les demandes d'origine. Toutes les autres chaînes de requête sont incluses.

Lorsque vous utilisez le paramètre Inclure les chaînes de requête suivantes ou Toutes les chaînes de requête sauf, vous spécifiez les chaînes de requête uniquement par leur nom. CloudFront inclut la chaîne de requête complète, y compris sa valeur, dans les demandes d'origine.

Création de politiques de demande d'origine

Vous pouvez utiliser une politique de demande d'origine pour contrôler les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans les demandes CloudFront envoyées à votre origine. Vous pouvez créer une politique de demande d'origine dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Après avoir créé une politique de demande d'origine, vous l'associez à un ou plusieurs comportements de cache dans une CloudFront distribution.

Les stratégies de demande d'origine ne sont pas obligatoires. Lorsqu'un comportement de cache n'a pas de stratégie de demande d'origine attachée, la demande d'origine inclut toutes les valeurs spécifiées dans la stratégie de cache, mais rien de plus.

> **Note**
>
> Pour utiliser une stratégie de demande d'origine, le comportement de cache doit également utiliser une stratégie de cache. Vous ne pouvez pas utiliser de stratégie de demande d'origine dans un comportement de cache sans stratégie de cache.

Console

Pour créer une stratégie de demande d'origine (console)

1. Connectez-vous à la page Politiques AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Choisissez Origin request (Demande d'origine), puis Create origin request policy (Créer une stratégie de demande d'origine).

3. Choisissez le paramètre souhaité pour cette stratégie de demande d'origine. Pour plus d'informations, consultez Comprendre les politiques relatives aux demandes d'origine.
4. Lorsque vous avez terminé, choisissez Create (Créer).

Après avoir créé une stratégie de demande d'origine, vous pouvez l'attacher à un comportement de cache.

Pour attacher une stratégie de demande d'origine à une distribution existante (console)

1. Ouvrez la page Distributions dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Comportements.
3. Choisissez le comportement du cache à mettre à jour, puis choisissez Modifier.

   Ou, pour créer un nouveau comportement de cache, choisissez Create behavior (Créer un comportement).
4. Dans la section Cache key and origin requests (Clé de cache et demandes d'origine), assurez-vous que l'option Cache policy and origin request policy (Politique de cache et politique de demande d'origine) est sélectionnée.
5. Pour Origin request policy (Stratégie de demande d'origine), choisissez la stratégie de demande d'origine à attacher à ce comportement de cache.
6. Choisissez Save changes (Enregistrer les modifications) en bas de la page.

Pour attacher une stratégie de demande d'origine à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Dans la section Cache key and origin requests (Clé de cache et demandes d'origine), assurez-vous que l'option Cache policy and origin request policy (Politique de cache et politique de demande d'origine) est sélectionnée.
4. Pour Origin request policy (Stratégie de demande d'origine), choisissez la stratégie de demande d'origine à attacher au comportement de cache par défaut de cette distribution.

5. Choisissez les paramètres souhaités pour l'origine, le comportement de cache par défaut et les autres paramètres de distribution. Pour plus d'informations, consultez Référence des paramètres de distribution.
6. Lorsque vous avez terminé, choisissez Create distribution (Créer une distribution).

CLI

Pour créer une politique de demande d'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-request-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une stratégie de demande d'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-request-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-origin-request-policy.

```
aws cloudfront create-origin-request-policy --generate-cli-skeleton yaml-input >
 origin-request-policy.yaml
```

2. Ouvrez le fichier nommé `origin-request-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de stratégie de demande d'origine que vous souhaitez, puis enregistrez le fichier. Vous pouvez supprimer des champs facultatifs du fichier, mais ne supprimez pas les champs obligatoires.

   Pour de plus amples informations sur les paramètres de stratégie de demande d'origine, veuillez consulter Comprendre les politiques relatives aux demandes d'origine.
3. Utilisez la commande suivante pour créer la stratégie de demande d'origine à l'aide des paramètres d'entrée du fichier `origin-request-policy.yaml`.

```
aws cloudfront create-origin-request-policy --cli-input-yaml file://origin-
request-policy.yaml
```

Notez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de politique de demande d'origine, dont vous avez besoin pour associer la politique de demande d'origine au comportement du cache d'une CloudFront distribution.

Pour attacher une stratégie de demande d'origine à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour pour utiliser une stratégie de demande d'origine.

   - Dans le comportement du cache, ajoutez un champ nommé `OriginRequestPolicyId`. Pour la valeur du champ, utilisez l'ID de stratégie de demande d'origine que vous avez noté après la création de la stratégie.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la stratégie de demande d'origine. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une stratégie de demande d'origine à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml` qui contient tous les paramètres d'entrée de la commande create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `OriginRequestPolicyId`, entrez l'ID de stratégie de demande d'origine que vous avez noté après la création de la stratégie. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

   Pour de plus amples informations sur les paramètres de distribution, veuillez consulter Référence des paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Pour créer une politique de demande d'origine avec l' CloudFront API, utilisez CreateOriginRequestPolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez Comprendre les politiques relatives aux demandes d'origine la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une stratégie de demande d'origine, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la stratégie de demande d'origine dans le champ `OriginRequestPolicyId`, à l'intérieur d'un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utiliser des politiques de demande d'origine gérées

CloudFront fournit un ensemble de politiques de demande d'origine gérées que vous pouvez associer à tous les comportements de cache de votre distribution. Avec une stratégie de demande d'origine gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre stratégie de demande d'origine. Les stratégies gérées utilisent des paramètres optimisés pour des cas d'utilisation spécifiques.

Pour utiliser une stratégie de demande d'origine gérée, vous l'attachez à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une stratégie de demande d'origine, mais au lieu d'en créer une nouvelle, vous n'avez qu'à attacher l'une des stratégies de demande d'origine gérée. Vous attachez la stratégie par nom (avec la console) ou par ID (avec le AWS CLI ou les kits SDK). Les noms et les identifiants sont répertoriés dans la section suivante.

Pour plus d’informations, consultez Création de politiques de demande d'origine.

Les rubriques suivantes décrivent les stratégies de demande d’origine gérées que vous pouvez utiliser.

Rubriques

- AllViewer
- AllViewerAndCloudFrontHeaders-20/06
- AllViewerExceptHostHeader
- CORS- CustomOrigin
- CORS-S3Origin
- Élémentaire- - MediaTailor PersonalizedManifests
- UserAgentRefererHeaders

AllViewer

Afficher cette politique dans la CloudFront console

Cette politique inclut toutes les valeurs (en-têtes, cookies et chaînes de requête) dans la demande de visionnage.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`216adef6-5c7f-47e4-b989-5492eafa07d3`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : Tous les en-têtes de la demande de l'utilisateur
- Cookies inclus dans les demandes d'origine : Tous
- Chaînes de requête incluses dans les demandes d'origine : Toutes

AllViewerAndCloudFrontHeaders-20/06

Afficher cette politique dans la CloudFront console

Cette politique inclut toutes les valeurs (en-têtes, cookies et chaînes de requête) de la demande du lecteur, ainsi que tous les CloudFront en-têtes publiés jusqu'en juin 2022 (CloudFront les en-têtes publiés après juin 2022 ne sont pas inclus).

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`33f36d7e-f396-46d9-90e0-52428a34d9dc`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : tous les en-têtes de la demande de visualisation, ainsi que les en-têtes suivants : CloudFront
  - `CloudFront-Forwarded-Proto`
  - `CloudFront-Is-Android-Viewer`
  - `CloudFront-Is-Desktop-Viewer`
  - `CloudFront-Is-IOS-Viewer`
  - `CloudFront-Is-Mobile-Viewer`
  - `CloudFront-Is-SmartTV-Viewer`

- `CloudFront-Is-Tablet-Viewer`
- `CloudFront-Viewer-Address`
- `CloudFront-Viewer-ASN`
- `CloudFront-Viewer-City`
- `CloudFront-Viewer-Country`
- `CloudFront-Viewer-Country-Name`
- `CloudFront-Viewer-Country-Region`
- `CloudFront-Viewer-Country-Region-Name`
- `CloudFront-Viewer-Http-Version`
- `CloudFront-Viewer-Latitude`
- `CloudFront-Viewer-Longitude`
- `CloudFront-Viewer-Metro-Code`
- `CloudFront-Viewer-Postal-Code`
- `CloudFront-Viewer-Time-Zone`
- `CloudFront-Viewer-TLS`

- Cookies inclus dans les demandes d'origine : Tous
- Chaînes de requête incluses dans les demandes d'origine : Toutes

AllViewerExceptHostHeader

Afficher cette politique dans la CloudFront console

Cette politique n'inclut pas l'en-tête `Host` de la demande de visionnage, mais inclut toutes les autres valeurs (en-têtes, cookies et chaînes de requête) de la demande de visionnage.

Cette politique inclut également des en-têtes de CloudFront demande supplémentaires pour le protocole HTTP, la version HTTP, la version TLS, ainsi que tous les en-têtes de type d'appareil et de localisation du spectateur.

Cette politique est destinée à être utilisée avec Amazon API Gateway et les origines des URL des AWS Lambda fonctions. Ces origines supposent que l'`Host`en-tête contienne le nom de domaine d'origine, et non le nom de domaine de la CloudFront distribution. Le transfert de l'en-tête `Host` de la demande de visionnage vers ces origines peut empêcher leur fonctionnement.

> **Note**
>
> Lorsque vous utilisez cette politique de gestion des demandes d'origine pour supprimer l'`Host`en-tête du lecteur, vous CloudFront ajoutez un nouvel `Host` en-tête avec le nom de domaine de l'origine à la demande d'origine.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`b689b0a8-53d0-40ab-baf2-68738e2966ac`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : tous les en-têtes de la demande de visionnage à l'exception de l'en-tête `Host`
- Cookies inclus dans les demandes d'origine : Tous
- Chaînes de requête incluses dans les demandes d'origine : Toutes

CORS- CustomOrigin

Afficher cette politique dans la CloudFront console

Cette stratégie inclut l'en-tête qui active les demandes de partage de ressources croisées (CORS) lorsque l'origine est une origine personnalisée.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`59781a5b-3903-41f3-afcb-af62929ccde1`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

CORS-S3Origin

Afficher cette politique dans la CloudFront console

Cette stratégie inclut les en-têtes qui activent les demandes de partage de ressources croisées (CORS) lorsque l'origine est un compartiment Amazon S3.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`88a5eaf4-2fd4-4709-b370-b4c650ea3fcf`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

Élémentaire- - MediaTailor PersonalizedManifests

Afficher cette politique dans la CloudFront console

Cette stratégie est destinée à être utilisée avec une origine correspondant à un point de terminaison AWS Elemental MediaTailor .

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`775133bc-15f2-49f9-abea-afb2e0bf67d2`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`

  - `User-Agent`
  - `X-Forwarded-For`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Toutes

UserAgentRefererHeaders

Afficher cette politique dans la CloudFront console

Cette stratégie inclut uniquement les en-têtes `User-Agent` et `Referer`. Il n'inclut pas de chaînes de requête ni de cookies.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`acba4595-bd28-49b8-b9fe-13317c0390fa`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `User-Agent`
  - `Referer`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

Ajouter des en-têtes de CloudFront demande

Vous pouvez configurer CloudFront pour ajouter des en-têtes HTTP spécifiques aux demandes CloudFront reçues des utilisateurs et transmises à votre fonction d'origine ou de périphérie. Les valeurs de ces en-têtes HTTP sont basées sur des caractéristiques de l'utilisateur ou sur la demande de l’utilisateur. Les en-têtes fournissent des informations sur le type d'appareil, l'adresse IP, l'emplacement géographique, le protocole de demande (HTTP ou HTTPS), la version HTTP, les détails de la connexion TLS et l’empreinte JA3 de l’utilisateur..

Avec ces en-têtes, votre origine ou votre fonction périphérique peut recevoir des informations sur l'utilisateur sans avoir besoin d'écrire votre propre code pour déterminer ces informations. Si votre origine renvoie des réponses différentes en fonction des informations contenues dans ces en-têtes,

vous pouvez les inclure dans la clé de cache afin que les réponses soient CloudFront mises en cache séparément. Par exemple, votre origine peut répondre avec du contenu dans une langue spécifique en fonction du pays dans lequel se trouve le visualiseur, ou avec du contenu adapté à un type d'appareil spécifique. Votre origine peut également écrire ces en-têtes dans des fichiers journaux, que vous pouvez utiliser pour déterminer où se trouvent vos spectateurs, quels types d'appareils ils se trouvent, et plus encore.

Pour inclure ces en-têtes dans la clé de cache, utilisez une politique de cache. Pour plus d'informations, consultez Contrôlez la clé de cache à l'aide d'une politique et the section called "Comprendre la clé de cache".

Pour recevoir des en-têtes à l'origine sans les inclure dans la clé de cache, utilisez une politique de demande de l'origine. Pour plus d'informations, consultez Contrôlez les demandes d'origine à l'aide d'une politique.

Rubriques

En-têtes pour déterminer le type d'appareil de l'utilisateur

Vous pouvez ajouter les en-têtes suivants pour déterminer le type d'appareil de l'utilisateur. En fonction de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes sur `true` ou`false`. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront définit à la fois `CloudFront-Is-Mobile-Viewer` et `CloudFront-Is-Tablet-Viewer` à`true`.

- `CloudFront-Is-Android-Viewer`— Réglé sur `true` quand CloudFront détermine que le spectateur est un appareil doté du système d'exploitation Android.
- `CloudFront-Is-Desktop-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le lecteur est un appareil de bureau.
- `CloudFront-Is-IOS-Viewer`— Réglé sur `true` quand CloudFront détermine que le spectateur est un appareil doté d'un système d'exploitation mobile Apple, tel qu'un iPhone, un iPod touch et certains iPad.

- `CloudFront-Is-Mobile-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le spectateur est un appareil mobile.
- `CloudFront-Is-SmartTV-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le téléspectateur est un téléviseur intelligent.
- `CloudFront-Is-Tablet-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le lecteur est une tablette.

En-têtes pour déterminer l'emplacement de l'utilisateur

Vous pouvez ajouter les en-têtes suivants pour déterminer la position du spectateur. CloudFront détermine les valeurs de ces en-têtes en fonction de l'adresse IP du spectateur. Pour les caractères non ASCII dans les valeurs de ces en-têtes, le CloudFront pourcentage code le caractère conformément à la section 1.2 de la RFC 3986.

- `CloudFront-Viewer-Address` : contient l'adresse IP de l'utilisateur et le port source de la demande. Par exemple, une valeur d'en-tête de `198.51.100.10:46532` signifie que l'adresse IP de l'utilisateur est 198.51.100.10 et que le port source de la demande est 46532.
- `CloudFront-Viewer-ASN` : contient le numéro de système autonome (ASN) de l'utilisateur.

> **Note**
>
> Vous pouvez ajouter `CloudFront-Viewer-Address` et `CloudFront-Viewer-ASN` dans une politique de demande d'origine, mais pas dans une politique de cache.

- `CloudFront-Viewer-Country` – Contient le code de pays à deux lettres du pays de l'utilisateur. Pour obtenir une liste des codes de pays, consultez ISO 3166-1 alpha-2.
- `CloudFront-Viewer-City` – Contient le nom de la ville de l'utilisateur.

Lorsque vous ajoutez les en-têtes suivants, CloudFront appliquez-les à toutes les demandes, à l'exception de celles qui proviennent du AWS réseau :

- `CloudFront-Viewer-Country-Name` – Contient le nom du pays de l'utilisateur.
- `CloudFront-Viewer-Country-Region` – Contient un code (jusqu'à trois caractères) représentant la région de l'utilisateur. La région est la subdivision de premier niveau (la plus large ou la moins spécifique) du code ISO 3166-2.

- `CloudFront-Viewer-Country-Region-Name` – Contient le nom de la région de l'utilisateur. La région est la subdivision de premier niveau (la plus large ou la moins spécifique) du code ISO 3166-2.
- `CloudFront-Viewer-Latitude` – Contient la latitude approximative de l'utilisateur.
- `CloudFront-Viewer-Longitude` – Contient la longitude approximative de l'utilisateur.
- `CloudFront-Viewer-Metro-Code` – Contient le code régional de l'utilisateur. Ceci n'est présent que lorsque l'utilisateur est aux États-Unis.
- `CloudFront-Viewer-Postal-Code` – Contient le code postal de l'utilisateur.
- `CloudFront-Viewer-Time-Zone` Contient le fuseau horaire de l'utilisateur, au format de base de données de fuseau horaire IANA (par exemple, `America/Los_Angeles`).

En-têtes pour déterminer la structure de l'en-tête de l'utilisateur

Vous pouvez ajouter les en-têtes suivants pour identifier l'utilisateur en fonction des en-têtes qu'il envoie. Par exemple, différents navigateurs peuvent envoyer des en-têtes HTTP dans un certain ordre. Si le navigateur spécifié dans l'en-tête `User-Agent` ne correspond pas à l'ordre d'en-tête attendu par ce navigateur, vous pouvez refuser la demande. De plus, si la valeur `CloudFront-Viewer-Header-Count` ne correspond pas au nombre d'en-têtes de `CloudFront-Viewer-Header-Order`, vous pouvez refuser la demande.

- `CloudFront-Viewer-Header-Order` : contient les noms d'en-tête de l'utilisateur dans l'ordre demandé, séparés par deux points. Par exemple : `CloudFront-Viewer-Header-Order: Host:User-Agent:Accept:Accept-Encoding`. Les en-têtes dépassant la limite de 7 680 caractères sont tronqués.
- `CloudFront-Viewer-Header-Count` : contient le nombre total d'en-têtes de l'utilisateur.

Autres CloudFront en-têtes

Vous pouvez ajouter les en-têtes suivants pour déterminer le protocole, la version, l'empreinte JA3 et les détails de connexion TLS de l'utilisateur :

- `CloudFront-Forwarded-Proto` – Contient le protocole de la demande de l'utilisateur (HTTP ou HTTPS).
- `CloudFront-Viewer-Http-Version` – Contient la version HTTP de la demande de l'utilisateur.

- `CloudFront-Viewer-JA3-Fingerprint` : contient l'empreinte JA3 de l'utilisateur. L'empreinte JA3 peut vous aider à déterminer si la demande provient d'un client connu, s'il s'agit d'un logiciel malveillant, d'un bot malveillant ou d'une application attendue (répertoriée dans la liste des applications autorisées). Cet en-tête repose sur le paquet `Client Hello` SSL/TLS de l'utilisateur et n'est présent que pour les demandes HTTPS.

  > **Note**
  >
  > Vous pouvez ajouter `CloudFront-Viewer-JA3-Fingerprint` dans une politique de demande d'origine, mais pas dans une politique de cache.

- `CloudFront-Viewer-TLS`— Contient la version SSL/TLS, le code et des informations sur le handshake SSL/TLS utilisé pour la connexion entre le lecteur et. CloudFront Spécifiez la valeur au format suivant :

  ```
  SSL/TLS_version:cipher:handshake_information
  ```

  Pour *`handshake_information`*, l'en-tête peut contenir les valeurs suivantes :

  - `fullHandshake` – Une liaison complète a été effectuée pour la session SSL/TLS.
  - `sessionResumed` – Une session SSL/TLS précédente a été reprise.
  - `connectionReused` – Une connexion SSL/TLS précédente a été réutilisée.

  Voici quelques exemples de valeurs pour cet en-tête.

  ```
  TLSv1.3:TLS_AES_128_GCM_SHA256:sessionResumed
  ```

  ```
  TLSv1.2:ECDHE-ECDSA-AES128-GCM-SHA256:connectionReused
  ```

  ```
  TLSv1.1:ECDHE-RSA-AES128-SHA256:fullHandshake
  ```

  ```
  TLSv1:ECDHE-RSA-AES256-SHA:fullHandshake
  ```

  Pour obtenir la liste complète des versions SSL/TLS possibles et des chiffrements pouvant figurer dans cette valeur d'en-tête, reportez-vous à la section the section called “Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront”.

> **Note**
>
> Vous pouvez ajouter `CloudFront-Viewer-TLS` dans une politique de demande d'origine, mais pas dans une politique de cache.

Découvrez comment les politiques de demande d'origine et les politiques de cache fonctionnent ensemble

Vous pouvez utiliser une politique de demande CloudFront d'origine pour contrôler les demandes CloudFront envoyées à l'origine, appelées demandes d'origine. Pour utiliser une politique de demande d'origine, vous devez attacher une politique de cache au même comportement de cache. Vous ne pouvez pas utiliser de stratégie de demande d'origine dans un comportement de cache sans stratégie de cache. Pour plus d'informations, consultez Contrôlez les demandes d'origine à l'aide d'une politique.

Les politiques de demande d'origine et les politiques de cache fonctionnent ensemble pour déterminer les valeurs CloudFront incluses dans les demandes d'origine. Toutes les chaînes de requête URL, tous les en-têtes HTTP et tous les cookies que vous spécifiez dans la clé de cache (à l'aide d'une politique de cache) sont automatiquement inclus dans les demandes d'origine. Toutes les chaînes de requête, tous les en-têtes et tous les cookies supplémentaires que vous spécifiez dans une politique de demande d'origine sont également inclus dans les demandes d'origine (mais pas dans la clé de cache).

Les politiques de demande d'origine et les politiques de cache comportent des paramètres qui peuvent sembler contradictoires. Par exemple, une politique peut autoriser certaines valeurs tandis qu'une autre les bloque. Le tableau suivant explique les valeurs CloudFront incluses dans les demandes d'origine lorsque vous utilisez conjointement les paramètres d'une politique de demande d'origine et d'une politique de cache. Ces paramètres s'appliquent généralement à tous les types de valeurs (chaînes de requête, en-têtes et cookies), à l'exception du fait que vous ne pouvez pas spécifier tous les en-têtes ni utiliser une liste de blocage d'en-têtes dans une politique de cache.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Politique de cache				
Aucun	Aucune valeur provenant de la demande de visionnage n'est incluse dans la demande d'origine, à l'exception des valeurs par défaut incluses dans chaque demande d'origine. Pour plus d'informations, consultez Contrôlez les demandes d'origine à l'aide d'une politique.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Seules les valeurs spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine.	Toutes les valeurs de la demande de visionnage à l'exception de celles spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine.
Tous Remarque : Vous ne pouvez pas spécifier tous les en-têtes dans une politique de cache.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage sont inclus dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage, ainsi que tous les en-têtes spécifiés dans la politique de demande	Toutes les chaînes de requête et tous les cookies de la demande de visionnage sont inclus dans la demande d'origine, même ceux spécifiés

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
			d'origine sont inclus dans la demande d'origine.	dans la liste de blocages de la politique de demande d'origine. Le paramètre de politique de cache remplace la liste de blocages de la politique de demande d'origine.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Liste verte	Seules les valeurs spécifiées dans la demande de visionnage sont incluses dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Toutes les valeurs spécifiées dans la politique de cache ou dans la politique de demande d'origine sont incluses dans la demande d'origine.	Les valeurs spécifiées dans la politique de cache sont incluses dans la demande d'origine, même si ces mêmes valeurs sont spécifiées dans la liste de blocages de la politique de demande d'origine. La liste verte de la politique de cache remplace la liste de blocages de la politique de demande d'origine.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Liste de blocages Remarque : Vous ne pouvez pas spécifier d'en-têtes dans la liste de blocages d'une politique de cache.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage à l'exception de ceux spécifiés sont inclus dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Les valeurs spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine, même si ces mêmes valeurs sont spécifiées dans la liste de blocages de la politique de cache. La liste verte de la politique de demande d'origine remplace la liste de blocages de la politique de cache.	Toutes les valeurs de la demande de visionnage à l'exception de celles spécifiées dans la politique de cache ou dans la politique de demande d'origine sont incluses dans la demande d'origine.

Ajouter ou supprimer des en-têtes HTTP dans les CloudFront réponses avec une politique

Vous pouvez configurer CloudFront pour modifier les en-têtes HTTP dans les réponses qu'il envoie aux utilisateurs (navigateurs Web et autres clients). CloudFront peut supprimer les en-têtes qu'il a reçus de l'origine, ou ajouter des en-têtes à la réponse, avant de l'envoyer aux spectateurs. Ces modifications ne nécessitent pas d'écrire de code ou de modifier l'origine.

Par exemple, vous pouvez supprimer des en-têtes tels que `X-Powered-By` et `Vary` afin qu'ils CloudFront ne soient pas inclus dans les réponses envoyées aux spectateurs. Vous pouvez également ajouter des en-têtes HTTP tels que les suivants :

- Un en-tête `Cache-Control` pour contrôler la mise en cache du navigateur.
- Un en-tête `Access-Control-Allow-Origin` pour activer le partage des ressources cross-origin (Cross-Origin Resource Sharing, CORS). Vous pouvez également ajouter d'autres en-têtes CORS.
- Un ensemble d'en-têtes de sécurité courants, tels que `Strict-Transport-Security`, `Content-Security-Policy` et `X-Frame-Options`.
- Un `Server-Timing` en-tête permettant de consulter les informations relatives aux performances et au routage de la demande et de la réponse CloudFront.

Pour spécifier les en-têtes qui CloudFront ajoutent ou suppriment dans les réponses HTTP, vous utilisez une politique d'en-têtes de réponse. Vous associez une politique d'en-têtes de réponse à un autre comportement de cache et vous CloudFront modifiez les en-têtes des réponses qu'il envoie aux demandes correspondant au comportement du cache. CloudFront modifie les en-têtes des réponses qu'il fournit depuis le cache et celles qu'il transmet depuis l'origine. Si la réponse d'origine inclut un ou plusieurs en-têtes ajoutés dans une politique d'en-têtes de réponse, la politique peut spécifier si elle CloudFront utilise l'en-tête reçu de l'origine ou si elle remplace cet en-tête par celui de la politique d'en-têtes de réponse.

CloudFront fournit des politiques d'en-têtes de réponse prédéfinies, appelées politiques gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces politiques gérées ou créer vos propres politiques. Vous pouvez associer une politique d'en-têtes de réponse unique à plusieurs comportements de cache dans plusieurs distributions de votre Compte AWS.

Pour plus d’informations, consultez les rubriques suivantes.

Rubriques

Comprendre les politiques relatives aux en-têtes de réponse

Vous pouvez utiliser une politique d'en-têtes de réponse pour spécifier les en-têtes HTTP qu'Amazon CloudFront supprime ou ajoute dans les réponses qu'il envoie aux utilisateurs. Pour plus d'informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajouter ou supprimer des en-têtes de réponse avec une politique.

Les rubriques suivantes expliquent les paramètres dans une politique d’en-têtes de réponses. Les paramètres sont regroupés en catégories, qui sont représentées dans les rubriques suivantes.

Rubriques

Détails de la politique (métadonnées)

Les paramètres des détails de la politique contiennent des métadonnées sur une politique d'en-têtes de réponses.

- Name (Nom) : nom permettant d'identifier la politique d’en-têtes de réponses. Dans la console, utilisez le nom pour attacher la politique à un comportement de cache.
- Description (facultative) : commentaire permettant de décrire la politique d’en-têtes de réponses. Cette option est facultative, mais elle peut vous aider à identifier l'objectif de la politique.

En-têtes CORS

Les paramètres de partage des ressources cross-origin (CORS) permettent d'ajouter et de configurer des en-têtes CORS dans une politique d'en-têtes de réponses.

Cette liste explique comment spécifier des paramètres et des valeurs valides dans une politique d'en-têtes de réponse. Pour plus d'informations sur chacun de ces en-têtes et sur leur mode d'utilisation pour les demandes et réponses CORS réelles, consultez la section partage des ressources cross-origin dans MDN Web Docs et dans les spécifications de protocole CORS.

Access-Control-Allow-Credentials

Il s'agit d'un paramètre booléen (`true`ou`false`) qui détermine si l'`Access-Control-Allow-Credentials`en-tête est CloudFront ajouté dans les réponses aux requêtes CORS. Lorsque ce paramètre est défini sur`true`, CloudFront ajoute l'`Access-Control-Allow-Credentials: true`en-tête dans les réponses aux demandes CORS. Sinon, CloudFront n'ajoute pas cet en-tête aux réponses.

Access-Control-Allow-Headers

Spécifie les noms d'en-tête qui sont CloudFront utilisés comme valeurs pour l'`Access-Control-Allow-Headers`en-tête dans les réponses aux demandes de pré-vol CORS. Les valeurs valides pour ce paramètre incluent les noms d'en-têtes HTTP ou le caractère générique (*), qui indique que tous les en-têtes sont admis.

> **Note**
>
> L'`Authorization`en-tête ne peut pas utiliser de caractère générique et doit être répertorié explicitement.

Exemples d'utilisation valide du caractère générique

Exemple	Correspond à	Ne correspond pas à
`x-amz-*`	`x-amz-test` `x-amz-`	`x-amz`
`x-*-amz`	`x-test-amz`	

Exemple	Correspond à	Ne correspond pas à
	`x--amz`	
`*`	Tous les en-têtes sauf `Authorization`	`Authorization`

Access-Control-Allow-Methods

Spécifie les méthodes HTTP qui sont CloudFront utilisées comme valeurs pour l'`Access-Control-Allow-Methods`en-tête dans les réponses aux requêtes CORS de pré-vol. Les valeurs valides sont `GET`, `DELETE`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT` et `ALL`. `ALL` est une valeur spéciale qui inclut toutes les méthodes HTTP répertoriées.

Access-Control-Allow-Origin

Spécifie les valeurs qui CloudFront peuvent être utilisées dans l'en-tête de `Access-Control-Allow-Origin` réponse. Les valeurs valides pour ce paramètre incluent une origine spécifique (telle que `http://www.example.com`) ou le caractère générique (`*`), ce qui indique que toutes les origines sont autorisées. Consultez le tableau suivant pour obtenir des exemples :

> **Note**
>
> Le caractère générique (`*`) est autorisé à l'extrémité gauche du domaine (`*.example.org`).
> Le caractère générique (`*`) n'est pas autorisé dans les positions suivantes :
>
> - Domaines de premier niveau (`example.*`)
> - À droite des sous-domaines (`test.*.example.org`)
> - À l'intérieur des termes (`exa*mple.org`)

Le tableau suivant présente des exemples d'utilisation valide du caractère générique :

Exemple	Correspond à	Ne correspond pas à
`http://*.example.org`	`http://www.example.org`	**`https`**`://test.example.org`

Exemple	Correspond à	Ne correspond pas à

	`http://test.example.org`
	
	`http://test.example.org:123`
		`https``://test.example.org:123`

`*.example.org`	`test.example.org`
	
	`test.test.example.org`
	
	`.example.org`
	
	`http://test.example.org`
	
	`https://test.example.org`
	
	`http://test.example.org:123`
	
	`https://test.example.org:123`	

`example.org`	`http://example.org`
	
	`https://example.org`	

`http://example.org`		**`https`**`://example.org` `http://example.org:123`

`http://example.org:*`	`http://example.org:123`
	
	`http://example.org`	

Exemple	Correspond à	Ne correspond pas à

`http://example.org:1*3`	`http://example.org:123`
	
	`http://example.org:1893`
	
	`http://example.org:13`	

`*.example.org:1*`	`test.example.org:123`	

Access-Control-Expose-Headers

Spécifie les noms d'en-tête qui sont CloudFront utilisés comme valeurs pour l'`Access-Control-Expose-Headers`en-tête dans les réponses aux demandes CORS. Les valeurs valides pour ce paramètre incluent les noms d'en-têtes HTTP ou le caractère générique (`*`).

Access-Control-Max-Age

Un nombre de secondes, CloudFront utilisé comme valeur de l'`Access-Control-Max-Age`en-tête dans les réponses aux demandes de pré-vol CORS.

Origin override (Remplacement de l’origine)

Paramètre booléen qui détermine le CloudFront comportement lorsque la réponse provenant de l'origine contient l'un des en-têtes CORS figurant également dans la politique.

- Lorsqu'elle est définie sur `true` et que la réponse d'origine contient un en-tête CORS qui figure également dans la politique, CloudFront ajoute l'en-tête CORS de la politique à la réponse. CloudFront envoie ensuite cette réponse au spectateur. CloudFront ignore l'en-tête qu'il a reçu de l'origine.
- Lorsqu'elle est définie sur `false` et que la réponse d'origine contient un en-tête CORS (que l'en-tête CORS figure ou non dans la politique), elle CloudFront inclut l'en-tête CORS qu'elle a reçu de l'origine à la réponse. CloudFront n'ajoute aucun en-tête CORS dans la politique à la réponse envoyée au lecteur.

En-têtes de sécurité

Vous pouvez utiliser les paramètres des en-têtes de sécurité pour ajouter et configurer plusieurs en-têtes de réponse HTTP liés à la sécurité dans une politique d'en-têtes de réponse.

Cette liste explique comment vous pouvez spécifier le paramètre et les valeurs valides dans une politique d'en-têtes de réponse. Pour plus d'informations sur chacun de ces en-têtes et sur leur mode d'utilisation dans les réponses HTTP réelles, consultez les liens d'accès à MDN Web Docs.

Content-Security-Policy

Spécifie les directives de politique de sécurité du contenu qui sont CloudFront utilisées comme valeurs pour l'en-tête de `Content-Security-Policy` réponse.

Pour plus d'informations sur cet en-tête et sur les directives valides de la politique, consultez la section Content-Security-Policy dans MDN Web Docs.

> **Note**
>
> La valeur d'en-tête `Content-Security-Policy` est limitée à 1 783 caractères.

Referrer-Policy

Spécifie la directive de politique de référence CloudFront utilisée comme valeur pour l'en-tête de `Referrer-Policy` réponse. Les valeurs valides pour ce paramètre sont `no-referrer`, `no-referrer-when-downgrade`, `origin`, `origin-when-cross-origin`, `same-origin`, `strict-origin`, `strict-origin-when-cross-origin` et `unsafe-url`.

Pour plus d'informations sur cet en-tête et ces directives, consultez la section Referrer-Policy dans MDN Web Docs.

Strict-Transport-Security

Spécifie les directives et les paramètres CloudFront utilisés comme valeur pour l'en-tête de `Strict-Transport-Security` réponse. Pour ce paramètre, spécifiez séparément :

- Un nombre de secondes, qui est CloudFront utilisé comme valeur pour la `max-age` directive de cet en-tête
- Un paramètre booléen (`true`ou`false`) pour`preload`, qui détermine si la `preload` directive est CloudFront incluse dans la valeur de cet en-tête

- Un paramètre booléen (`true`ou`false`) pour`includeSubDomains`, qui détermine si la `includeSubDomains` directive est CloudFront incluse dans la valeur de cet en-tête

Pour plus d'informations sur cet en-tête et ces directives, consultez la section Strict-Transport-Security dans MDN Web Docs.

X-Content-Type-Options

Il s'agit d'un paramètre booléen (`true`ou`false`) qui détermine si l'`X-Content-Type-Options`en-tête est CloudFront ajouté aux réponses. Lorsque ce paramètre est défini`true`, CloudFront ajoute l'`X-Content-Type-Options: nosniff`en-tête aux réponses. Sinon, cet en-tête CloudFront n'est pas ajouté.

Pour plus d'informations sur cet en-tête, consultez la section X-Content-Type-Options dans MDN Web Docs.

X-Frame-Options

Spécifie la directive CloudFront à utiliser comme valeur pour l'en-tête de `X-Frame-Options` réponse. Les valeurs valides pour ce paramètre sont `DENY` ou `SAMEORIGIN`.

Pour plus d'informations sur cet en-tête et ces directives, consultez la section X-Frame-Options dans MDN Web Docs.

X-XSS-Protection

Spécifie les directives et les paramètres CloudFront utilisés comme valeur pour l'en-tête de `X-XSS-Protection` réponse. Pour ce paramètre, spécifiez séparément :

- Un paramètre `X-XSS-Protection` de `0` (désactive le filtrage XSS) ou `1` (active le filtrage XSS)
- Un paramètre booléen (`true`ou`false`) pour`block`, qui détermine si la `mode=block` directive est CloudFront incluse dans la valeur de cet en-tête
- Un URI de rapport, qui détermine si CloudFront la `report=`*`reporting URI`* directive est incluse dans la valeur de cet en-tête

Vous pouvez spécifier `true` pour `block`, ou une URI de génération de rapports, mais pas les deux conjointement. Pour plus d'informations sur cet en-tête et ces directives, consultez la section X-XSS-Protection dans MDN Web Docs.

Origin override (Remplacement de l'origine)

Chacun de ces paramètres d'en-tête de sécurité contient un paramètre booléen (`true`ou`false`) qui détermine le CloudFront comportement lorsque la réponse de l'origine contient cet en-tête.

Lorsque ce paramètre est défini sur `true` et que la réponse d'origine contient l'en-tête, CloudFront ajoute l'en-tête de la politique à la réponse envoyée au lecteur. Il ignore l'en-tête qu'il a reçu de l'origine.

Lorsque ce paramètre est défini sur `false` et que la réponse d'origine contient l'en-tête, CloudFront inclut l'en-tête reçu de l'origine dans la réponse qu'elle envoie au spectateur.

Lorsque la réponse d'origine ne contient pas d'en-tête, CloudFront ajoute l'en-tête dans la politique à la réponse envoyée au spectateur. CloudFront effectue cette opération lorsque ce paramètre est défini sur `true` ou`false`.

En-têtes personnalisés

Vous pouvez utiliser les paramètres d'en-têtes personnalisés pour ajouter et configurer des en-têtes HTTP personnalisés dans une politique d'en-têtes de réponse. CloudFront ajoute ces en-têtes à chaque réponse qu'il renvoie aux spectateurs. Pour chaque en-tête personnalisé, spécifiez également la valeur de l'en-tête, bien que la spécification d'une valeur soit facultative. Cela est dû au fait qu'il est CloudFront possible d'ajouter un en-tête de réponse sans valeur.

Chaque en-tête personnalisé possède également son propre paramètre Origin override (Remplacement de l’origine) :

- Lorsque ce paramètre est défini sur `true` et que la réponse d'origine contient l'en-tête personnalisé figurant dans la politique, CloudFront ajoute l'en-tête personnalisé de la politique à la réponse qu'elle envoie au lecteur. Il ignore l'en-tête qu'il a reçu de l'origine.
- Lorsque ce paramètre est `false` activé et que la réponse d'origine contient l'en-tête personnalisé figurant dans la politique, CloudFront inclut l'en-tête personnalisé reçu de l'origine dans la réponse qu'elle envoie au lecteur.
- Lorsque la réponse d'origine ne contient pas l'en-tête personnalisé figurant dans la politique, CloudFront ajoute l'en-tête personnalisé de la politique à la réponse envoyée au lecteur. CloudFront effectue cette opération lorsque ce paramètre est défini sur `true` ou`false`.

Suppression d’en-têtes

Vous pouvez spécifier les en-têtes que vous CloudFront souhaitez supprimer des réponses qu'il reçoit depuis l'origine afin qu'ils ne soient pas inclus dans les réponses CloudFront envoyées aux spectateurs. CloudFront supprime les en-têtes de chaque réponse envoyée aux spectateurs, que

les objets soient servis depuis le CloudFront cache ou depuis l'origine. Par exemple, vous pouvez supprimer des en-têtes inutiles pour les navigateurs, tels que `X-Powered-By` ou`Vary`, afin de CloudFront supprimer ces en-têtes des réponses envoyées aux utilisateurs.

Lorsque vous spécifiez des en-têtes à supprimer à l'aide d'une politique d'en-têtes de réponse, CloudFront supprimez d'abord les en-têtes, puis ajoutez tous les en-têtes spécifiés dans d'autres sections de la politique d'en-têtes de réponse (en-têtes CORS, en-têtes de sécurité, en-têtes personnalisés, etc.). Si vous spécifiez un en-tête à supprimer mais que vous ajoutez également le même en-tête dans une autre section de la politique, CloudFront incluez l'en-tête dans les réponses envoyées aux spectateurs.

> **Note**
>
> Vous pouvez utiliser une politique d'en-têtes de réponse pour supprimer `Date` les en-têtes `Server` et CloudFront reçus de l'origine, afin que ces en-têtes (tels qu'ils proviennent de l'origine) ne soient pas inclus dans les réponses CloudFront envoyées aux spectateurs. Toutefois, si vous le faites, CloudFront ajoute sa propre version de ces en-têtes aux réponses qu'il envoie aux spectateurs. Pour l'`Server`en-tête qui CloudFront ajoute, la valeur de l'en-tête est`CloudFront`.

En-têtes que vous ne pouvez pas supprimer

Vous ne pouvez pas supprimer les en-têtes suivants à l'aide d'une politique d'en-têtes de réponse. Si vous spécifiez ces en-têtes dans la section Remove headers (Supprimer les en-têtes) d'une politique d'en-têtes de réponse (`ResponseHeadersPolicyRemoveHeadersConfig` dans l'API), vous recevez un message d'erreur.

- `Connection`
- `Content-Encoding`
- `Content-Length`
- `Expect`
- `Host`
- `Keep-Alive`
- `Proxy-Authenticate`
- `Proxy-Authorization`

- Proxy-Connection
- Trailer
- Transfer-Encoding
- Upgrade
- Via
- Warning
- X-Accel-Buffering
- X-Accel-Charset
- X-Accel-Limit-Rate
- X-Accel-Redirect
- X-Amz-Cf-.*
- X-Amzn-Auth
- X-Amzn-Cf-Billing
- X-Amzn-Cf-Id
- X-Amzn-Cf-Xff
- X-Amzn-ErrorType
- X-Amzn-Fle-Profile
- X-Amzn-Header-Count
- X-Amzn-Header-Order
- X-Amzn-Lambda-Integration-Tag
- X-Amzn-RequestId
- X-Cache
- X-Edge-.*
- X-Forwarded-Proto
- X-Real-Ip

En-tête Server-Timing

Utilisez le paramètre Server-Timing d'en-tête pour activer l'Server-Timingen-tête dans les réponses HTTP envoyées depuis CloudFront. Vous pouvez utiliser cet en-tête pour consulter

les statistiques qui peuvent vous aider à mieux comprendre le comportement, les performances CloudFront et votre origine. Par exemple, vous pouvez voir quelle couche de cache a servi un accès au cache. Vous pouvez également voir la latence du premier octet à partir de l'origine en cas d'échec d'accès au cache Les indicateurs figurant dans l'`Server-Timing`en-tête peuvent vous aider à résoudre les problèmes ou à tester l'efficacité de votre configuration CloudFront ou de votre configuration d'origine.

Pour plus d'informations sur l'utilisation de l'`Server-Timing`en-tête avec CloudFront, consultez les rubriques suivantes.

Pour activer l'en-tête `Server-Timing`, créez (ou modifiez) une politique d'en-têtes de réponse.

Rubriques

- Taux d'échantillonnage et en-tête de requête Pragma
- En-tête Server-Timing d'origine
- Métriques d'en-tête Server-Timing
- Exemples d'en-têtes Server-Timing

Taux d'échantillonnage et en-tête de requête Pragma

Lorsque vous activez l'en-tête `Server-Timing` dans une politique d'en-têtes de réponse, spécifiez également le taux d'échantillonnage. Le taux d'échantillonnage est un nombre compris entre 0 et 100 (inclus) qui indique le pourcentage de réponses auxquelles vous CloudFront souhaitez ajouter l'`Server-Timing`en-tête. Lorsque vous définissez le taux d'échantillonnage sur 100, CloudFront ajoute l'`Server-Timing`en-tête à la réponse HTTP pour chaque demande correspondant au comportement du cache auquel la politique des en-têtes de réponse est attachée. Lorsque vous le définissez sur 50, il CloudFront ajoute l'en-tête à 50 % des réponses pour les demandes qui correspondent au comportement du cache. Vous pouvez définir le taux d'échantillonnage sur n'importe quelle valeur comprise entre 0 et 100, avec quatre décimales au maximum.

Lorsque le taux d'échantillonnage est défini sur un nombre inférieur à 100, vous ne pouvez pas contrôler les réponses auxquelles l'`Server-Timing`en-tête est CloudFront ajouté, mais uniquement le pourcentage. Toutefois, vous pouvez ajouter l'en-tête `Pragma` avec une valeur définie sur `server-timing` dans une demande HTTP pour recevoir l'en-tête `Server-Timing` dans la réponse à cette demande. Cela fonctionne quel que soit le taux d'échantillonnage défini. Même lorsque le taux d'échantillonnage est défini sur zéro (0), CloudFront ajoute l'`Server-Timing`en-tête à la réponse si la demande contient l'`Pragma: server-timing`en-tête.

En-tête Server-Timing d'origine

En cas d'échec du cache et que CloudFront la demande est transmise à l'origine, l'origine peut inclure un `Server-Timing` en-tête dans sa réponse à CloudFront. Dans ce cas, CloudFront ajoute ses métriques à l'`Server-Timing`en-tête qu'il a reçu de l'origine. La réponse CloudFront envoyée au spectateur contient un seul `Server-Timing` en-tête qui inclut la valeur provenant de l'origine et les métriques CloudFront ajoutées. La valeur d'en-tête provenant de l'origine peut se trouver à la fin ou entre deux ensembles de mesures qui s' CloudFront ajoutent à l'en-tête.

En cas d'accès au cache, la réponse envoyée au CloudFront visualiseur contient un seul `Server-Timing` en-tête qui inclut uniquement les CloudFront métriques contenues dans la valeur d'en-tête (la valeur de l'origine n'est pas incluse).

Métriques d’en-tête Server-Timing

Lorsque CloudFront vous ajoutez l'`Server-Timing`en-tête à une réponse HTTP, la valeur de l'en-tête contient une ou plusieurs mesures qui peuvent vous aider à mieux comprendre le comportement, les performances CloudFront et votre origine. La liste suivante contient toutes les métriques et leurs valeurs potentielles. Un `Server-Timing` en-tête ne contient que certaines de ces métriques, en fonction de la nature de la demande et de la réponse CloudFront.

Certaines de ces métriques sont incluses dans l’en-tête `Server-Timing` avec un nom uniquement (sans valeur). D'autres sont composées d’un nom et d’une valeur. Lorsqu'une métrique a une valeur, le nom et la valeur sont séparés par un point-virgule (`;`). Lorsque l'en-tête contient plusieurs métriques, celles-ci sont séparées par une virgule (`,`).

cdn-cache-hit

CloudFront a fourni une réponse depuis le cache sans faire de demande à l'origine.

cdn-cache-refresh

CloudFront a fourni une réponse depuis le cache après avoir envoyé une demande à l'origine pour vérifier que l'objet mis en cache est toujours valide. Dans ce cas, l'objet CloudFront n'a pas été récupéré dans son intégralité depuis l'origine.

cdn-cache-miss

CloudFront n'a pas fourni de réponse depuis le cache. Dans ce cas, j' CloudFrontai demandé l'objet complet à l'origine avant de renvoyer la réponse.

cdn-pop

Contient une valeur qui décrit le CloudFront point de présence (POP) qui a traité la demande.

cdn-rid

Contient une valeur avec l'identifiant CloudFront unique de la demande. Vous pouvez utiliser cet identifiant de demande (RID) lors du dépannage de problèmes liés à AWS Support.

cdn-hit-layer

Cette métrique est présente lorsqu'elle CloudFront fournit une réponse depuis le cache sans faire de demande à l'origine. Contient l'une des valeurs suivantes :

- EDGE — CloudFront a fourni la réponse mise en cache à partir d'un emplacement POP.
- REC — CloudFront a fourni la réponse mise en cache à partir d'un emplacement de cache périphérique régional (REC).
- Origin Shield : CloudFront a fourni la réponse mise en cache depuis le REC agissant en tant qu'Origin Shield.

cdn-upstream-layer

Lorsque l'objet complet est CloudFront demandé depuis l'origine, cette métrique est présente et contient l'une des valeurs suivantes :

- EDGE : un emplacement POP a envoyé la demande directement à l'origine.
- REC : un emplacement REC a envoyé la demande directement à l'origine.
- Origin Shield : le REC qui agit en tant qu'Origin Shield a envoyé la demande directement à l'origine.

cdn-upstream-dns

Contient une valeur indiquant le nombre de millisecondes passées à récupérer l'enregistrement DNS pour l'origine. La valeur zéro (0) indique que vous avez CloudFront utilisé un résultat DNS mis en cache ou réutilisé une connexion existante.

cdn-upstream-connect

Contient une valeur indiquant le nombre de millisecondes entre le moment où la demande DNS d'origine est terminée et une connexion TCP (et TLS, le cas échéant) à l'origine. La valeur zéro (0) indique que vous avez CloudFront réutilisé une connexion existante.

cdn-upstream-fbl

Contient une valeur indiquant le nombre de millisecondes entre le moment où la demande HTTP d'origine est terminée et le moment où le premier octet est reçu dans la réponse de l'origine (latence du premier octet).

cdn-downstream-fbl

Contient une valeur indiquant le nombre de millisecondes entre le moment où l'emplacement périphérique a fini de recevoir la demande et celui où il a envoyé le premier octet de la réponse à l'utilisateur.

Exemples d'en-têtes Server-Timing

Voici des exemples d'`Server-Timing`en-têtes qu'un utilisateur peut recevoir CloudFront lorsque le paramètre `Server-Timing` d'en-tête est activé.

Example – échec d'accès au cache

L'exemple suivant montre un `Server-Timing` en-tête qu'un utilisateur peut recevoir lorsque l'objet demandé n'est pas dans le CloudFront cache.

```
Server-Timing: cdn-upstream-layer;desc="EDGE",cdn-upstream-dns;dur=0,cdn-upstream-
connect;dur=114,cdn-upstream-fbl;dur=177,cdn-cache-miss,cdn-pop;desc="PHX50-C2",cdn-
rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==",cdn-downstream-
fbl;dur=436
```

Cet en-tête `Server-Timing` indique ce qui suit :

- La demande d'origine a été envoyée depuis un CloudFront point de présence (POP) (`cdn-upstream-layer;desc="EDGE"`).
- CloudFront a utilisé un résultat DNS mis en cache pour l'origine (`cdn-upstream-dns;dur=0`).
- Il a fallu 114 millisecondes CloudFront pour terminer la connexion TCP (et TLS, le cas échéant) à l'origine (). `cdn-upstream-connect;dur=114`
- Il a fallu 177 millisecondes CloudFront pour recevoir le premier octet de la réponse depuis l'origine, après avoir terminé la requête (). `cdn-upstream-fbl;dur=177`
- L'objet demandé n'était pas dans CloudFront le cache (`cdn-cache-miss`).
- La demande a été reçue à l'emplacement périphérique identifié par le code `PHX50-C2`(`cdn-pop;desc="PHX50-C2"`).

- L'identifiant CloudFront unique de cette demande était `yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==` (`cdn-rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg=="`).
- Il a fallu 436 millisecondes pour CloudFront envoyer le premier octet de la réponse au spectateur, après avoir reçu la demande du spectateur (). `cdn-downstream-fbl;dur=436`

Example – accès au cache

L'exemple suivant montre un `Server-Timing` en-tête qu'un utilisateur peut recevoir lorsque l'objet demandé se trouve dans CloudFront le cache.

```
Server-Timing: cdn-cache-hit,cdn-pop;desc="SEA19-C1",cdn-
rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==",cdn-hit-
layer;desc="REC",cdn-downstream-fbl;dur=137
```

Cet en-tête `Server-Timing` indique ce qui suit :

- L’objet demandé était dans le cache (`cdn-cache-hit`).
- La demande a été reçue à l’emplacement périphérique identifié par le code `SEA19-C1`(`cdn-pop;desc="SEA19-C1"`).
- L'identifiant CloudFront unique de cette demande était `nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==` (`cdn-rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g=="`).
- L’objet demandé a été mis en cache dans un emplacement REC (Regional Edge Cache) (`cdn-hit-layer;desc="REC"`).
- Il a fallu 137 millisecondes pour CloudFront envoyer le premier octet de la réponse au spectateur, après avoir reçu la demande du spectateur (). `cdn-downstream-fbl;dur=137`

Création de politiques relatives aux en-têtes de réponse

Vous pouvez utiliser une politique d'en-têtes de réponse pour spécifier les en-têtes HTTP qu'Amazon CloudFront ajoute ou supprime dans les réponses HTTP. Pour plus d'informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajouter ou supprimer des en-têtes de réponse avec une politique.

Vous pouvez créer une politique d'en-têtes de réponse dans la CloudFront console. Vous pouvez également en créer un AWS CloudFormation en utilisant le AWS Command Line Interface (AWS CLI)

ou l' CloudFront API. Après avoir créé une politique d'en-têtes de réponse, vous l'associez à un ou plusieurs comportements de cache dans une CloudFront distribution.

Avant de créer une politique d'en-têtes de réponse personnalisée, vérifiez si l'une des politiques d'en-têtes de réponse gérées est adaptée à votre cas d'utilisation. Si c'est le cas, vous pouvez l'attacher à votre comportement de cache. De cette façon, vous n'avez pas besoin de créer ou de gérer votre propre politique d'en-têtes de réponse.

Console

Pour créer une politique d'en-têtes de réponses (console)

1. Connectez-vous au AWS Management Console, puis accédez à l'onglet En-têtes de réponse sur la page Politiques de la CloudFront console à https://console.aws.amazon.com/cloudfront/v4/home#/policies/responseHeaders l'adresse.
2. Choisissez Create response headers policy (Créer une politique d'en-têtes de réponses).
3. Dans le formulaire Create response headers policy (Créer une politique d'en-têtes de réponses), procédez comme suit :

   a. Dans le panneau Details (Détails), saisissez un Name (Nom) pour la politique d'en-têtes de réponses et (éventuellement) une Description qui explique le rôle de la politique.

   b. Dans le panneau Cross-origin resource sharing (CORS) (Partage des ressources cross-origine [CORS]), choisissez le bouton bascule Configure CORS (Configurer CORS) et configurez tous les en-têtes CORS que vous souhaitez ajouter à la politique. Si vous souhaitez que les en-têtes configurés remplacent les en-têtes provenant de l'origine, cochez la case Remplacer l'origine. CloudFront

      Pour plus d'informations sur les paramètres d'en-têtes CORS, consultez la section the section called "En-têtes CORS".

   c. Dans Security headers (En-têtes de sécurité), choisissez le bouton bascule et configurez chacun des en-têtes de sécurité que vous souhaitez ajouter à la politique.

      Pour plus d'informations sur les paramètres des en-têtes de sécurité, consultez la section the section called "En-têtes de sécurité".

   d. Dans le panneau Custom headers (En-têtes personnalisés), ajoutez tous les en-têtes personnalisés que vous souhaitez inclure dans la politique.

Pour plus d'informations sur les paramètres d'en-têtes personnalisés, consultez la section the section called “En-têtes personnalisés”.

e. Dans le panneau Supprimer les en-têtes, ajoutez les noms des en-têtes que vous CloudFront souhaitez supprimer de la réponse de l'origine et ne pas inclure dans la réponse envoyée aux CloudFront spectateurs.

   Pour plus d'informations sur les paramètres de suppression d'en-têtes, consultez the section called “Suppression d’en-têtes”.

f. Dans le volet Server-Timing header (En-tête Server-Timing), sélectionnez l’option à bascule Enable (Activer) et saisissez un taux d'échantillonnage (nombre compris entre 0 et 100 inclus).

   Pour plus d'informations sur l'en-tête `Server-Timing`, consultez the section called “En-tête Server-Timing”.

4. Choisissez Create (Créer) pour créer la politique.

Après avoir créé une politique d'en-têtes de réponse, vous pouvez l'associer à un comportement de cache dans une CloudFront distribution.

Pour attacher une politique d’en-têtes de réponses à une distribution existante (console)

1. Ouvrez la page Distributions dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Behaviors (Comportements).
3. Sélectionnez le comportement du cache à mettre à jour, puis choisissez Edit (Modifier).

   Ou, pour créer un comportement de cache, choisissez Create behavior (Créer un comportement).
4. Pour Response headers policy (Politique d’en-têtes de réponses), choisissez la politique à ajouter au comportement du cache.
5. Choisissez Save changes (Enregistrer les modifications) pour mettre à jour le comportement du cache. [Si vous créez un comportement de cache, choisissez Create behavior (Créer un comportement)].

Pour attacher une politique d’en-têtes de réponses à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Pour Response headers policy (Politique d’en-têtes de réponses), choisissez la politique à ajouter au comportement du cache.
4. Définissez les autres paramètres de votre distribution. Pour plus d’informations, consultez la section the section called “Paramètres de distribution”.
5. Choisissez Create distribution (Créer une distribution) pour créer la distribution.

AWS CloudFormation

Pour créer une politique d'en-têtes de réponse avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::ResponseHeadersPolicy` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, pour créer une politique d'en-têtes de réponse.

```
Type: AWS::CloudFront::ResponseHeadersPolicy
Properties:
  ResponseHeadersPolicyConfig:
    Name: EXAMPLE-Response-Headers-Policy
    Comment: Example response headers policy for the documentation
    CorsConfig:
      AccessControlAllowCredentials: false
      AccessControlAllowHeaders:
        Items:
          - '*'
      AccessControlAllowMethods:
        Items:
          - GET
          - OPTIONS
      AccessControlAllowOrigins:
        Items:
          - https://example.com
          - https://docs.example.com
      AccessControlExposeHeaders:
        Items:
          - '*'
      AccessControlMaxAgeSec: 600
```

```
      OriginOverride: false
    CustomHeadersConfig:
      Items:
        - Header: Example-Custom-Header-1
          Value: value-1
          Override: true
        - Header: Example-Custom-Header-2
          Value: value-2
          Override: true
    SecurityHeadersConfig:
      ContentSecurityPolicy:
        ContentSecurityPolicy: default-src 'none'; img-src 'self'; script-src
 'self'; style-src 'self'; object-src 'none'; frame-ancestors 'none'
        Override: false
      ContentTypeOptions: # You don't need to specify a value for 'X-Content-Type-
Options'.
                          # Simply including it in the template sets its value to
 'nosniff'.
        Override: false
      FrameOptions:
        FrameOption: DENY
        Override: false
      ReferrerPolicy:
        ReferrerPolicy: same-origin
        Override: false
      StrictTransportSecurity:
        AccessControlMaxAgeSec: 63072000
        IncludeSubdomains: true
        Preload: true
        Override: false
      XSSProtection:
        ModeBlock: true # You can set ModeBlock to 'true' OR set a value for
 ReportUri, but not both
        Protection: true
        Override: false
    ServerTimingHeadersConfig:
      Enabled: true
      SamplingRate: 50
    RemoveHeadersConfig:
      Items:
        - Header: Vary
        - Header: X-Powered-By
```

Pour plus d'informations, consultez la section AWS::CloudFront::ResponseHeadersPolitique du guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer une politique d'en-têtes de réponse avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-response-headers-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une politique d’en-têtes de réponses (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `response-headers-policy.yaml`. Ce fichier contient tous les paramètres d’entrée de la commande create-response-headers-policy.

```
aws cloudfront create-response-headers-policy --generate-cli-skeleton yaml-input
 > response-headers-policy.yaml
```

2. Ouvrez le fichier `response-headers-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier un nom de politique et la configuration souhaitée pour la politique d'en-têtes de réponse, puis enregistrez le fichier.

   Pour plus d’informations sur les paramètres de la politique d’en-têtes de réponses, consultez la section the section called “Comprendre les politiques relatives aux en-têtes de réponse”.

3. Utilisez la commande suivante pour créer une politique d'en-têtes de réponse. La politique que vous créez utilise les paramètres d'entrée du fichier `response-headers-policy.yaml`.

```
aws cloudfront create-response-headers-policy --cli-input-yaml file://response-
headers-policy.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Il s'agit de l'ID de la politique d'en-têtes de réponse. Vous en avez besoin pour associer la politique au comportement du cache d'une CloudFront distribution.

Pour attacher une politique d'en-têtes de réponses à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *distribution_ID* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes au comportement de cache afin que celui-ci utilise la politique d'en-têtes de réponse.

   - Dans le comportement de cache, ajoutez un champ nommé `ResponseHeadersPolicyId`. Pour la valeur du champ, utilisez l'ID de politique d'en-têtes de réponse que vous avez noté après la création de la politique.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la politique d'en-têtes de réponses. Remplacez *distribution_ID* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une politique d'en-têtes de réponses à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `ResponseHeadersPolicyId`, saisissez l'ID de politique d'en-têtes de réponses que vous avez noté après la création de la politique. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

   Pour de plus amples informations sur les paramètres de distribution, veuillez consulter Référence des paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Pour créer une politique d'en-têtes de réponse avec l' CloudFront API, utilisez CreateResponseHeadersPolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez the section called “Comprendre les politiques relatives aux en-têtes de réponse” la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une politique d'en-têtes de réponses, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la politique d'en-têtes de demande dans le champ `ResponseHeadersPolicyId`, dans un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utiliser des politiques d'en-têtes de réponse gérés

Avec une politique d'en-têtes de CloudFront réponse, vous pouvez spécifier les en-têtes HTTP qu'Amazon CloudFront supprime ou ajoute dans les réponses qu'il envoie aux utilisateurs. Pour plus d'informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajouter ou supprimer des en-têtes de réponse avec une politique.

CloudFront fournit des politiques d'en-têtes de réponse gérés que vous pouvez associer aux comportements du cache dans vos CloudFront distributions. Avec une politique d’en-têtes de réponses gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre politique. Les politiques gérées contiennent des ensembles d'en-têtes de réponses HTTP pour les cas d'utilisation courants.

Pour utiliser une politique d’en-têtes de réponses gérée, attachez-la à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une politique d'en-têtes de réponse personnalisée. Toutefois, au lieu de créer une nouvelle politique, vous attachez l'une des politiques gérées. Vous attachez la politique soit par son nom (avec la console), soit par son identifiant (avec AWS CloudFormation AWS CLI, le ou les AWS SDK). Les noms et les identifiants sont répertoriés dans la section suivante.

Pour plus d’informations, consultez the section called “Création de politiques relatives aux en-têtes de réponse”.

Les rubriques suivantes décrivent les politiques d'en-têtes de réponse gérées que vous pouvez utiliser.

Rubriques

- Cors-et- SecurityHeadersPolicy
- CORS-With-Preflight
- CORS- - with-preflight-and SecurityHeadersPolicy
- SecurityHeadersPolicy
- SimpleCORS

Cors-et- SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS simples de n'importe quelle origine. Cette politique ajoute également un ensemble d'en-têtes de sécurité à toutes les réponses

CloudFront envoyées aux spectateurs. Cette politique combine les politiques the section called “SimpleCORS” et the section called “SecurityHeadersPolicy” en une seule.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`e61eb60c-9c35-4d20-a928-2b84e02af89c`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Origin`	`*`	Non
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

CORS-With-Preflight

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS de n'importe quelle origine, y compris les demandes de contrôle en amont. Pour les requêtes de pré-vol (à l'aide de la `OPTIONS` méthode HTTP), CloudFront ajoute les trois en-têtes suivants à la réponse. Pour les requêtes CORS simples, CloudFront ajoute uniquement l'`Access-Control-Allow-Origin`en-tête.

Si la réponse CloudFront reçue de l'origine inclut l'un de ces en-têtes, CloudFront utilise l'en-tête reçu (et sa valeur) dans sa réponse au spectateur. CloudFrontn'utilise pas l'en-tête dans cette politique.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`5cc3b908-e619-4b99-88e5-2cf7f45965bd`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Methods`	`DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`	Non
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	

CORS- - with-preflight-and SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS de n'importe quelle origine. Cela inclut les demandes de contrôle en amont. Cette politique ajoute également un ensemble d'en-têtes de sécurité à toutes les réponses CloudFront envoyées aux spectateurs. Cette politique combine les politiques the section called “CORS-With-Preflight” et the section called “SecurityHeadersPolicy” en une seule.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`eaab4381-ed33-4a86-88ca-d9558dc6cd63`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Methods`	`DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT`	Non
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour ajouter un ensemble d'en-têtes de sécurité à toutes les réponses CloudFront envoyées aux utilisateurs. Pour plus d'informations sur ces en-têtes de sécurité, consultez les recommandations de sécurité web de Mozilla.

Avec cette politique d'en-têtes de réponse, des CloudFront ajouts `X-Content-Type-Options: nosniff` à toutes les réponses. C'est le cas lorsque la réponse CloudFront reçue de l'origine incluait cet en-tête et lorsque ce n'était pas le cas. Pour tous les autres en-têtes de cette politique, si la

réponse CloudFront reçue de l'origine inclut l'en-tête, CloudFront utilise l'en-tête reçu (et sa valeur) dans sa réponse au spectateur. Il n'utilise pas l'en-tête de cette politique.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`67f7725c-6f97-4210-82d7-5512b31e9d03`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

SimpleCORS

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS simples de n'importe quelle origine. Avec cette politique, CloudFront ajoute l'en-tête `Access-Control-Allow-Origin: *` à toutes les réponses pour les requêtes CORS simples.

Si la réponse CloudFront reçue de l'origine inclut l'`Access-Control-Allow-Origin`en-tête, CloudFront utilise cet en-tête (et sa valeur) dans sa réponse au spectateur. CloudFront n'utilise pas l'en-tête dans cette politique.

Lors de l'utilisation AWS CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`60669652-455b-4ae9-85a4-c4c02393f86c`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Origin`	*	Non

Comportement des demandes et des réponses

Les sections suivantes expliquent comment CloudFront traite les demandes des visiteurs et les transmet à votre Amazon S3 ou à votre origine personnalisée, et comment CloudFront traite les réponses provenant de votre origine, notamment comment CloudFront traite et met en cache les codes de statut HTTP 4xx et 5xx.

Rubriques

Comment CloudFront traite les requêtes HTTP et HTTPS

Pour les origines d'Amazon S3, CloudFront accepte par défaut les requêtes via les protocoles HTTP et HTTPS pour les objets d'une CloudFront distribution. CloudFront transmet ensuite les demandes à votre compartiment Amazon S3 en utilisant le même protocole que celui dans lequel les demandes ont été effectuées.

Pour les origines personnalisées, lorsque vous créez votre distribution, vous pouvez spécifier le mode d' CloudFrontaccès à votre origine : HTTP uniquement ou en utilisant le protocole utilisé par le lecteur. Pour plus d'informations sur le CloudFront traitement des requêtes HTTP et HTTPS pour des origines personnalisées, consultezProtocoles.

Pour plus d’informations sur la façon de restreindre votre distribution pour que les utilisateurs finaux puissent uniquement accéder aux objets à l’aide de HTTPS, consultez Utilisez le protocole HTTPS avec CloudFront.

> **Note**
>
> Les frais pour les requêtes HTTPS sont plus élevés que ceux pour les requêtes HTTP. Pour plus d'informations sur les taux de facturation, consultez la section CloudFront tarification.

Comportement des demandes et des réponses pour les origines Amazon S3 Origins

Pour comprendre comment CloudFront traite les demandes et les réponses lorsque vous utilisez Amazon S3 comme origine, consultez les sections suivantes :

Rubriques

Comment CloudFront traite et transmet les demandes à votre Amazon S3 d'origine

Découvrez comment CloudFront traite les demandes des visiteurs et les transmet à votre point d'origine Amazon S3.

Table des matières

- Protocoles
- Chaînes de requête
- Délai d'attente et tentatives de connexion à l'origine
- Délai de réponse de l'origine
- Demandes simultanées pour le même objet (réduction des demandes)

Durée de conservation dans le cache et durée de vie minimale

Pour contrôler la durée pendant laquelle vos objets restent dans CloudFront le cache avant CloudFront de transmettre une autre demande à votre origine, vous pouvez :

- Configurer votre origine pour ajouter un `Cache-Control` ou un champ d'en-tête `Expires` à chaque objet.
- Spécifiez une valeur pour le TTL minimal dans les comportements CloudFront du cache.
- Utiliser la valeur par défaut de 24 heures.

Pour de plus amples informations, veuillez consulter Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Adresses IP client

Si un utilisateur envoie une demande CloudFront et n'inclut pas d'en-tête de `X-Forwarded-For` demande, CloudFront obtient l'adresse IP du spectateur à partir de la connexion TCP, ajoute un `X-Forwarded-For` en-tête qui inclut l'adresse IP et transmet la demande à l'origine. Par exemple, s'il CloudFront obtient l'adresse IP `192.0.2.2` de la connexion TCP, il transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.2
```

Si un utilisateur envoie une demande CloudFront et inclut un en-tête de `X-Forwarded-For` demande, CloudFront obtient son adresse IP via la connexion TCP, l'ajoute à la fin de l'`X-Forwarded-For`en-tête et transmet la demande à l'origine. Par exemple, si la demande du spectateur inclut `X-Forwarded-For: 192.0.2.4,192.0.2.3` et CloudFront obtient l'adresse IP `192.0.2.2` de la connexion TCP, elle transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

> **Note**
>
> L'en-tête `X-Forwarded-For` contient les adresses IPv4 (par exemple, 192.0.2.44) et les adresses IPv6 (par exemple, 2001:0db8:85a3::8a2e:0370:7334).

Requêtes GET conditionnelles

Lorsqu'il CloudFront reçoit une demande pour un objet expiré depuis un cache périphérique, il la transmet à l'origine Amazon S3 pour obtenir la dernière version de l'objet ou pour obtenir la confirmation d'Amazon S3 que le cache CloudFront périphérique possède déjà la dernière version. Lorsque Amazon S3 a initialement envoyé l'objet à CloudFront, il a inclus une `ETag` valeur et une `LastModified` valeur dans la réponse. Dans la nouvelle demande transmise CloudFront à Amazon S3, CloudFront ajoute l'un des en-têtes suivants ou les deux :

- Un en-tête `If-Match` ou `If-None-Match` qui contient la valeur `ETag` pour la version expirée de l'objet.
- Un en-tête `If-Modified-Since` qui contient la valeur `LastModified` pour la version expirée de l'objet.

Amazon S3 utilise ces informations pour déterminer si l'objet a été mis à jour et, par conséquent, s'il convient de renvoyer l'objet dans son intégralité CloudFront ou de renvoyer uniquement un code d'état HTTP 304 (non modifié).

Cookies

Amazon S3 ne traite pas les cookies. Si vous configurez un comportement de cache pour transférer des cookies vers une origine Amazon S3, CloudFront transférez les cookies, mais Amazon S3 les ignore. Toutes les demandes futures pour le même objet, que vous faites varier le cookie ou non, sont servies à partir de l'objet existant dans le cache.

Partage des ressources cross-origin (CORS)

Si vous CloudFront souhaitez respecter les paramètres de partage de ressources entre origines d'Amazon S3, configurez CloudFront pour transférer les en-têtes sélectionnés vers Amazon S3. Pour plus d'informations, consultez Contenu du cache basé sur les en-têtes des demandes.

Demandes GET qui incluent un corps de texte

Si une `GET` demande d'utilisateur inclut un corps, CloudFront renvoie un code d'état HTTP 403 (Interdit) au lecteur.

Méthodes HTTP

Si vous configurez CloudFront pour traiter toutes les méthodes HTTP qu'il prend en charge, CloudFront accepte les demandes suivantes des utilisateurs et les transmet à votre point d'origine Amazon S3 :

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront ne met pas en cache les réponses aux demandes qui utilisent les autres méthodes.

Si vous souhaitez utiliser des téléchargements en plusieurs parties pour ajouter des objets à un compartiment Amazon S3, vous devez ajouter un contrôle CloudFront d'accès à l'origine (OAC) à votre distribution et donner à l'OAC les autorisations nécessaires. Pour plus d'informations, consultez the section called “Restreindre l'accès à une origine Amazon Simple Storage Service”.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transférer vers Amazon S3 toutes les méthodes HTTP compatibles, CloudFront vous devez créer un CloudFront OAC pour restreindre l'accès à votre contenu Amazon S3 et donner à l'OAC les autorisations requises. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes parce que vous souhaitez les utiliser, vous devez configurer les `PUT` politiques relatives aux compartiments Amazon S3 afin de traiter les `DELETE` demandes de manière appropriée afin que les utilisateurs ne puissent pas supprimer les ressources que vous ne souhaitez pas voir

supprimées. Pour plus d'informations, consultez the section called "Restreindre l'accès à une origine Amazon Simple Storage Service".

Pour de plus amples informations sur les opérations prises en charge par Amazon S3, veuillez consulter la documentation Amazon S3.

En-têtes de requête HTTP qui CloudFront suppriment ou mettent à jour

CloudFront supprime ou met à jour certains en-têtes avant de transférer les demandes à votre origine Amazon S3. Pour la plupart des en-têtes, ce comportement est le même que pour les origines personnalisées. Pour obtenir la liste complète des en-têtes de requête HTTP et leur mode CloudFront de traitement, consultezEn-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3).

Longueur maximale d'une demande et longueur maximale d'une URL

La longueur maximale d'une demande, avec le chemin, la chaîne de requête (le cas échéant) et les en-têtes inclus, est de 20480 octets.

CloudFront construit une URL à partir de la requête. La longueur maximale de cette URL est de 8 192 caractères.

Si une demande ou une URL dépasse la longueur maximale, CloudFront renvoie le code d'état HTTP 413 (Request Entity Too Large) au visualiseur, puis met fin à la connexion TCP avec le visualiseur.

OCSP Stapling

Lorsqu'un utilisateur soumet une demande HTTPS pour un objet, CloudFront il doit confirmer auprès de l'autorité de certification (CA) que le certificat SSL du domaine n'a pas été révoqué. L'agrafage OCSP accélère la validation du certificat en permettant de valider le certificat et de CloudFront mettre en cache la réponse de l'autorité de certification, de sorte que le client n'a pas besoin de valider le certificat directement auprès de l'autorité de certification.

L'amélioration des performances de l'agrafage OCSP est plus prononcée lorsque vous recevez de CloudFront nombreuses requêtes HTTPS pour des objets du même domaine. Chaque serveur situé dans un emplacement CloudFront périphérique doit soumettre une demande de validation distincte. Lorsqu'il CloudFront reçoit un grand nombre de requêtes HTTPS pour le même domaine, chaque serveur situé à la périphérie reçoit rapidement une réponse de l'autorité de certification qu'il peut agrafer sur un paquet dans le cadre de la poignée de main SSL. Lorsque le téléspectateur est

convaincu que le certificat est valide, il CloudFront peut servir l'objet demandé. Si votre distribution ne reçoit pas beaucoup de trafic dans un emplacement CloudFront périphérique, les nouvelles demandes sont plus susceptibles d'être dirigées vers un serveur qui n'a pas encore validé le certificat auprès de l'autorité de certification. Dans ce cas, le visualiseur exécute séparément l'étape de validation et le CloudFront serveur sert l'objet. Ce CloudFront serveur soumet également une demande de validation à l'autorité de certification. Ainsi, la prochaine fois qu'il recevra une demande contenant le même nom de domaine, il recevra une réponse de validation de la part de l'autorité de certification.

Protocoles

CloudFront transmet les requêtes HTTP ou HTTPS au serveur d'origine en fonction du protocole de la demande du visualiseur, HTTP ou HTTPS.

> **Important**
>
> Si votre compartiment Amazon S3 est configuré comme point de terminaison de site Web, vous ne pouvez pas le configurer CloudFront pour utiliser le protocole HTTPS pour communiquer avec votre origine, car Amazon S3 ne prend pas en charge les connexions HTTPS dans cette configuration.

Chaînes de requête

Vous pouvez configurer si CloudFront les paramètres de chaîne de requête sont transmis à votre origine Amazon S3. Pour plus d'informations, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

Délai d'attente et tentatives de connexion à l'origine

Le délai d'expiration de la connexion d'origine est le nombre de secondes d' CloudFront attente lorsque vous essayez d'établir une connexion avec l'origine.

Les tentatives de connexion à l'origine correspondent au nombre de CloudFront tentatives de connexion à l'origine.

Ensemble, ces paramètres déterminent la durée des CloudFront tentatives de connexion à l'origine avant de basculer vers l'origine secondaire (dans le cas d'un groupe d'origine) ou de renvoyer une réponse d'erreur au lecteur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de

10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

Pour de plus amples informations, veuillez consulter Contrôlez les délais et les tentatives d'origine.

Délai de réponse de l'origine

Le délai de réponse de l'origine, également appelé délai d'attente des opérations de lecture depuis l'origine ou délai de demande à l'origine, s'applique aux deux valeurs suivantes :

- Durée, en secondes, d' CloudFront attente d'une réponse après le transfert d'une demande à l'origine.
- Temps d' CloudFront attente, en secondes, après réception d'un paquet de réponse provenant de l'origine et avant de recevoir le paquet suivant.

CloudFront le comportement dépend de la méthode HTTP de la requête du spectateur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas dans les 30 secondes ou cesse de répondre pendant 30 secondes, CloudFront interrompt la connexion. Si le nombre spécifié de tentatives de connexion d'origine est supérieur à 1, CloudFront réessaie pour obtenir une réponse complète. CloudFront essaie jusqu'à 3 fois, selon la valeur du paramètre des tentatives de connexion d'origine. Si l'origine ne répond pas lors de la dernière tentative, elle CloudFront ne réessaie pas tant qu'elle n'a pas reçu une autre demande de contenu sur la même origine.
- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` demandes : si l'origine ne répond pas dans les 30 secondes, CloudFront interrompt la connexion et n'essaie pas de la contacter à nouveau. Le client peut soumettre à nouveau la demande si nécessaire.

Vous ne pouvez pas modifier le délai de réponse pour une origine Amazon S3 (un compartiment S3 qui n'est pas configuré avec un hébergement de site web statique).

Demandes simultanées pour le même objet (réduction des demandes)

Lorsqu'un emplacement CloudFront périphérique reçoit une demande pour un objet et que celui-ci n'est pas dans le cache ou que l'objet mis en cache a expiré, envoie CloudFront immédiatement la demande à l'origine. Toutefois, s'il existe des demandes simultanées pour le même objet, c'est-à-dire si des demandes supplémentaires pour le même objet (avec la même clé de cache) arrivent à l'emplacement périphérique avant de CloudFront recevoir la réponse à la première demande, faites

CloudFront une pause avant de transmettre les demandes supplémentaires à l'origine. Cette brève pause permet de réduire la charge sur l'origine. CloudFront envoie la réponse de la demande initiale à toutes les demandes qu'elle a reçues pendant sa pause. Ce processus se nomme la réduction des demandes. Dans CloudFront les journaux, la première demande est identifiée comme étant `Miss` dans le `x-edge-result-type` champ, et les demandes réduites sont identifiées comme un`Hit`. Pour plus d'informations sur CloudFront les journaux, consultezthe section called “CloudFront et journalisation des fonctions Edge”.

CloudFront réduit uniquement les demandes qui partagent une clé de cache. Si les demandes supplémentaires ne partagent pas la même clé de cache parce que, par exemple, vous avez configuré CloudFront le cache en fonction des en-têtes de demande, des cookies ou des chaînes de requête, CloudFront transfère toutes les demandes avec une clé de cache unique à votre origine.

Si vous souhaitez empêcher le regroupement de toutes les demandes, vous pouvez utiliser la politique de cache géré`CachingDisabled`, qui empêche également la mise en cache. Pour plus d’informations, consultez Utiliser des politiques de cache gérées.

Si vous souhaitez empêcher la réduction des demandes pour des objets spécifiques, vous pouvez définir le TTL minimum pour le comportement du cache sur 0 et configurer l'origine à envoyer`Cache-Control: private`,, `Cache-Control: no-store` `Cache-Control: no-cache`Cache-Control: `max-age=0`, ou. `Cache-Control: s-maxage=0` Ces configurations augmenteront la charge sur votre origine et introduiront une latence supplémentaire pour les demandes simultanées qui sont suspendues pendant l' CloudFront attente de la réponse à la première demande.

> **Important**
>
> Actuellement, la réduction des demandes CloudFront n'est pas prise en charge si vous activez le transfert de cookies dans la politique de cache, la politique de demande d'origine ou les anciens paramètres de cache.

Comment CloudFront traite les réponses provenant de votre Amazon S3

Découvrez comment CloudFront traite les réponses provenant de votre Amazon S3 d'origine.

Table des matières

- Taille de fichier maximale pouvant être mise en cache
- Redirections

Requêtes annulées

Si un objet ne se trouve pas dans le cache périphérique et si un utilisateur met fin à une session (par exemple, ferme un navigateur) après avoir récupéré l'objet depuis votre origine mais avant de pouvoir livrer l'objet demandé, il CloudFront ne CloudFront met pas l'objet en cache dans l'emplacement périphérique.

En-têtes de réponse HTTP qui CloudFront suppriment ou mettent à jour

CloudFront supprime ou met à jour les champs d'en-tête suivants avant de transmettre la réponse de votre origine Amazon S3 au lecteur :

- `X-Amz-Id-2`
- `X-Amz-Request-Id`
- `Set-Cookie`— Si vous configurez CloudFront pour transférer les cookies, le champ `Set-Cookie` d'en-tête sera transmis aux clients. Pour plus d'informations, consultez Contenu du cache basé sur les cookies.
- `Trailer`
- `Transfer-Encoding`— Si votre origine Amazon S3 renvoie ce champ d'en-tête, CloudFront définissez la valeur sur `chunked` avant de renvoyer la réponse au lecteur.
- `Upgrade`
- `Via`— CloudFront définit la valeur suivante dans la réponse au visualiseur :

  `Via: version_http chaîne_alphanumérique.cloudfront.net (CloudFront)`

  Par exemple, la valeur est similaire à la suivante :

  `Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)`

Taille de fichier maximale pouvant être mise en cache

La taille maximale d'un corps de réponse enregistré CloudFront dans son cache est de 50 Go. Cette taille inclut les réponses de transfert fragmentées qui ne spécifient pas la valeur d'en-tête `Content-Length`.

Vous pouvez utiliser CloudFront pour mettre en cache un objet dont la taille est supérieure à cette taille en utilisant des demandes de plage pour demander les objets dans des parties dont la taille est inférieure ou égale à 50 Go. CloudFrontmet en cache ces parties car chacune d'elles a une taille inférieure ou égale à 50 Go. Une fois que l'utilisateur a récupéré toutes les parties de l'objet, il peut reconstruire l'objet d'origine plus large. Pour plus d'informations, consultez Utiliser les demandes de plage pour mettre en cache de large objets.

Redirections

Vous pouvez configurer un compartiment Amazon S3 pour rediriger toutes les demandes vers un autre nom d'hôte ; il peut s'agir d'un autre compartiment Amazon S3 ou d'un serveur HTTP. Si vous configurez un compartiment pour rediriger toutes les demandes et si le compartiment est l'origine d'une CloudFront distribution, nous vous recommandons de le configurer pour rediriger toutes les demandes vers une CloudFront distribution en utilisant soit le nom de domaine de la distribution (par exemple, d111111abcdef8.cloudfront.net) soit un autre nom de domaine (un CNAME) associé à une distribution (par exemple, exemple.com). Dans le cas contraire, les demandes CloudFront des utilisateurs sont ignorées et les objets sont servis directement depuis la nouvelle origine.

> **Note**
>
> Si vous redirigez des demandes vers un nom de domaine alternatif, vous devez également mettre à jour le service DNS pour votre domaine en ajoutant un enregistrement CNAME. Pour de plus amples informations, veuillez consulter Utilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames).

Voici ce qui se passe lorsque vous configurez un compartiment pour rediriger toutes les demandes :

1. Un utilisateur (par exemple, un navigateur) demande un objet à CloudFront.
2. CloudFront transmet la demande au compartiment Amazon S3 qui est à l'origine de votre distribution.
3. Amazon S3 renvoie un code de statut HTTP 301 (Déplacé de façon permanente), ainsi que le nouvel emplacement.
4. CloudFront met en cache le code d'état de redirection et le nouvel emplacement, et renvoie les valeurs au visualiseur. CloudFront ne suit pas la redirection pour récupérer l'objet depuis le nouvel emplacement.

5. Le visualiseur envoie une autre demande pour l'objet, mais cette fois, il indique le nouvel emplacement d'où il provient CloudFront :

   - Si le compartiment Amazon S3 redirige toutes les demandes vers une CloudFront distribution, en utilisant le nom de domaine de la distribution ou un autre nom de domaine, CloudFront demande l'objet depuis le compartiment Amazon S3 ou le serveur HTTP du nouvel emplacement. Lorsque le nouvel emplacement renvoie l'objet, le CloudFront renvoie au visualiseur et le met en cache dans un emplacement périphérique.
   - Si le compartiment Amazon S3 redirige les demandes vers un autre emplacement, la deuxième demande est ignorée CloudFront. Le compartiment Amazon S3 ou le serveur HTTP du nouvel emplacement renvoie l'objet directement au visualiseur, de sorte que l'objet n'est jamais mis en cache dans un cache CloudFront périphérique.

Comportement des demandes et des réponses pour les origines personnalisées

Pour comprendre comment CloudFront traite les demandes et les réponses lorsque vous utilisez des origines personnalisées, consultez les sections suivantes :

Rubriques

Comment CloudFront traite et transmet les demandes à votre point d'origine personnalisé

Découvrez comment CloudFront traite les demandes des visiteurs et les transmet à votre origine personnalisée.

Table des matières

- Compression
- Demandes conditionnelles
- Cookies
- Partage des ressources cross-origin (CORS)
- Chiffrement
- Demandes GET qui incluent un corps de texte
- Méthodes HTTP
- En-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3)
- Version de HTTP
- Longueur maximale d’une demande et longueur maximale d’une URL
- OCSP Stapling
- Connexions persistantes
- Protocoles
- Chaînes de requête
- Délai d’attente et tentatives de connexion à l’origine
- Délai de réponse de l’origine
- Demandes simultanées pour le même objet (réduction des demandes)
- En-tête User-Agent

Authentification

Si vous transférez l'`Authorization`en-tête à votre origine, vous pouvez ensuite configurer votre serveur d'origine pour demander l'authentification du client pour les types de demandes suivants :

- `DELETE`
- `GET`
- `HEAD`
- `PATCH`
- `PUT`
- `POST`

Pour les OPTIONS demandes, l'authentification du client ne peut être configurée que si vous utilisez les CloudFront paramètres suivants :

- CloudFront est configuré pour transmettre l'Authorizationen-tête à votre origine
- CloudFront est configuré pour ne pas mettre en cache la réponse aux OPTIONS demandes

Pour plus d'informations, consultez Configurer CloudFront pour transférer l'Authorizationen-tête.

Vous pouvez utiliser le protocole HTTP ou HTTPS pour transférer les demandes vers votre serveur d'origine. Pour plus d'informations, consultez Utilisez le protocole HTTPS avec CloudFront.

Durée de conservation dans le cache et durée de vie minimale

Pour contrôler la durée pendant laquelle vos objets restent dans CloudFront le cache avant CloudFront de transmettre une autre demande à votre origine, vous pouvez :

- Configurer votre origine pour ajouter un Cache-Control ou un champ d'en-tête Expires à chaque objet.
- Spécifiez une valeur pour le TTL minimal dans les comportements CloudFront du cache.
- Utiliser la valeur par défaut de 24 heures.

Pour de plus amples informations, veuillez consulter Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Adresses IP client

Si un utilisateur envoie une demande sans CloudFront inclure d'en-tête de X-Forwarded-For demande, CloudFront obtient l'adresse IP du spectateur à partir de la connexion TCP, ajoute un X-Forwarded-For en-tête incluant l'adresse IP et transmet la demande à l'origine. Par exemple, s'il CloudFront obtient l'adresse IP 192.0.2.2 de la connexion TCP, il transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.2
```

Si un utilisateur envoie une demande CloudFront et inclut un en-tête de X-Forwarded-For demande, CloudFront obtient son adresse IP via la connexion TCP, l'ajoute à la fin de l'X-Forwarded-Foren-tête et transmet la demande à l'origine. Par exemple, si la demande du spectateur inclut X-Forwarded-For: 192.0.2.4,192.0.2.3 et CloudFront obtient l'adresse IP 192.0.2.2 de la connexion TCP, elle transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Certaines applications, telles que les équilibreurs de charge (y compris Elastic Load Balancing), les pare-feux d'applications Web, les proxys inverses, les systèmes de prévention des intrusions et API Gateway, ajoutent l'adresse IP du serveur CloudFront périphérique qui a transmis la demande à la fin de l'en-tête. `X-Forwarded-For` Par exemple, si elle est CloudFront incluse `X-Forwarded-For: 192.0.2.2` dans une demande transmise à ELB et si l'adresse IP du serveur CloudFront Edge est 192.0.2.199, la demande que reçoit votre instance EC2 contient l'en-tête suivant :

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> L'en-tête `X-Forwarded-For` contient les adresses IPv4 (par exemple, 192.0.2.44) et les adresses IPv6 (par exemple, 2001:0db8:85a3::8a2e:0370:7334).
> Notez également que l'`X-Forwarded-For`en-tête peut être modifié par chaque nœud sur le chemin vers le serveur actuel (CloudFront). Pour plus d'informations, consultez la section 8.1 de la RFC 7239. Vous pouvez également modifier l'en-tête à l'aide des fonctions de calcul de CloudFront pointe.

Authentification SSL côté client

CloudFront ne prend pas en charge l'authentification client avec des certificats SSL côté client. Si une origine demande un certificat côté client, elle CloudFront supprime la demande.

Compression

Pour plus d'informations, consultez Servir des fichiers compressés.

Demandes conditionnelles

Lorsqu'il CloudFront reçoit une demande pour un objet expiré depuis un cache périphérique, il la transmet à l'origine soit pour obtenir la dernière version de l'objet, soit pour obtenir de l'origine la confirmation que le cache CloudFront périphérique possède déjà la dernière version. Généralement, lorsque l'origine a envoyé l'objet pour la dernière fois CloudFront, elle a inclus une `ETag` valeur, une `LastModified` valeur ou les deux valeurs dans la réponse. Dans la nouvelle demande transmise CloudFront à l'origine, ajoutez l' CloudFront un des éléments suivants ou les deux :

- Un en-tête `If-Match` ou `If-None-Match` qui contient la valeur `ETag` pour la version expirée de l'objet.
- Un en-tête `If-Modified-Since` qui contient la valeur `LastModified` pour la version expirée de l'objet.

L'origine utilise ces informations pour déterminer si l'objet a été mis à jour et, par conséquent, s'il convient de renvoyer l'objet entier CloudFront ou de renvoyer uniquement un code d'état HTTP 304 (non modifié).

> **Note**
>
> `If-Modified-Since`et les demandes `If-None-Match` conditionnelles ne sont pas prises en charge lorsqu'elle CloudFront est configurée pour transférer les cookies (tous ou un sous-ensemble).
> Pour plus d'informations, consultez Contenu du cache basé sur les cookies.

Cookies

Vous pouvez configurer CloudFront pour transférer les cookies à votre origine. Pour plus d'informations, consultez Contenu du cache basé sur les cookies.

Partage des ressources cross-origin (CORS)

Si vous souhaitez CloudFront respecter les paramètres de partage de ressources entre origines, configurez CloudFront pour transférer l'`Origin`en-tête vers votre origine. Pour plus d'informations, consultez Contenu du cache basé sur les en-têtes des demandes.

Chiffrement

Vous pouvez demander aux utilisateurs d'utiliser le protocole HTTPS pour envoyer des demandes CloudFront et de CloudFront transférer les demandes à votre origine personnalisée en utilisant le protocole utilisé par le lecteur. Pour plus d'informations, consultez les paramètres de distribution suivants :

- Viewer Protocol Policy
- Protocole (origines personnalisées uniquement)

CloudFront transmet les requêtes HTTPS au serveur d'origine à l'aide des protocoles SSLv3, TLSv1.0, TLSv1.1 et TLSv1.2. Pour les origines personnalisées, vous pouvez choisir les protocoles SSL que vous CloudFront souhaitez utiliser pour communiquer avec votre origine :

- Si vous utilisez la CloudFront console, choisissez les protocoles en cochant les cases Protocoles SSL d'origine. Pour plus d'informations, consultez Créer une distribution.
- Si vous utilisez l' CloudFront API, spécifiez les protocoles à l'aide de l'`OriginSslProtocols`élément. Pour plus d'informations, consultez OriginSslProtocolset consultez DistributionConfigle Amazon CloudFront API Reference.

Si l'origine est un compartiment Amazon S3, utilise CloudFront toujours TLSv1.2.

> **Important**
>
> Les autres versions de SSL et TLS ne sont pas prises en charge.

Pour plus d'informations sur l'utilisation du protocole HTTPS avec CloudFront, consultezUtilisez le protocole HTTPS avec CloudFront. Pour obtenir la liste des chiffrements compatibles CloudFront avec les communications HTTPS entre les utilisateurs et CloudFront, et entre CloudFront et votre origine, voir. Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront

Demandes GET qui incluent un corps de texte

Si une `GET` demande d'utilisateur inclut un corps, CloudFront renvoie un code d'état HTTP 403 (Interdit) au lecteur.

Méthodes HTTP

Si vous configurez CloudFront pour traiter toutes les méthodes HTTP qu'il prend en charge, CloudFront accepte les demandes suivantes des utilisateurs et les transmet à votre origine personnalisée :

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`

- `POST`
- `PUT`

CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront ne met pas en cache les réponses aux demandes qui utilisent les autres méthodes.

Pour plus d'informations sur la façon de configurer si votre origine personnalisée traite ces méthodes, consultez la documentation de votre origine.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transmettre à votre origine toutes les méthodes HTTP compatibles, configurez votre serveur d'origine pour qu' CloudFront il gère toutes les méthodes. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes parce que vous souhaitez les utiliser`POST`, vous devez configurer votre serveur d'origine pour qu'il gère les `DELETE` demandes de manière appropriée afin que les utilisateurs ne puissent pas supprimer les ressources que vous ne souhaitez pas qu'ils suppriment. Pour plus d'informations, consultez la documentation de votre serveur HTTP.

En-têtes et CloudFront comportement des requêtes HTTP (personnalisés et origines d'Amazon S3)

Le tableau suivant répertorie les en-têtes de requête HTTP que vous pouvez transmettre aux origines Amazon S3 et personnalisée (avec les exceptions qui sont notées). Pour chaque en-tête, le tableau comprend des informations sur les points suivants :

- CloudFront comportement si vous ne configurez pas CloudFront pour transférer l'en-tête vers votre origine, ce qui entraîne la mise en cache CloudFront de vos objets en fonction des valeurs de l'en-tête.
- Si vous pouvez configurer CloudFront pour mettre en cache des objets en fonction des valeurs d'en-tête de cet en-tête.

  Vous pouvez configurer CloudFront pour mettre en cache des objets en fonction des valeurs `User-Agent` des en-têtes `Date` et, mais nous ne le recommandons pas. Ces en-têtes ont de nombreuses valeurs possibles, et la mise en cache basée sur leurs valeurs entraînerait le transfert d'un plus grand nombre de demandes CloudFront vers votre origine.

Pour plus d'informations sur la mise en cache selon des valeurs d'en-tête, consultez Contenu du cache basé sur les en-têtes des demandes.

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
En-têtes définis par un tiers	Paramètres de cache existants : CloudFront transmet les en-têtes à votre source.	Oui
`Accept`	CloudFront supprime l'en-tête.	Oui
`Accept-Charset`	CloudFront supprime l'en-tête.	Oui
`Accept-Encoding`	Si la valeur contient `gzip` ou `ubr`, CloudFront transmet un `Accept-Encoding` en-tête normalisé à votre origine. Pour plus d'informations, consultez Prise en charge de la compression et Servir des fichiers compressés.	Oui
`Accept-Language`	CloudFront supprime l'en-tête.	Oui
`Authorization`	• `GET` et `HEAD` demandes : CloudFront supprime le champ `Authorization` d'en-tête avant de transférer la demande à votre origine. • `OPTIONS` demandes — CloudFront supprime le champ `Authorization` d'en-tête avant de	Oui

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
	transférer la demande à votre origine si vous configurez CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront transmet le champ `Authorization` d'en-tête à votre origine si vous ne configurez pas CloudFront pour mettre en cache les réponses aux requêtes OPTIONS. • `DELETE`, `PATCH`, `POST`, et `PUT` demandes : CloudFront ne supprime pas le champ d'en-tête avant de transférer la demande à votre origine.	
`Cache-Control`	CloudFront transmet l'en-tête à votre origine.	Non
`CloudFront-Forwarded-Proto`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configurer la mise en cache en fonction du protocole de la demande.	Oui
`CloudFront-Is-Desktop-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`CloudFront-Is-Mobile-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui
`CloudFront-Is-Tablet-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui
`CloudFront-Viewer-Country`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine.	Oui
`Connection`	CloudFront remplace cet en-tête par `Connection: Keep-Alive` avant de transmettre la demande à votre origine.	Non
`Content-Length`	CloudFront transmet l'en-tête à votre origine.	Non
`Content-MD5`	CloudFront transmet l'en-tête à votre origine.	Oui
`Content-Type`	CloudFront transmet l'en-tête à votre origine.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Cookie`	Si vous configurez CloudFront pour transférer les cookies, le champ d'`Cookie`en-tête sera redirigé vers votre origine. Si ce n'est pas le cas, CloudFront supprime le champ `Cookie` d'en-tête. Pour plus d'informations, consultez Contenu du cache basé sur les cookies.	Non
`Date`	CloudFront transmet l'en-tête à votre origine.	Oui, mais non recommandé
`Expect`	CloudFront supprime l'en-tête.	Oui
`From`	CloudFront transmet l'en-tête à votre origine.	Oui
`Host`	CloudFront définit la valeur du nom de domaine de l'origine associé à l'objet demandé. Vous ne pouvez pas mettre en cache en fonction de l'en-tête Host pour Amazon S3 ou MediaStore Origins.	Oui (personnalisée) Non (S3 et MediaStore)
`If-Match`	CloudFront transmet l'en-tête à votre origine.	Oui
`If-Modified-Since`	CloudFront transmet l'en-tête à votre origine.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`If-None-Match`	CloudFront transmet l'en-tête à votre origine.	Oui
`If-Range`	CloudFront transmet l'en-tête à votre origine.	Oui
`If-Unmodified-Since`	CloudFront transmet l'en-tête à votre origine.	Oui
`Max-Forwards`	CloudFront transmet l'en-tête à votre origine.	Non
`Origin`	CloudFront transmet l'en-tête à votre origine.	Oui
`Pragma`	CloudFront transmet l'en-tête à votre origine.	Non
`Proxy-Authenticate`	CloudFront supprime l'en-tête.	Non
`Proxy-Authorization`	CloudFront supprime l'en-tête.	Non
`Proxy-Connection`	CloudFront supprime l'en-tête.	Non
`Range`	CloudFront transmet l'en-tête à votre origine. Pour plus d'informations, consultez Comment CloudFront traite les demandes partielles pour un objet (plage GETS).	Oui, par défaut

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Referer`	CloudFront supprime l'en-tête.	Oui
`Request-Range`	CloudFront transmet l'en-tête à votre origine.	Non
`TE`	CloudFront supprime l'en-tête.	Non
`Trailer`	CloudFront supprime l'en-tête.	Non
`Transfer-Encoding`	CloudFront transmet l'en-tête à votre origine.	Non
`Upgrade`	CloudFront supprime l'en-tête, sauf si vous avez établi une WebSocket connexion.	Non (sauf pour les WebSocket connexions)
`User-Agent`	CloudFront remplace la valeur de ce champ d'en-tête par`Amazon CloudFront` . Si vous souhaitez CloudFront mettre en cache votre contenu en fonction de l'appareil utilisé par l'utilisateur, consultezConfiguration de la mise en cache en fonction du type d'appareil.	Oui, mais non recommandé
`Via`	CloudFront transmet l'en-tête à votre origine.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront le cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Warning`	CloudFront transmet l'en-tête à votre origine.	Oui
`X-Amz-Cf-Id`	CloudFront ajoute l'en-tête à la demande du lecteur avant de la transmettre à votre source. La valeur d'en-tête contient une chaîne chiffrée qui identifie de façon unique la demande.	Non
`X-Edge-*`	CloudFront supprime tous les `X-Edge-*` en-têtes.	Non
`X-Forwarded-For`	CloudFront transmet l'en-tête à votre origine. Pour plus d'informations, consultez Adresses IP client.	Oui
`X-Forwarded-Proto`	CloudFront supprime l'en-tête.	Non
`X-HTTP-Method-Override`	CloudFront supprime l'en-tête.	Oui
`X-Real-IP`	CloudFront supprime l'en-tête.	Non

Version de HTTP

CloudFront transmet les demandes à votre origine personnalisée à l'aide du protocole HTTP/1.1.

Longueur maximale d’une demande et longueur maximale d’une URL

La longueur maximale d’une demande, avec le chemin, la chaîne de requête (le cas échéant) et les en-têtes inclus, est de 20480 octets.

CloudFront construit une URL à partir de la requête. La longueur maximale de cette URL est de 8 192 caractères.

Si une demande ou une URL dépasse ces valeurs maximales, CloudFront renvoie le code d'état HTTP 413, Request Entity Too Large, au visualiseur, puis met fin à la connexion TCP avec le visualiseur.

OCSP Stapling

Lorsqu'un utilisateur soumet une demande HTTPS pour un objet, il CloudFront doit confirmer auprès de l'autorité de certification (CA) que le certificat SSL du domaine n'a pas été révoqué. L'agrafage OCSP accélère la validation du certificat en permettant de valider le certificat et de CloudFront mettre en cache la réponse de l'autorité de certification, de sorte que le client n'a pas besoin de valider le certificat directement auprès de l'autorité de certification.

L'amélioration des performances de l'agrafage OCSP est plus prononcée lors de la CloudFront réception de nombreuses requêtes HTTPS pour des objets du même domaine. Chaque serveur situé dans un emplacement CloudFront périphérique doit soumettre une demande de validation distincte. Lorsqu'il CloudFront reçoit un grand nombre de requêtes HTTPS pour le même domaine, chaque serveur situé à la périphérie reçoit rapidement une réponse de l'autorité de certification lui indiquant qu'il peut « agrafer » un paquet dans le cadre de la poignée de contact SSL ; lorsque le téléspectateur est convaincu que le certificat est valide, il CloudFront peut servir l'objet demandé. Si votre distribution ne reçoit pas beaucoup de trafic dans un emplacement CloudFront périphérique, les nouvelles demandes sont plus susceptibles d'être dirigées vers un serveur qui n'a pas encore validé le certificat auprès de l'autorité de certification. Dans ce cas, le visualiseur exécute séparément l'étape de validation et le CloudFront serveur sert l'objet. Ce CloudFront serveur soumet également une demande de validation à l'autorité de certification. Ainsi, la prochaine fois qu'il recevra une demande contenant le même nom de domaine, il recevra une réponse de validation de la part de l'autorité de certification.

Connexions persistantes

Lorsqu'il CloudFront reçoit une réponse de votre origine, il essaie de maintenir la connexion pendant plusieurs secondes au cas où une autre demande arriverait pendant cette période. Maintenir une

connexion persistante permet de gagner le temps requis pour ré-établir la connexion TCP et établir une autre liaison TLS pour les demandes ultérieures.

Pour plus d'informations, y compris sur la manière de configurer la durée des connexions persistantes, consultez Délai d'attente des connexions actives (origines personnalisées uniquement) dans la section Référence des paramètres de distribution.

Protocoles

CloudFront transmet les requêtes HTTP ou HTTPS au serveur d'origine en fonction des éléments suivants :

- Protocole de la demande à laquelle le spectateur envoie CloudFront, HTTP ou HTTPS.
- La valeur du champ Origin Protocol Policy dans la CloudFront console ou, si vous utilisez l' CloudFront API, l'`OriginProtocolPolicy`élément du type `DistributionConfig` complexe. Dans la CloudFront console, les options sont HTTP uniquement, HTTPS uniquement et Match Viewer.

Si vous spécifiez HTTP uniquement ou HTTPS uniquement, CloudFront transfère les demandes au serveur d'origine en utilisant le protocole spécifié, quel que soit le protocole indiqué dans la demande du lecteur.

Si vous spécifiez Match Viewer, CloudFront transmet les demandes au serveur d'origine en utilisant le protocole indiqué dans la demande du visualiseur. Notez que l'objet n'est mis en CloudFront cache qu'une seule fois, même si les utilisateurs font des demandes à l'aide des protocoles HTTP et HTTPS.

> **Important**
>
> Si une CloudFront demande est transmise à l'origine à l'aide du protocole HTTPS, et si le serveur d'origine renvoie un certificat non valide ou un certificat auto-signé, CloudFront la connexion TCP est interrompue.

Pour plus d'informations sur la mise à jour d'une distribution à l'aide de la CloudFront console, consultezMettre à jour une distribution. Pour plus d'informations sur la mise à jour d'une distribution à l'aide de l' CloudFront API, UpdateDistributionconsultez le Amazon CloudFront API Reference.

Chaînes de requête

Vous pouvez configurer si les paramètres CloudFront de la chaîne de requête sont transmis à votre origine. Pour plus d'informations, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

Délai d'attente et tentatives de connexion à l'origine

Le délai d'expiration de la connexion d'origine est le nombre de secondes d' CloudFront attente lorsque vous essayez d'établir une connexion avec l'origine.

Les tentatives de connexion à l'origine correspondent au nombre de CloudFront tentatives de connexion à l'origine.

Ensemble, ces paramètres déterminent la durée des CloudFront tentatives de connexion à l'origine avant de basculer vers l'origine secondaire (dans le cas d'un groupe d'origine) ou de renvoyer une réponse d'erreur au lecteur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

Pour de plus amples informations, veuillez consulter Contrôlez les délais et les tentatives d'origine.

Délai de réponse de l'origine

Le délai de réponse de l'origine, également appelé délai d'attente des opérations de lecture depuis l'origine ou délai de demande à l'origine, s'applique aux deux valeurs suivantes :

- Durée, en secondes, d' CloudFront attente d'une réponse après le transfert d'une demande à l'origine.
- Temps d' CloudFront attente, en secondes, après réception d'un paquet de réponse provenant de l'origine et avant de recevoir le paquet suivant.

CloudFront le comportement dépend de la méthode HTTP de la requête du spectateur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas ou cesse de répondre dans le délai imparti, interrompt CloudFront la connexion. Si le nombre spécifié de tentatives de connexion d'origine est supérieur à 1, CloudFront réessaie pour obtenir une réponse complète. CloudFront essaie jusqu'à 3 fois, selon la valeur du paramètre des tentatives de connexion d'origine. Si l'origine ne répond

pas lors de la dernière tentative, elle CloudFront ne réessaie pas tant qu'elle n'a pas reçu une autre demande de contenu sur la même origine.

- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` demandes : si l'origine ne répond pas dans les 30 secondes, CloudFront interrompt la connexion et n'essaie pas de la contacter à nouveau. Le client peut soumettre à nouveau la demande si nécessaire.

Pour de plus amples informations, y compris sur la manière de configurer le délai de réponse de l'origine, veuillez consulter Délai de réponse (origines personnalisées uniquement).

Demandes simultanées pour le même objet (réduction des demandes)

Lorsqu'un emplacement CloudFront périphérique reçoit une demande pour un objet et que celui-ci n'est pas dans le cache ou que l'objet mis en cache a expiré, envoie CloudFront immédiatement la demande à l'origine. Toutefois, s'il existe des demandes simultanées pour le même objet, c'est-à-dire si des demandes supplémentaires pour le même objet (avec la même clé de cache) arrivent à l'emplacement périphérique avant de CloudFront recevoir la réponse à la première demande, faites CloudFront une pause avant de transmettre les demandes supplémentaires à l'origine. Cette brève pause permet de réduire la charge sur l'origine. CloudFront envoie la réponse de la demande initiale à toutes les demandes qu'elle a reçues pendant sa pause. Ce processus se nomme la réduction des demandes. Dans CloudFront les journaux, la première demande est identifiée comme étant `Miss` dans le `x-edge-result-type` champ, et les demandes réduites sont identifiées comme un`Hit`. Pour plus d'informations sur CloudFront les journaux, consultezthe section called “CloudFront et journalisation des fonctions Edge”.

CloudFront réduit uniquement les demandes qui partagent une clé de cache. Si les demandes supplémentaires ne partagent pas la même clé de cache parce que, par exemple, vous avez configuré CloudFront le cache en fonction des en-têtes de demande, des cookies ou des chaînes de requête, CloudFront transfère toutes les demandes avec une clé de cache unique à votre origine.

Si vous souhaitez empêcher le regroupement de toutes les demandes, vous pouvez utiliser la politique de cache géré`CachingDisabled`, qui empêche également la mise en cache. Pour plus d'informations, consultez Utiliser des politiques de cache gérées.

Si vous souhaitez empêcher la réduction des demandes pour des objets spécifiques, vous pouvez définir le TTL minimum pour le comportement du cache sur 0 et configurer l'origine à envoyer`Cache-Control: private`,, `Cache-Control: no-store` `Cache-Control: no-cache`Cache-Control: `max-age=0`, ou. `Cache-Control: s-maxage=0` Ces configurations augmenteront la

charge sur votre origine et introduiront une latence supplémentaire pour les demandes simultanées qui sont suspendues pendant l' CloudFront attente de la réponse à la première demande.

> **Important**
>
> Actuellement, la réduction des demandes CloudFront n'est pas prise en charge si vous activez le transfert de cookies dans la politique de cache, la politique de demande d'origine ou les anciens paramètres de cache.

En-tête **`User-Agent`**

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de l'appareil utilisé par l'utilisateur pour consulter votre contenu, nous vous recommandons de configurer CloudFront pour transférer un ou plusieurs des en-têtes suivants vers votre origine personnalisée :

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

Sur la base de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes `false` avant `true` ou avant le transfert de la demande à votre origine. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront vous pouvez définir les deux options `CloudFront-Is-Mobile-Viewer` et la valeur `CloudFront-Is-Tablet-Viewer` sur`true`. Pour plus d'informations sur la configuration CloudFront de la mise en cache en fonction des en-têtes de demande, consultezContenu du cache basé sur les en-têtes des demandes.

Vous pouvez configurer CloudFront pour mettre en cache des objets en fonction des valeurs de l'`User-Agent`en-tête, mais nous ne le recommandons pas. L'`User-Agent`en-tête comporte de nombreuses valeurs possibles, et la mise en cache basée sur ces valeurs entraînerait le transfert CloudFront d'un plus grand nombre de demandes vers votre origine.

Si vous ne configurez pas CloudFront pour mettre en cache les objets en fonction des valeurs de l'`User-Agent` CloudFront `User-Agent`en-tête, ajoutez un en-tête avec la valeur suivante avant de transmettre une demande à votre origine :

`User-Agent = Amazon CloudFront`

CloudFront ajoute cet en-tête, que la demande du visualiseur contienne ou non un `User-Agent` en-tête. Si la demande du visualiseur inclut un `User-Agent` en-tête, CloudFront supprimez-le.

Comment CloudFront traite les réponses provenant de votre origine personnalisée

Découvrez comment CloudFront traite les réponses provenant de votre origine personnalisée.

Table des matières

Réponses **`100 Continue`**

Votre origine ne peut pas envoyer plus d'une réponse de type 100-Continue à CloudFront. Après la première réponse 100-Continue, CloudFront attend une réponse HTTP 200 OK. Si votre origine envoie une autre réponse 100-Continue après la première, elle CloudFront renverra une erreur.

Mise en cache

- Assurez-vous que le serveur d'origine définit des valeurs valides et précises pour les champs d'en-tête `Date` et `Last-Modified`.
- CloudFront respecte normalement un `Cache-Control: no-cache` en-tête dans la réponse depuis l'origine. Pour une exception, consultez Demandes simultanées pour le même objet (réduction des demandes).

Requêtes annulées

Si un objet ne se trouve pas dans le cache périphérique et si un utilisateur met fin à une session (par exemple, ferme un navigateur) après avoir récupéré l'objet depuis votre origine mais avant de pouvoir livrer l'objet demandé, il CloudFront ne CloudFront met pas l'objet en cache dans l'emplacement périphérique.

Négociation de contenu

Si votre origine est renvoyée `Vary:*` dans la réponse, et si la valeur du TTL minimum pour le comportement de cache correspondant est 0, CloudFront met l'objet en cache tout en transmettant toutes les demandes suivantes à l'origine pour confirmer que le cache contient la dernière version de l'objet. CloudFront n'inclut aucun en-tête conditionnel, tel que `If-None-Match` ou`If-Modified-Since`. Par conséquent, votre origine renvoie l'objet à CloudFront en réponse à chaque demande.

Si votre origine renvoie `Vary:*` la réponse, et si la valeur de Minimum TTL pour le comportement de cache correspondant est une autre valeur, CloudFront traite l'`Vary`en-tête comme décrit dansEn-têtes de réponse HTTP qui CloudFront suppriment ou remplacent.

Cookies

Si vous activez les cookies pour un comportement de cache, et si l'origine renvoie des cookies avec un objet, met en CloudFront cache à la fois l'objet et les cookies. Notez que cela réduit la capacité de mise en cache pour un objet. Pour de plus amples informations, veuillez consulter Contenu du cache basé sur les cookies.

Connexions TCP annulées

Si la connexion TCP entre votre origine CloudFront et votre origine est interrompue alors que votre origine renvoie un objet CloudFront, le CloudFront comportement dépend du fait que votre origine a inclus ou non un `Content-Length` en-tête dans la réponse :

- En-tête Content-Length : CloudFront renvoie l'objet au visualiseur au fur et à mesure qu'il l'obtient depuis votre origine. Toutefois, si la valeur de l'`Content-Length`en-tête ne correspond pas à la taille de l'objet, l'objet CloudFront n'est pas mis en cache.
- Encodage de transfert : découpé : CloudFront renvoie l'objet au visualiseur au fur et à mesure qu'il l'obtient depuis votre origine. Toutefois, si la réponse segmentée n'est pas complète, l'objet CloudFront n'est pas mis en cache.

- Aucun en-tête Content-Length : CloudFront renvoie l'objet au visualiseur et le met en cache, mais l'objet n'est peut-être pas complet. Sans `Content-Length` en-tête, CloudFront impossible de déterminer si la connexion TCP a été interrompue accidentellement ou intentionnellement.

Nous vous recommandons de configurer votre serveur HTTP pour ajouter un `Content-Length` en-tête afin d' CloudFront empêcher la mise en cache d'objets partiels.

En-têtes de réponse HTTP qui CloudFront suppriment ou remplacent

CloudFront supprime ou met à jour les champs d'en-tête suivants avant de transmettre la réponse de votre origine au lecteur :

- `Set-Cookie`— Si vous configurez CloudFront pour transférer les cookies, le champ `Set-Cookie` d'en-tête sera transmis aux clients. Pour plus d'informations, consultez Contenu du cache basé sur les cookies.
- `Trailer`
- `Transfer-Encoding`— Si votre origine renvoie ce champ d'en-tête CloudFront , définissez la valeur sur `chunked` avant de renvoyer la réponse au spectateur.
- `Upgrade`
- `Vary` – Notez ce qui suit :
  - Si vous configurez CloudFront pour transférer l'un des en-têtes spécifiques à l'appareil vers votre origine (`CloudFront-Is-Desktop-Viewer`,, `CloudFront-Is-Mobile-ViewerCloudFront-Is-SmartTV-Viewer`,`CloudFront-Is-Tablet-Viewer`) et que vous configurez votre origine pour qu'elle revienne `Vary:User-Agent` à CloudFront, CloudFront revient `Vary:User-Agent` au visualiseur. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.
  - Si vous configurez votre origine pour inclure l'un `Accept-Encoding` ou l'autre `Cookie` dans l'`Vary`en-tête, CloudFront inclut les valeurs dans la réponse au visualiseur.
  - Si vous configurez CloudFront pour transférer les en-têtes vers votre origine, et si vous configurez votre origine pour renvoyer les noms des en-têtes CloudFront dans l'`Vary`en-tête (par exemple,`Vary:Accept-Charset,Accept-Language`), CloudFront renvoie l'`Vary`en-tête avec ces valeurs au visualiseur.
  - Pour plus d'informations sur CloudFront le traitement d'une valeur de `*` dans l'`Vary`en-tête, consultezNégociation de contenu.

- Si vous configurez votre origine pour inclure d'autres valeurs dans l'`Vary`en-tête, CloudFront supprimez les valeurs avant de renvoyer la réponse au visualiseur.

- `Via`— CloudFront définit la valeur suivante dans la réponse au visualiseur :

  `Via: `*`version_http chaîne_alphanumérique`*`.cloudfront.net (CloudFront)`

  Par exemple, la valeur est similaire à la suivante :

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Taille de fichier maximale pouvant être mise en cache

La taille maximale d'un corps de réponse enregistré CloudFront dans son cache est de 50 Go. Cette taille inclut les réponses de transfert fragmentées qui ne spécifient pas la valeur d'en-tête `Content-Length`.

Vous pouvez utiliser CloudFront pour mettre en cache un objet dont la taille est supérieure à cette taille en utilisant des demandes de plage pour demander les objets dans des parties dont la taille est inférieure ou égale à 50 Go. CloudFrontmet en cache ces parties car chacune d'elles a une taille inférieure ou égale à 50 Go. Une fois que l'utilisateur a récupéré toutes les parties de l'objet, il peut reconstruire l'objet d'origine plus large. Pour plus d'informations, consultez Utiliser les demandes de plage pour mettre en cache de large objets.

Origine non disponible

Si votre serveur d'origine n'est pas disponible et CloudFront reçoit une demande pour un objet qui se trouve dans le cache périphérique mais qui a expiré (par exemple, parce que le délai spécifié dans la `Cache-Control max-age` directive est dépassé), CloudFront il diffuse la version expirée de l'objet ou affiche une page d'erreur personnalisée. Pour plus d'informations sur CloudFront le comportement lorsque vous avez configuré des pages d'erreur personnalisées, consultezComment CloudFront traite les erreurs lorsque vous avez configuré des pages d'erreur personnalisées.

Dans certains cas, un objet rarement demandé est expulsé et n'est plus disponible dans le cache périphérique. CloudFront ne peut pas servir un objet qui a été expulsé.

Redirections

Si vous changez l'emplacement d'un objet sur le serveur d'origine, vous pouvez configurer votre serveur Web afin de rediriger les demandes vers le nouvel emplacement. Après avoir configuré

la redirection, la première fois qu'un utilisateur soumet une demande pour l'objet, CloudFront Front envoie la demande à l'origine, qui répond par une redirection (par exemple,`302 Moved Temporarily`). CloudFront met en cache la redirection et la renvoie au visualiseur. CloudFront ne suit pas la redirection.

Vous pouvez configurer votre serveur Web afin de rediriger les demandes vers l'un des emplacements suivants :

- La nouvelle URL de l'objet sur le serveur d'origine. Lorsque le lecteur suit la redirection vers la nouvelle URL, il contourne l'URL d'origine CloudFront et se dirige directement vers l'URL d'origine. Par conséquent, nous vous recommandons de ne pas rediriger des demandes vers la nouvelle URL de l'objet sur l'origine.
- La nouvelle CloudFront URL de l'objet. Lorsque le lecteur soumet la demande contenant la nouvelle CloudFront URL, CloudFront récupère l'objet depuis le nouvel emplacement de votre origine, le met en cache à l'emplacement périphérique et renvoie l'objet au visualiseur. Les demandes suivantes pour l'objet seront servies par l'emplacement périphérique. Ceci évite la latence et la charge associées aux utilisateurs qui demandent l'objet à l'origine. Cependant, chaque nouvelle demande pour l'objet entraînera des frais pour deux demandes adressées àCloudFront.

En-tête **`Transfer-Encoding`**

CloudFront ne prend en charge que la `chunked` valeur de l'`Transfer-Encoding`en-tête. Si votre origine revient`Transfer-Encoding: chunked`, CloudFront renvoie l'objet au client dès qu'il est reçu à l'emplacement périphérique et met en cache l'objet au format fragmenté pour les demandes suivantes.

Si le visualiseur fait une `Range GET` demande et que l'origine revient`Transfer-Encoding: chunked`, CloudFront renvoie l'objet entier au visualiseur au lieu de la plage demandée.

Nous vous recommandons d'utiliser un encodage fragmenté si la longueur du contenu de votre réponse ne peut pas être prédéterminé. Pour de plus amples informations, veuillez consulter Connexions TCP annulées.

Comportement des requêtes et des réponses pour les groupes d'origine

Les demandes adressées à un groupe d'origine fonctionnent de la même manière que celles d'une origine qui n'est pas configurée comme un groupe d'origine, sauf en cas de basculement d'origine.

Comme pour toute autre origine, lorsqu'il CloudFront reçoit une demande et que le contenu est déjà mis en cache dans un emplacement périphérique, le contenu est diffusé aux spectateurs à partir du cache. En l'absence de cache et lorsque l'origine est un groupe d'origine, les demandes de l'utilisateur sont transférées à l'origine principale dans le groupe d'origine.

Le comportement de demande et de réponse pour l'origine principale est le même que pour une origine qui n'est pas incluse dans un groupe d'origine. Pour plus d'informations, consultez Comportement des demandes et des réponses pour les origines Amazon S3 Origins et Comportement des demandes et des réponses pour les origines personnalisées.

La section suivante décrit le comportement du basculement d'origine lorsque l'origine principale renvoie des codes de statut HTTP spécifiques :

- Code d'état HTTP 2xx (succès) : CloudFront met le fichier en cache et le renvoie au visualiseur.
- Code d'état HTTP 3xx (redirection) : CloudFront renvoie le code d'état au visualiseur.
- Code d'état HTTP 4xx ou 5xx (erreur client/serveur) : si le code d'état renvoyé a été configuré pour le basculement, CloudFront envoie la même demande à l'origine secondaire dans le groupe d'origine.
- Code d'état HTTP 4xx ou 5xx (erreur client/serveur) : si le code d'état renvoyé n'a pas été configuré pour le basculement, CloudFront renvoie l'erreur au visualiseur.

CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du spectateur est `GET`, `HEAD`, ou `OPTIONS`. CloudFront ne bascule pas lorsque le visualiseur envoie une autre méthode HTTP (par exemple `POST`, `PUT`, etc.).

Lorsque CloudFront vous envoyez une demande à une origine secondaire, le comportement de réponse est le même que pour une CloudFront origine ne faisant pas partie d'un groupe d'origine.

Pour de plus amples informations sur les groupes d'origine, veuillez consulter Optimisez la haute disponibilité grâce au basculement CloudFront d'origine.

Ajouter des en-têtes personnalisés aux demandes d'origine

Vous pouvez configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes qu'il envoie à votre origine. Vous pouvez utiliser des en-têtes personnalisés pour envoyer et collecter des informations provenant de votre origine que vous n'obtenez pas avec les demandes classiques des spectateurs. Vous pouvez même personnaliser les en-têtes pour chaque origine. CloudFrontprend en charge les en-têtes personnalisés pour les origines personnalisées et les origines Amazon S3.

Table des matières

Cas d’utilisation

Vous pouvez utiliser des en-têtes personnalisés, comme dans les exemples suivants :

Identifier les demandes provenant de CloudFront

Vous pouvez identifier les demandes provenant de votre origine CloudFront. Cela peut être utile si vous souhaitez savoir si les utilisateurs CloudFront contournent ou si vous utilisez plusieurs CDN et souhaitez obtenir des informations sur les demandes provenant de chaque CDN.

> **Note**
>
> Si vous utilisez une origine Amazon S3 avec journalisation des accès au serveur Amazon S3 activée, les journaux n'incluent pas les informations d'en-tête.

Détermination des demandes provenant d'une distribution particulière

Si vous configurez plusieurs CloudFront distributions pour utiliser la même origine, vous pouvez ajouter des en-têtes personnalisés différents dans chaque distribution. Vous pouvez ensuite utiliser les journaux de votre origine pour déterminer quelles demandes proviennent de quelle CloudFront distribution.

Activation du partage des ressources de plusieurs origines (CORS)

Si certains de vos utilisateurs ne prennent pas en charge le partage de ressources entre origines (CORS), vous pouvez configurer CloudFront pour toujours ajouter l'`Origin`en-tête aux demandes qu'il envoie à votre source. Ensuite, vous pouvez configurer votre origine pour renvoyer l'en-tête `Access-Control-Allow-Origin` pour chaque demande. Vous devez également configurer CloudFront pour respecter les paramètres CORS.

Contrôle de l'accès au contenu

Vous pouvez utiliser les en-têtes personnalisés pour contrôler l'accès au contenu. En configurant votre origine pour répondre aux demandes uniquement lorsqu'elles incluent un en-tête personnalisé ajouté par CloudFront, vous empêchez les utilisateurs de contourner CloudFront et d'accéder à votre contenu directement sur l'origine. Pour plus d'informations, consultez Restreindre l'accès aux fichiers dont l'origine est personnalisée.

Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine

Pour configurer une distribution afin d'ajouter des en-têtes personnalisés aux demandes qu'elle envoie à votre origine, mettez à jour la configuration de l'origine via l'une des méthodes suivantes :

- CloudFront console — Lorsque vous créez ou mettez à jour une distribution, spécifiez les noms et les valeurs des en-têtes dans les paramètres Ajouter des en-têtes personnalisés. Pour plus d'informations, consultez Ajout d'en-tête personnalisé.
- CloudFront API — Pour chaque origine à laquelle vous souhaitez ajouter des en-têtes personnalisés, spécifiez les noms et les valeurs des en-têtes dans le `CustomHeaders` champ intérieur`Origin`. Pour plus d'informations, consultez CreateDistributionou consultez UpdateDistributionle Amazon CloudFront API Reference.

Si les noms et valeurs d'en-tête que vous spécifiez ne sont pas déjà présents dans la demande du visualiseur, CloudFront ajoutez-les à la demande d'origine. Si un en-tête est présent, CloudFront remplace la valeur de l'en-tête avant de transmettre la demande à l'origine.

Pour les quotas qui s'appliquent aux en-têtes personnalisés d'origine, consultezQuotas sur les en-têtes.

En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine

Vous ne pouvez pas configurer CloudFront pour ajouter l'un des en-têtes suivants aux demandes qu'il envoie à votre origine :

- `Cache-Control`
- `Connection`

- `Content-Length`
- `Cookie`
- `Host`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Max-Forwards`
- `Pragma`
- `Proxy-Authorization`
- `Proxy-Connection`
- `Range`
- `Request-Range`
- `TE`
- `Trailer`
- `Transfer-Encoding`
- `Upgrade`
- `Via`
- En-têtes commençant par `X-Amz-`
- En-têtes commençant par `X-Edge-`
- `X-Real-Ip`

Configurer CloudFront pour transférer l'**`Authorization`**en-tête

Lorsque CloudFront vous transférez une demande d'utilisateur à votre source, certains CloudFront en-têtes de visionnage sont supprimés par défaut, y compris l'`Authorization`en-tête. Pour vous assurer que votre origine reçoit toujours l'en-tête `Authorization` dans les demandes d'origine, vous disposez des options suivantes :

- Ajoutez l'en-tête `Authorization` à la clé de cache à l'aide d'une stratégie de cache. Tous les en-têtes de la clé de cache sont automatiquement inclus dans les demandes d'origine. Pour plus d'informations, consultez Contrôlez la clé de cache à l'aide d'une politique.
- Utilisez une stratégie de demande d'origine qui transfère tous les en-têtes d'utilisateurs à l'origine. Vous ne pouvez pas transférer l'`Authorization`en-tête individuellement dans une politique de demande d'origine, mais lorsque vous transférez tous les en-têtes du lecteur, l'`Authorization`en-tête est CloudFront inclus dans les demandes du lecteur. CloudFront fournit une politique de demande d'origine gérée pour ce cas d'utilisation, appelée Managed- AllViewer. Pour plus d'informations, voir Utiliser des politiques de demande d'origine gérées.

Comment CloudFront traite les demandes partielles pour un objet (plage GETS)

Pour un objet large, l'utilisateur (navigateur web ou autre client) peut effectuer plusieurs demandes `GET` et utiliser l'en-tête de demande `Range` pour télécharger l'objet en parties plus petites. Ces demandes de plages d'octets, parfois appelées demandes `Range GET`, améliore l'efficacité des téléchargements partiels et la récupération de transferts ayant partiellement échoué.

Lorsqu'il CloudFront reçoit une `Range GET` demande, il vérifie le cache à l'emplacement périphérique qui a reçu la demande. Si le cache situé à cet emplacement périphérique contient déjà l'objet entier ou la partie demandée de l'objet, CloudFront diffuse immédiatement la plage demandée depuis le cache.

Si le cache ne contient pas la plage demandée, CloudFront transmet la demande à l'origine. (Pour optimiser les performances, vous CloudFront pouvez demander une plage plus large que celle demandée par le client dans le`Range GET`.) Ce qui se produit dépend de si l'origine prend en charge les demandes `Range GET` :

- Si l'origine prend en charge les **`Range GET`** demandes, elle renvoie la plage demandée. CloudFront sert la plage demandée et la met également en cache pour les demandes futures. (Amazon S3 prend en charge les demandes `Range GET`, tout comme de nombreux serveurs HTTP.)
- Si l'origine ne prend pas en charge les **`Range GET`** demandes, elle renvoie l'objet entier. CloudFront répond à la demande en cours en envoyant l'objet entier tout en le mettant en cache pour les demandes futures. Après avoir mis en CloudFront cache l'objet entier dans un cache périphérique, il répond aux nouvelles `Range GET` demandes en fournissant la plage demandée.

Dans les deux cas, CloudFront commence à servir la plage ou l'objet demandé à l'utilisateur final dès que le premier octet arrive depuis l'origine.

> **Note**
>
> Si le visualiseur fait une `Range GET` demande et que l'origine revient`Transfer-Encoding: chunked`, CloudFront renvoie l'objet entier au visualiseur au lieu de la plage demandée.

CloudFront suit généralement la spécification RFC pour l'`Range`en-tête. Toutefois, si vos `Range` en-têtes ne répondent pas aux exigences suivantes, CloudFront renvoie le code de statut HTTP `200` avec l'objet complet au lieu d'un code d'état `206` avec les plages spécifiées :

- Les plages doivent être répertoriées en ordre croissant. Par exemple, `100-200,300-400` est valide, mais pas `300-400,100-200`.
- Les plages ne doivent pas se chevaucher. Par exemple, `100-200,150-250` n'est pas valide.
- Toutes les spécifications de plages doivent être valides. Par exemple, vous ne pouvez pas spécifier une valeur négative dans une plage.

Pour plus d'informations sur l'en-tête de demande `Range`, consultez la section Demandes de plage dans RFC 7233, ou Plage dans MDN Web Docs.

Utiliser les demandes de plage pour mettre en cache de large objets

Lorsque la mise en cache est activée, CloudFront elle ne récupère ni ne met en cache un objet de plus de 50 Go. Lorsqu'une origine indique que l'objet est plus grand que cette taille (dans l'en-tête de `Content-Length` réponse), CloudFront ferme la connexion à l'origine et renvoie une erreur au visualiseur. (Lorsque la mise en cache est désactivée, CloudFront vous pouvez récupérer un objet dont la taille est supérieure à cette taille depuis l'origine et le transmettre au visualiseur. Cependant, CloudFront ne met pas l'objet en cache.)

Cependant, avec les demandes de plage, vous pouvez les utiliser CloudFront pour mettre en cache un objet dont la taille de fichier est supérieure à la taille de fichier maximale pouvant être mise en cache.

Example Exemple

1. Imaginons une origine avec un objet de 100 Go. Lorsque la mise en cache est activée, CloudFront aucun objet de cette taille ne peut être récupéré ou mis en cache. Toutefois, l'utilisateur peut envoyer plusieurs demandes de plage pour récupérer cet objet par parties, chacune d'entre elles étant inférieure à 50 Go.
2. Le spectateur peut demander l'objet par parties de 20 Go en envoyant une demande avec l'en-tête `Range: bytes=0-21474836480` pour récupérer la première partie, une autre demande avec l'en-tête `Range: bytes=21474836481-42949672960` pour récupérer la partie suivante, etc.
3. Lorsque l'utilisateur a reçu toutes les parties, il peut les combiner pour construire l'objet d'origine de 100 Go.
4. Dans ce cas, met en CloudFront cache chacune des parties de 20 Go de l'objet et peut répondre aux demandes ultérieures pour la même partie à partir du cache.

Comment CloudFront traite les codes d'état HTTP 3xx de votre origine

Lorsque CloudFront vous demandez un objet depuis votre compartiment Amazon S3 ou votre serveur d'origine personnalisé, votre origine renvoie parfois un code d'état HTTP 3xx. Ce message indique généralement l'une des situations suivantes :

- L'URL de l'objet a changé (par exemple, les codes d'état 301, 302, 307 ou 308)
- L'objet n'a pas changé depuis la dernière CloudFront demande (code d'état 304)

CloudFront met en cache 3xx réponses en fonction des paramètres de votre CloudFront distribution et des en-têtes de la réponse. CloudFront met en cache 307 et 308 réponses uniquement lorsque vous incluez l'`Cache-Control`en-tête dans les réponses depuis l'origine. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Si votre origine renvoie un code d'état de redirection (par exemple, 301 ou 307), CloudFront il ne suit pas la redirection. CloudFront transmet la réponse 301 ou 307 au spectateur, qui peut suivre la redirection en envoyant une nouvelle demande.

Comment CloudFront traite les codes d'état HTTP 4xx et 5xx de votre origine

Lorsque CloudFront vous demandez un objet depuis votre compartiment Amazon S3 ou votre serveur d'origine personnalisé, votre origine renvoie parfois un code d'état HTTP 4xx ou 5xx, qui indique qu'une erreur s'est produite. CloudFront le comportement dépend de :

- Si vous avez configuré des pages d'erreur personnalisées
- Si vous avez configuré la durée pendant laquelle vous souhaitez mettre CloudFront en cache les réponses aux erreurs depuis votre origine (TTL minimum de mise en cache des erreurs)
- Le code de statut
- Pour les codes d'état 5xx, si l'objet demandé se trouve actuellement dans le cache CloudFront périphérique
- Pour certains codes de statut 4xx, si l'origine renvoie un `Cache-Control max-age` ou un en-tête `Cache-Control s-maxage`

CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront ne met pas en cache les réponses aux demandes qui utilisent les autres méthodes.

Si l'origine ne répond pas, la CloudFront demande envoyée à l'origine expire, ce qui est considéré comme une erreur HTTP 5xx de la part de l'origine, même si l'origine n'a pas répondu avec cette erreur. Dans ce scénario, CloudFront continue de diffuser le contenu mis en cache. Pour plus d'informations, consultez Origine non disponible.

Si vous avez activé la journalisation, CloudFront écrit les résultats dans les journaux quel que soit le code d'état HTTP.

Pour plus d'informations sur les fonctionnalités et les options liées au message d'erreur renvoyé par CloudFront, consultez les rubriques suivantes :

- Pour plus d'informations sur les paramètres des pages d'erreur personnalisées dans la CloudFront console, consultezPages d'erreur personnalisées et mise en cache des erreurs.
- Pour plus d'informations sur l'erreur de mise en cache du TTL minimum dans la CloudFront console, consultez. Erreur de mise en cache de TTL minimum (secondes)

- Pour obtenir la liste des codes d'état HTTP mis en CloudFront cache, consultezCodes d'état HTTP 4xx et 5xx mis en cache CloudFront .

Rubriques

Comment CloudFront traite les erreurs lorsque vous avez configuré des pages d'erreur personnalisées

Si vous avez configuré des pages d'erreur personnalisées, CloudFront le comportement dépend de la présence ou non de l'objet demandé dans le cache périphérique.

L’objet demandé n’est pas dans le cache périphérique

CloudFront continue d'essayer d'obtenir l'objet demandé depuis votre origine lorsque toutes les conditions suivantes sont remplies :

- Un utilisateur demande un objet.
- L’objet n’est pas dans le cache périphérique.
- L’origine renvoie un code de statut HTTP 4xx ou 5xx et l’une des conditions suivantes est vraie :
  - L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.
  - L’origine renvoie un code de statut HTTP 4xx qui n’est pas limité par un en-tête de contrôle de cache et est inclus dans la liste suivante de codes de statut: Codes d'état HTTP 4xx et 5xx toujours mis en cache CloudFront .
  - L’origine renvoie un code de statut HTTP 4xx sans en-tête `Cache-Control max-age` ou sans en-tête `Cache-Control s-maxage`, et le code de statut est inclus dans la liste suivante de codes de statut : Control Codes d'état HTTP 4xx mis en CloudFront cache en fonction des en-têtes `Cache-Control`.

CloudFront effectue les opérations suivantes :

1. Dans le cache CloudFront périphérique qui a reçu la demande du lecteur, CloudFront vérifie la configuration de votre distribution et obtient le chemin de la page d'erreur personnalisée correspondant au code d'état renvoyé par votre origine.
2. CloudFront trouve le premier comportement de cache de votre distribution dont le modèle de chemin correspond au chemin de la page d'erreur personnalisée.
3. L'emplacement CloudFront périphérique envoie une demande de page d'erreur personnalisée à l'origine spécifiée dans le comportement du cache.
4. L’origine renvoie la page d’erreur personnalisée à l’emplacement périphérique.
5. CloudFront renvoie la page d'erreur personnalisée à l'afficheur qui a fait la demande, et met également en cache la page d'erreur personnalisée pour le maximum des valeurs suivantes :
   - La durée spécifiée par la durée de vie minimale (TTL) de la mise en cache des erreurs (10 secondes par défaut)
   - La durée spécifiée par un en-tête `Cache-Control max-age` ou un en-tête `Cache-Control s-maxage` qui est renvoyé par l’origine lorsque la première demande a généré l’erreur
6. Une fois le temps de mise en cache (déterminé à l'étape 5) écoulé, CloudFront essaie à nouveau d'obtenir l'objet demandé en transférant une autre demande à votre origine. CloudFront continue de réessayer aux intervalles spécifiés par le TTL minimum de mise en cache des erreurs.

L’objet demandé est dans le cache périphérique

CloudFront continue à servir l'objet qui se trouve actuellement dans le cache périphérique lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L’objet se trouve dans le cache périphérique, mais il a expiré
- L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.

CloudFront effectue les opérations suivantes :

1. Si votre origine renvoie un code de statut 5xx, il CloudFront sert l'objet même s'il a expiré. Pendant la durée de l'erreur de mise en cache, le TTL minimum CloudFront continue de répondre aux demandes des utilisateurs en servant l'objet depuis le cache périphérique.

Si votre origine renvoie un code d'état 4xx, CloudFront renvoie le code d'état, et non l'objet demandé, au spectateur.

2. Une fois que le TTL minimum de mise en cache d'erreur est expiré, CloudFront essaie à nouveau d'obtenir l'objet demandé en transférant une autre demande à votre origine. Notez que si l'objet n'est pas fréquemment demandé, cela CloudFront peut l'expulser du cache périphérique alors que votre serveur d'origine renvoie encore 5xx réponses. Pour plus d'informations sur la durée pendant laquelle les objets restent dans les caches CloudFront périphériques, consultezGérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Comment CloudFront traite les erreurs lorsque vous n'avez pas configuré de pages d'erreur personnalisées

Si vous n'avez pas configuré de pages d'erreur personnalisées, CloudFront le comportement dépend de la présence ou non de l'objet demandé dans le cache périphérique.

L’objet demandé n’est pas dans le cache périphérique

CloudFront continue d'essayer d'obtenir l'objet demandé depuis votre origine lorsque toutes les conditions suivantes sont remplies :

- Un utilisateur demande un objet.
- L’objet n’est pas dans le cache périphérique.
- L’origine renvoie un code de statut HTTP 4xx ou 5xx et l’une des conditions suivantes est vraie :
  - L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.
  - L’origine renvoie un code de statut HTTP 4xx qui n’est pas limité par un en-tête de contrôle de cache et est inclus dans la liste suivante de codes de statut: Codes d'état HTTP 4xx et 5xx toujours mis en cache CloudFront
  - L’origine renvoie un code de statut HTTP 4xx sans en-tête `Cache-Control max-age` ou sans en-tête `Cache-Control s-maxage`, et le code de statut est inclus dans la liste suivante de codes de statut : Control Codes d'état HTTP 4xx mis en CloudFront cache en fonction des en-têtes `Cache-Control`.

CloudFront effectue les opérations suivantes :

1. CloudFront renvoie le code d'état 4xx ou 5xx au visualiseur, et met également en cache le code d'état dans le cache périphérique qui a reçu la demande pour le maximum des éléments suivants :
   - La durée spécifiée par la durée de vie minimale (TTL) de la mise en cache des erreurs (10 secondes par défaut)
   - La durée spécifiée par un en-tête `Cache-Control max-age` ou un en-tête `Cache-Control s-maxage` qui est renvoyé par l'origine lorsque la première demande a généré l'erreur
2. Pendant la durée de la mise en cache (déterminée à l'étape 1), CloudFront répond aux demandes ultérieures du spectateur pour le même objet avec le code d'état 4xx ou 5xx mis en cache.
3. Une fois le temps de mise en cache (déterminé à l'étape 1) écoulé, CloudFront essaie à nouveau d'obtenir l'objet demandé en transférant une autre demande à votre origine. CloudFront continue de réessayer aux intervalles spécifiés par le TTL minimum de mise en cache des erreurs.

L'objet demandé est dans le cache périphérique

CloudFront continue à servir l'objet qui se trouve actuellement dans le cache périphérique lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L'objet se trouve dans le cache périphérique, mais il a expiré
- L'origine renvoie un code de statut HTTP 5xx à la place d'un code de statut 304 (Non modifié) ou une version mise à jour de l'objet.

CloudFront effectue les opérations suivantes :

1. Si votre origine renvoie un code d'erreur 5xx, CloudFront sert l'objet même s'il a expiré. Pendant la durée de l'erreur de mise en cache, le TTL minimum (10 secondes par défaut) CloudFront continue de répondre aux demandes des utilisateurs en diffusant l'objet depuis le cache périphérique.

   Si votre origine renvoie un code d'état 4xx, CloudFront renvoie le code d'état, et non l'objet demandé, au spectateur.
2. Une fois que le TTL minimum de mise en cache d'erreur est expiré, CloudFront essaie à nouveau d'obtenir l'objet demandé en transférant une autre demande à votre origine. Notez que si l'objet n'est pas fréquemment demandé, cela CloudFront peut l'expulser du cache périphérique alors que votre serveur d'origine renvoie encore 5xx réponses. Pour plus d'informations sur la durée pendant laquelle les objets restent dans les caches CloudFront périphériques, consultezGérer la durée pendant laquelle le contenu reste dans le cache (expiration).

Codes d'état HTTP 4xx et 5xx mis en cache CloudFront

CloudFront met en cache les codes de statut HTTP 4xx et 5xx renvoyés par votre origine, en fonction du code d'état spécifique renvoyé et du fait que votre origine renvoie ou non des en-têtes spécifiques dans la réponse.

Codes d'état HTTP 4xx et 5xx toujours mis en cache CloudFront

CloudFront met toujours en cache les codes d'état HTTP 4xx et 5xx suivants renvoyés par votre origine. Si vous avez configuré une page d'erreur personnalisée pour un code d'état HTTP, la page d'erreur personnalisée est mise en CloudFront cache.

404	Introuvable
414	URI de demande trop longue
500	Erreur de serveur interne
501	Non implémenté
502	Passerelle erronée
503	Service non disponible
504	Délai de passerelle expiré

Codes d'état HTTP 4xx mis en CloudFront cache en fonction des en-têtes **`Cache-Control`**

CloudFront ne met en cache les codes de statut HTTP 4xx suivants renvoyés par votre origine que si votre origine renvoie un en-tête `Cache-Control max-age` ou`Cache-Control s-maxage`. Si vous avez configuré une page d'erreur personnalisée pour l'un de ces codes d'état HTTP et que votre origine renvoie l'un des en-têtes de contrôle du cache, met en CloudFront cache la page d'erreur personnalisée.

400	Demande erronée
403	Accès interdit
405	Méthode non autorisée
412[1]	Échec de condition préalable
415[1]	Type de support non pris en charge

[1] CloudFront ne prend pas en charge la création de pages d'erreur personnalisées pour ces codes d'état HTTP.

Générez des réponses d'erreur personnalisées

Si un objet que vous diffusez n' CloudFront est pas disponible pour une raison quelconque, votre serveur Web renvoie généralement un code d'état HTTP pertinent CloudFront pour l'indiquer. Par exemple, si un utilisateur demande une URL non valide, votre serveur Web renvoie un code d'état HTTP 404 (Introuvable) à CloudFront, puis le CloudFront renvoie au lecteur. Au lieu d'utiliser cette réponse d'erreur par défaut, vous pouvez en créer une personnalisée qui sera CloudFront renvoyée au lecteur.

Si vous configurez CloudFront pour renvoyer une page d'erreur personnalisée pour un code d'état HTTP mais que la page d'erreur personnalisée n'est pas disponible, CloudFront renvoie au lecteur le code d'état CloudFront reçu de l'origine contenant les pages d'erreur personnalisées. Supposons, par exemple, que votre origine personnalisée renvoie un code de statut 500 et que vous ayez configuré CloudFront pour obtenir une page d'erreur personnalisée pour un code de statut 500 provenant d'un compartiment Amazon S3. Cependant, quelqu'un a accidentellement supprimé la page d'erreur personnalisée de votre compartiment Amazon S3. CloudFront renvoie un code d'état HTTP 404 (Not Found) au visualiseur qui a demandé l'objet.

Lorsque vous CloudFront renvoyez une page d'erreur personnalisée à un lecteur, vous payez les CloudFront frais standard pour la page d'erreur personnalisée, et non les frais pour l'objet demandé. Pour plus d'informations sur les CloudFront frais, consultez Amazon CloudFront Pricing.

Rubriques

Configurer le comportement de réponse aux erreurs

Plusieurs options s'offrent à vous pour gérer le CloudFront mode de réponse en cas d'erreur. Pour configurer des réponses d'erreur personnalisées, vous pouvez utiliser la CloudFront console, l' CloudFront API ou AWS CloudFormation. Indépendamment de la façon dont vous choisissez de mettre à jour la configuration, tenez compte des conseils et recommandations suivants :

- Enregistrez vos pages d'erreur personnalisées dans un emplacement accessible à CloudFront. Nous vous recommandons de les stocker dans un compartiment Amazon S3 et de ne pas les stocker dans le même emplacement que le reste du contenu de votre site Web ou de votre application. Si vous stockez les pages d'erreur personnalisées sur la même origine que votre site Web ou votre application, et que l'origine commence à renvoyer des erreurs 5xx, CloudFront vous ne pouvez pas obtenir les pages d'erreur personnalisées car le serveur d'origine n'est pas disponible. Pour plus d’informations, consultez Stockez des objets et des pages d'erreur personnalisées à différents endroits.
- Assurez-vous qu'il CloudFront est autorisé à obtenir vos pages d'erreur personnalisées. Si les pages d'erreur personnalisées sont stockées dans Amazon S3, elles doivent être accessibles au public ou vous devez configurer un contrôle CloudFront d'accès à l'origine (OAC). Si les pages d'erreur personnalisées sont stockées dans une origine personnalisée, les pages doivent être accessibles publiquement.
- (Facultatif) Configurez votre origine de sorte qu'elle ajoute un en-tête `Cache-Control` ou `Expires` avec les pages d'erreur personnalisées, si vous le souhaitez. Vous pouvez également utiliser le paramètre TTL minimal de mise en cache des erreurs pour contrôler la durée de mise en cache CloudFront des pages d'erreur personnalisées. Pour plus d’informations, consultez Contrôlez la durée de mise en CloudFront cache des erreurs.

Configurer des réponses aux erreurs personnalisées

Pour configurer des réponses d'erreur personnalisées dans la CloudFront console, vous devez disposer d'une CloudFront distribution. Dans la console, les paramètres de configuration des réponses d'erreur personnalisées ne sont disponibles que pour les distributions existantes. Pour savoir comment créer une distribution, consultez Commencez avec une CloudFront distribution de base.

Console

Pour configurer des réponses d'erreur personnalisées (console)

1. Connectez-vous à la page Distributions AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#distributions.
2. Dans la liste des distributions, sélectionnez la distribution à mettre à jour.
3. Cliquez sur l'onglet Pages d'erreur, puis cliquez sur Créer une réponse d'erreur personnalisée.
4. Entrez les valeurs applicables. Pour plus d'informations, consultez Pages d'erreur personnalisées et mise en cache des erreurs.
5. Après avoir saisi les valeurs souhaitées, cliquez sur Créer.

CloudFront API or AWS CloudFormation

Pour configurer des réponses d'erreur personnalisées avec l' CloudFront API AWS CloudFormation, utilisez le `CustomErrorResponse` type dans une distribution. Pour plus d'informations, consultez les ressources suivantes :

- AWS::CloudFront::Distribution CustomErrorResponse dans le guide de l'utilisateur AWS CloudFormation
- CustomErrorResponsedans le Amazon CloudFront API Reference

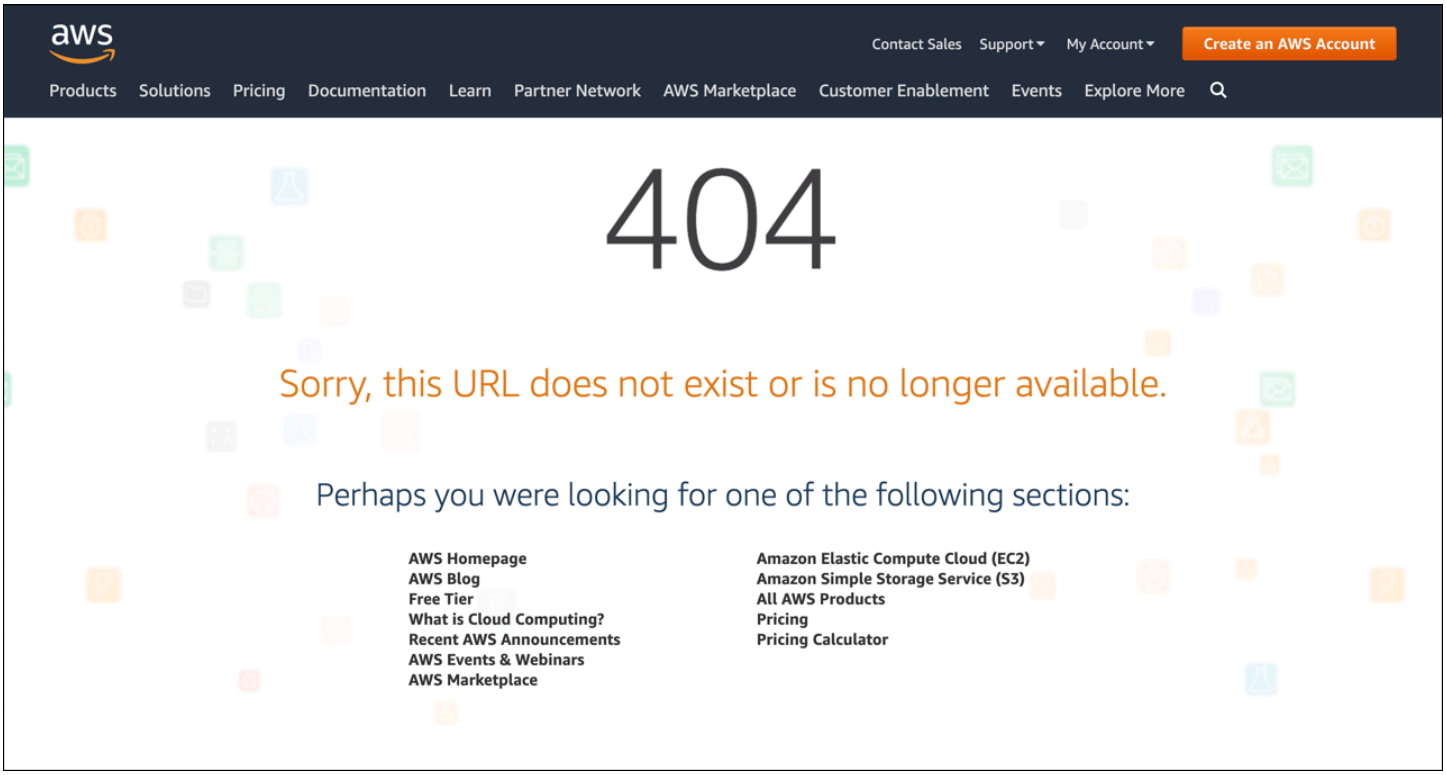
Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques

Si vous préférez afficher un message d'erreur personnalisé au lieu du message par défaut (par exemple, une page qui utilise le même format que le reste de votre site Web), vous pouvez demander

à l'utilisateur de CloudFront renvoyer un objet (tel qu'un fichier HTML) contenant votre message d'erreur personnalisé.

Pour spécifier le fichier que vous souhaitez renvoyer et les erreurs pour lesquelles le fichier doit être renvoyé, vous mettez à jour votre CloudFront distribution pour spécifier ces valeurs. Pour plus d'informations, consultez Configurer le comportement de réponse aux erreurs.

Par exemple, voici une page d'erreur personnalisée :



Vous pouvez spécifier un objet différent pour chaque code de statut HTTP pris en charge, ou utiliser le même objet pour tous les codes de statut pris en charge. Vous pouvez choisir de spécifier des pages d'erreur personnalisées pour certains codes d'état et pas d'autres.

Les objets que vous servez CloudFront peuvent être indisponibles pour diverses raisons. Ces raisons se divisent en deux grandes catégories :

- Les erreurs client indiquent un problème lié à la demande. Par exemple, un objet portant le nom spécifié n'est pas disponible, ou l'utilisateur ne dispose pas des autorisations requises pour obtenir un objet dans votre compartiment Amazon S3. Lorsqu'une erreur client se produit, l'origine renvoie un code d'état HTTP compris entre 4xx et. CloudFront
- Les erreurs serveur indiquent un problème lié au serveur d'origine. Par exemple, le serveur HTTP est occupé ou indisponible. Lorsqu'une erreur de serveur se produit, soit votre serveur d'origine

renvoie un code d'état HTTP de l'ordre de 5xx à CloudFront, soit CloudFront il ne reçoit pas de réponse de votre serveur d'origine pendant un certain temps et suppose un code d'état 504 (Gateway Timeout).

Les codes d'état HTTP pour lesquels une page d'erreur personnalisée CloudFront peut être renvoyée sont les suivants :

- 400, 403, 404, 405, 414, 416

> **Remarques**
>
> - S'il CloudFront détecte que la demande n'est peut-être pas sûre, CloudFront renvoie une erreur 400 (mauvaise demande) au lieu d'une page d'erreur personnalisée.
> - Vous pouvez créer une page d'erreur personnalisée pour le code d'état HTTP 416 (plage demandée non satisfaisante), et vous pouvez modifier le code d'état HTTP qui est CloudFront renvoyé aux utilisateurs lorsque votre origine renvoie un code d'état 416 à CloudFront. (Pour plus d'informations, consultez Modifier les codes de réponse renvoyés par CloudFront.) Cependant, CloudFront ne met pas en cache les réponses du code d'état 416, donc même si vous spécifiez une valeur pour Error Caching Minimum TTL pour le code d'état 416, CloudFront il ne l'utilise pas.

- 500, 501, 502, 503, 504

> **Note**
>
> Dans certains cas, CloudFront ne renvoie pas de page d'erreur personnalisée pour le code d'état HTTP 503, même si vous le configurez CloudFront à cet effet. Si le code CloudFront d'erreur est `Capacity Exceeded` ou`Limit Exceeded`, CloudFront renvoie un code d'état 503 au lecteur sans utiliser votre page d'erreur personnalisée.

Pour une explication détaillée de la gestion CloudFront des réponses d'erreur provenant de votre origine, consultezComment CloudFront traite les codes d'état HTTP 4xx et 5xx de votre origine.

Stockez des objets et des pages d'erreur personnalisées à différents endroits

Si vous souhaitez stocker vos objets et vos pages d’erreur personnalisées dans des emplacements différents, votre distribution doit inclure un comportement de cache pour lequel les conditions suivantes sont vraies :

- La valeur de Modèle de chemin correspond au chemin d’accès de vos messages d’erreur personnalisés. Par exemple, supposons que vous ayez enregistré des pages d’erreur personnalisées pour les erreurs 4xx dans un compartiment Amazon S3 d’un répertoire nommé `/4xx-errors`. Votre distribution doit inclure un comportement de cache pour lequel le modèle de chemin transmet les demandes de vos pages d'erreur personnalisées vers cet emplacement (par exemple,, `/4xx-errors/*`.
- La valeur d’Origine spécifie la valeur d’ID d’origine pour l’origine qui contient vos pages d’erreur personnalisées.

Pour plus d’informations, consultez Paramètres de comportement du cache.

Modifier les codes de réponse renvoyés par CloudFront

Vous pouvez configurer CloudFront pour renvoyer au lecteur un code d'état HTTP différent de celui CloudFront reçu de l'origine. Par exemple, si votre origine renvoie un code d'état 500 àCloudFront, vous souhaiterez peut-être CloudFront renvoyer une page d'erreur personnalisée et un code d'état 200 (OK) au lecteur. Il existe plusieurs raisons pour lesquelles vous souhaiterez peut-être CloudFront renvoyer au spectateur un code de statut différent de celui renvoyé par votre source d'origine CloudFront :

- Certains dispositifs Internet (certains pare-feu et proxys d'entreprise, par exemple) interceptent les codes d'état HTTP 4xx et 5xx, et empêchent le renvoi d'une réponse à l'utilisateur. Dans ce cas, si vous remplacez `200`, la réponse n'est pas interceptée.
- Si vous ne vous souciez pas de faire la distinction entre les différentes erreurs client ou serveur, vous pouvez spécifier `400` ou `500` comme valeur CloudFront renvoyée pour tous les codes d'état 4xx ou 5xx.
- Vous pouvez décider de renvoyer un code d'état `200` (OK) et un site Web statique pour que vos clients ne sachent pas que votre site Web est en panne.

Si vous activez les journaux CloudFront standard et que vous configurez CloudFront pour modifier le code d'état HTTP dans la réponse, la valeur de la `sc-status` colonne des journaux contient le code d'état que vous spécifiez. Cela n'affecte pas la valeur de la colonne `x-edge-result-type`. Elle contient le type de résultat de la réponse de l'origine. Supposons, par exemple, que vous configuriez CloudFront pour renvoyer un code d'état de `200` au visualiseur lorsque l'origine renvoie `404` (Non trouvé) à CloudFront. Lorsque l'origine répond à une demande avec un code d'état `404`, la valeur de la colonne `sc-status` dans le journal sera `200`, mais la valeur de la colonne `x-edge-result-type` sera `Error`.

Vous pouvez configurer CloudFront pour renvoyer l'un des codes d'état HTTP suivants ainsi qu'une page d'erreur personnalisée :

- 200
- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

Contrôlez la durée de mise en CloudFront cache des erreurs

CloudFront met en cache les réponses aux erreurs pendant une durée par défaut de 10 secondes. CloudFront soumet ensuite la demande suivante pour l'objet à votre origine pour voir si le problème à l'origine de l'erreur a été résolu et si l'objet demandé est disponible.

Vous pouvez spécifier la durée de mise en cache des erreurs (TTL minimum de mise en cache des erreurs) pour chaque code d'état 4xx et 5xx mis en cache. CloudFront (Pour plus d’informations, consultez Codes d'état HTTP 4xx et 5xx mis en cache CloudFront .) Lorsque vous spécifiez une durée, veuillez noter les points suivants :

- Si vous spécifiez une courte durée de mise en cache des erreurs, CloudFront vous transmettez plus de demandes à votre origine que si vous spécifiez une durée plus longue. Pour les erreurs 5xx, cela peut aggraver le problème qui a initialement amené votre origine à renvoyer une erreur.
- Lorsque votre origine renvoie une erreur pour un objet, elle CloudFront répond aux demandes concernant l'objet soit par la réponse d'erreur, soit par votre page d'erreur personnalisée jusqu'à ce que la durée de mise en cache des erreurs soit écoulée. Si vous spécifiez une longue durée de mise en cache des erreurs, vous CloudFront pouvez continuer à répondre aux demandes avec une réponse d'erreur ou votre page d'erreur personnalisée pendant une longue période une fois que l'objet sera de nouveau disponible.

> **Note**
>
> Vous pouvez créer une page d'erreur personnalisée pour le code d'état HTTP 416 (plage demandée non satisfaisante), et vous pouvez modifier le code d'état HTTP qui est CloudFront renvoyé aux utilisateurs lorsque votre origine renvoie un code d'état 416 à CloudFront. (Pour plus d'informations, consultez Modifier les codes de réponse renvoyés par CloudFront.) Cependant, CloudFront ne met pas en cache les réponses du code d'état 416, donc même si vous spécifiez une valeur pour Error Caching Minimum TTL pour le code d'état 416, CloudFront il ne l'utilise pas.

Si vous souhaitez contrôler la durée de mise en CloudFront cache des erreurs pour des objets individuels, vous pouvez configurer votre serveur d'origine pour ajouter l'en-tête applicable à la réponse d'erreur pour cet objet.

Si l'origine ajoute une `Cache-Control: s-maxage` directive `Cache-Control: max-age` ou, ou un `Expires` en-tête, met en CloudFront cache les réponses d'erreur pour la valeur la plus élevée entre la valeur de l'en-tête ou le TTL minimal de mise en cache des erreurs.

> **Note**
>
> Les valeurs `Cache-Control: max-age` et `Cache-Control: s-maxage` ne peuvent pas être supérieures à la valeur de Maximum TTL (Durée de vie maximale) définie pour le comportement de cache pour lequel la page d'erreur est récupérée.

Si l'origine ajoute d'autres `Cache-Control` directives ou n'ajoute aucun en-tête, CloudFront met en cache les réponses d'erreur pour la valeur de Error Caching Minimum TTL.

Si le délai d'expiration d'un code d'état 4xx ou 5xx pour un objet est supérieur à votre attente, et que l'objet est à nouveau disponible, vous pouvez invalider le code de l'erreur mise en cache à l'aide de l'URL de l'objet demandé. Si votre origine renvoie une réponse d'erreur pour plusieurs objets, vous devez invalider chaque objet séparément. Pour en savoir plus sur l'invalidation d'objets, consultez Invalider des fichiers pour supprimer du contenu.

Ajouter, supprimer ou remplacer du contenu CloudFront diffusé

Cette section explique comment vous assurer que vous CloudFront pouvez accéder au contenu que vous souhaitez proposer à vos visiteurs, comment spécifier les objets de votre site Web ou de votre application, et comment supprimer ou remplacer du contenu.

Rubriques

Ajoutez et accédez à du contenu qui CloudFront diffuse

Lorsque vous CloudFront souhaitez distribuer du contenu (objets), vous ajoutez des fichiers à l'une des origines que vous avez spécifiées pour la distribution et vous exposez un CloudFront lien vers les fichiers. Un emplacement CloudFront périphérique ne récupère pas les nouveaux fichiers depuis une origine tant que l'emplacement périphérique n'a pas reçu les demandes des utilisateurs les concernant. Pour plus d’informations, consultez Comment CloudFront diffuse le contenu.

Lorsque vous ajoutez un fichier que vous CloudFront souhaitez distribuer, assurez-vous de l'ajouter à l'un des compartiments Amazon S3 spécifiés dans votre distribution ou, pour une origine personnalisée, à un répertoire du domaine spécifié. De plus vérifiez que le modèle de chemin dans le comportement de cache applicable envoie les demandes à l’origine correcte.

Par exemple, imaginons qu’un modèle de chemin pour un comportement de cache soit `*.html`. Si aucun autre comportement de cache n'est configuré pour transférer les demandes vers cette origine, seuls `*.html` les fichiers CloudFront seront transférés. Dans ce scénario, par exemple, vous ne CloudFront distribuerez jamais les fichiers .jpg que vous téléchargez vers l'origine, car vous n'avez pas créé de comportement de cache incluant les fichiers .jpg.

CloudFront les serveurs ne déterminent pas le type MIME des objets qu'ils servent. Lorsque vous chargez un fichier dans votre origine, nous vous recommandons de définir le champ d'en-tête `Content-Type` pour celui-ci.

Utiliser la gestion des versions de fichiers pour mettre à jour ou supprimer le contenu d'une distribution CloudFront

Pour mettre à jour le contenu existant CloudFront configuré pour être distribué pour vous, nous vous recommandons d'utiliser un identifiant de version dans les noms de fichiers ou de dossiers. Cela vous permet de contrôler la gestion du contenu CloudFront diffusé.

Mettre à jour les fichiers existants à l'aide de noms de fichiers versionnés

Lorsque vous mettez à jour des fichiers existants dans une CloudFront distribution, nous vous recommandons d'inclure une sorte d'identifiant de version dans le nom de vos fichiers ou dans le nom de votre répertoire afin de mieux contrôler votre contenu. Cet identifiant peut être un horodatage, un numéro séquentiel ou toute autre méthode permettant de faire la distinction entre deux versions du même objet.

Par exemple, au lieu de nommer un fichier graphique image.jpg, vous pouvez l'appeler image_1.jpg. Lorsque vous souhaitez commencer à servir une nouvelle version du fichier, vous appellerez alors le nouveau fichier image_2.jpg et vous mettrez à jour les liens de votre application Web ou site Web pour pointer sur image_2.jpg. Sinon, vous pouvez placer tous les graphiques dans un répertoire images_v1, et lorsque vous souhaitez commencer à servir des nouvelles versions d'un ou plusieurs graphiques, vous créez un nouveau répertoire images_v2, et vous mettez à jour vos liens pour pointer sur ce répertoire. Avec le versionnement, vous n'avez pas à attendre l'expiration d'un objet avant de CloudFront commencer à proposer une nouvelle version de celui-ci, et vous n'avez pas à payer pour l'invalidation de l'objet.

Même si vous versionnez vos fichiers, nous vous recommandons de définir une date d'expiration. Pour de plus amples informations, veuillez consulter Gérer la durée pendant laquelle le contenu reste dans le cache (expiration).

> **Note**
>
> La spécification de noms de fichier ou de répertoire versionnés n'est pas liée à la gestion des versions d'objets Amazon S3.

Supprimez le contenu pour CloudFront ne pas le distribuer

Vous pouvez supprimer de votre origine les fichiers que vous ne souhaitez plus inclure dans votre CloudFront distribution. Cependant, le contenu du cache périphérique CloudFront continuera à être diffusé aux spectateurs jusqu'à ce que les fichiers expirent.

Si vous souhaitez supprimer un fichier immédiatement, vous devez effectuer l'une des actions suivantes :

- Utilisez la gestion des versions de fichiers. Lorsque vous utilisez le versionnement, les différentes versions d'un fichier ont des noms différents que vous pouvez utiliser dans votre CloudFront distribution, afin de modifier le fichier renvoyé aux lecteurs. Pour plus d'informations, consultez Mettre à jour les fichiers existants à l'aide de noms de fichiers versionnés.
- Invalidez le fichier. Pour plus d'informations, consultez Invalider des fichiers pour supprimer du contenu.

Personnalisez le format d'URL pour les fichiers dans CloudFront

Une fois que vous avez configuré votre origine avec les objets (contenu) que vous souhaitez proposer CloudFront à vos visiteurs, vous devez utiliser les bonnes URL pour référencer ces objets dans le code de votre site Web ou de votre application afin que celui-ci CloudFront puisse les diffuser.

Le nom de domaine que vous utilisez dans les URL pour les objets de vos pages web ou de votre application web peut être l'un des noms suivants :

- Le nom de domaine, par exemple`d111111abcdef8.cloudfront.net`, qui est attribué CloudFront automatiquement lorsque vous créez une distribution
- Votre propre nom de domaine, comme `example.com`

Par exemple, vous pouvez utiliser l'une des URL suivantes pour renvoyer le fichier `image.jpg`:

```
https://d111111abcdef8.cloudfront.net/images/image.jpg
```

```
https://example.com/images/image.jpg
```

Vous utilisez le même format d'URL que vous stockiez le contenu dans des compartiments Amazon S3 ou dans une origine personnalisée, comme l'une de vos propres serveurs web.

> **Note**
>
> Le format d'URL dépend en partie de la valeur que vous spécifiez pour Chemin d'origine dans votre distribution. Cette valeur indique CloudFront le chemin du répertoire principal pour vos objets. Pour plus d'informations sur la définition du chemin d'accès d'origine lorsque vous créez une distribution, consultez Chemin d'origine.

Pour plus d'informations sur les formats d'URL, consultez les sections suivantes.

Utilisez votre propre nom de domaine (exemple.com)

Au lieu d'utiliser le nom de domaine par défaut qui CloudFront vous est attribué lorsque vous créez une distribution, vous pouvez ajouter un autre nom de domaine plus facile à utiliser, par exemple`example.com`. En configurant votre propre nom de domaine avec CloudFront, vous pouvez utiliser une URL comme celle-ci pour les objets de votre distribution :

```
https://example.com/images/image.jpg
```

Si vous prévoyez d'utiliser le protocole HTTPS entre les utilisateurs et CloudFront, consultezUtiliser des noms de domaine alternatifs et le protocole HTTPS.

Utiliser une barre oblique (/) dans les URL

Lorsque vous spécifiez des URL pour les annuaires de votre CloudFront distribution, choisissez de toujours utiliser une barre oblique de fin ou de ne jamais utiliser de barre oblique de fin. Par exemple, choisissez uniquement l'un des formats suivants pour toutes vos URL :

```
https://d111111abcdef8.cloudfront.net/images/
```

```
https://d111111abcdef8.cloudfront.net/images
```

Pourquoi est-ce important ?

Les deux formats fonctionnent pour créer des liens vers CloudFront des objets, mais la cohérence peut aider à éviter les problèmes lorsque vous souhaitez invalider un répertoire ultérieurement. CloudFront stocke les URL exactement telles qu'elles sont définies, y compris les barres obliques finales. Ainsi, si votre format n'est pas cohérent, vous devrez invalider les URL du répertoire avec et sans barre oblique, pour vous assurer que le répertoire sera supprimé CloudFront .

Ce n’est pas pratique d’invalider les deux formats d’URL et cela peut entraîner des coûts supplémentaires. En effet, si vous devez doubler les invalidations pour couvrir les deux types d’URL, vous risquez de dépasser le nombre maximum d’invalidations gratuites autorisées pour le mois. Et si cela se produit, vous devrez payer pour toutes les invalidations, même s'il n'existe qu'un seul format pour chaque URL de répertoire. CloudFront

Création d'URL signées pour le contenu restreint

Si vous avez un contenu auquel vous souhaitez limiter l’accès, vous pouvez créer des URL signées. Par exemple, si vous voulez distribuer votre contenu uniquement aux utilisateurs qui se sont authentifiés, vous pouvez créer des URL qui sont valides uniquement pendant une période spécifiée ou qui sont disponibles uniquement à partir d’une adresse IP spécifiée. Pour plus d’informations, consultez Diffusez du contenu privé avec des URL signées et des cookies signés.

Spécifier un objet racine par défaut

Vous pouvez configurer CloudFront pour renvoyer un objet spécifique (l'objet racine par défaut) lorsqu'un utilisateur demande l'URL racine de votre distribution au lieu de demander un objet dans votre distribution. Spécifier un objet racine par défaut vous permet d’éviter d’exposer le contenu de votre distribution.

Rubriques

- Comment spécifier un objet racine par défaut
- Fonctionnement de l'objet racine par défaut
- Comment CloudFront fonctionne si vous ne définissez pas d'objet racine

Comment spécifier un objet racine par défaut

Pour éviter d’exposer le contenu de votre distribution ou de renvoyer une erreur, spécifiez un objet racine par défaut pour votre distribution en procédant comme suit.

Pour spécifier un objet racine par défaut pour votre distribution

1. Chargez l’objet racine par défaut sur l’origine sur laquelle pointe votre distribution.

   Le fichier peut être de n'importe quel type pris en charge par CloudFront. Pour une liste des contraintes relatives au nom du fichier, consultez la description de l'`DefaultRootObject`élément dans DistributionConfig.

> **Note**
>
> Si le nom de fichier de l'objet racine par défaut est trop long ou contient un caractère non valide, CloudFront renvoie l'erreur`HTTP 400 Bad Request - InvalidDefaultRootObject`. En outre, CloudFront met le code en cache pendant 10 secondes (par défaut) et écrit les résultats dans les journaux d'accès.

2. Vérifiez que les autorisations associées à l'objet accordent CloudFront au moins `read` l'accès.

   Pour de plus amples informations sur les autorisations Amazon S3, veuillez consulter Gestion des autorisations d'accès à vos ressources Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

3. Mettez à jour votre distribution pour qu'elle fasse référence à l'objet racine par défaut à l'aide de la CloudFront console ou de l' CloudFront API.

   Pour spécifier un objet racine par défaut à l'aide de la CloudFront console :

   a. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

   b. Dans le volet supérieur de la liste de distributions, sélectionnez la distribution à mettre à jour.

   c. Dans le volet Paramètres, sous l’onglet Général, sélectionnez Modifier.

   d. Dans la boîte de dialogue Modifier les paramètres, dans le champ Objet racine par défaut, entrez le nom de fichier de l’objet racine par défaut.

      Entrez uniquement le nom de l’objet, par exemple, `index.html`. N’ajoutez pas `/` devant le nom de l’objet.

   e. Sélectionnez Enregistrer les modifications.

   Pour mettre à jour votre configuration à l'aide de l' CloudFront API, vous devez spécifier une valeur pour l'`DefaultRootObject`élément dans votre distribution. Pour plus d'informations sur l'utilisation de l' CloudFront API pour spécifier un objet racine par défaut, consultez UpdateDistributionle Amazon CloudFront API Reference.

4. Vérifiez que vous avez activé l’objet racine par défaut en demandant votre URL racine. Si votre navigateur n’affiche pas l’objet racine par défaut, effectuez les opérations suivantes :

a. Vérifiez que votre distribution est entièrement déployée en consultant l'état de votre distribution dans la CloudFront console.
b. Répétez les étapes 2 et 3 pour vérifier que vous avez accordé les autorisations correctes et que vous avez correctement mis à jour la configuration de votre distribution pour spécifier l'objet racine par défaut.

Fonctionnement de l'objet racine par défaut

Imaginons que la requête suivante pointe vers l'objet `image.jpg`:

`https://d111111abcdef8.cloudfront.net/image.jpg`

En revanche, la requête suivante pointe vers l'URL racine de la même distribution plutôt que sur un objet particulier, comme dans le premier exemple :

`https://d111111abcdef8.cloudfront.net/`

Lorsque vous définissez un objet racine par défaut, une demande d'utilisateur final qui appelle la racine de votre distribution renvoie l'objet racine par défaut. Par exemple, si vous désignez le fichier `index.html` comme objet racine par défaut, une demande pour :

`https://d111111abcdef8.cloudfront.net/`

Renvoie:

`https://d111111abcdef8.cloudfront.net/index.html`

> **Note**
>
> CloudFront ne détermine pas si une URL comportant plusieurs barres obliques (`https://d111111abcdef8.cloudfront.net///`) est équivalente à. `https://d111111abcdef8.cloudfront.net/` C'est votre serveur d'origine qui effectue cette comparaison.

Si vous définissez un objet racine par défaut, une demande d'utilisateur final pour un sous-répertoire de votre distribution ne renvoie pas l'objet racine par défaut. Supposons, par exemple, qu'`index.html`il s'agisse de votre objet racine par défaut et qu'il CloudFront reçoive une demande d'utilisateur final pour le `install` répertoire de votre CloudFront distribution :

`https://d111111abcdef8.cloudfront.net/install/`

CloudFront ne renvoie pas l'objet racine par défaut même si une copie de `index.html` apparaît dans le `install` répertoire.

Si vous configurez votre distribution pour autoriser toutes les méthodes HTTP compatibles, CloudFront l'objet racine par défaut s'applique à toutes les méthodes. Par exemple, si votre objet racine par défaut est index.php et que vous écrivez dans votre application pour envoyer une `POST` demande à la racine de votre domaine (https://example.com), CloudFront envoie la demande à https://example.com/index.php.

Le comportement des objets racines CloudFront par défaut est différent de celui des documents d'index Amazon S3. Lorsque vous configurez un compartiment Amazon S3 comme site web et que vous spécifiez le document d’index, Amazon S3 renvoie le document d’index même si un utilisateur demande un sous-répertoire du compartiment. (Une copie du document d’index doit apparaître dans chaque sous-répertoire.) Pour plus d’informations sur la configuration de compartiments Amazon S3 en tant que sites web et sur les documents d’index, consultez le chapitre Hébergement de sites web sur Amazon S3 dans le Guide de l’utilisateur Amazon Simple Storage Service.

> **Important**
>
> N'oubliez pas qu'un objet racine par défaut s'applique uniquement à votre CloudFront distribution. Vous devez quand-même gérer la sécurité pour votre origine. Par exemple, si vous utilisez une origine Amazon S3, vous devez quand-même définir vos ACL de compartiment Amazon S3 de façon appropriée pour assurer le niveau d’accès souhaité sur votre compartiment.

Comment CloudFront fonctionne si vous ne définissez pas d'objet racine

Si vous ne définissez pas un objet racine par défaut, des demandes pour la racine de votre distribution sont transmises à votre serveur d’origine. Si vous utilisez une origine Amazon S3, l’un des éléments suivants peut être renvoyé :

- Liste du contenu de votre compartiment Amazon S3 — Dans l'une des conditions suivantes, le contenu de votre origine est visible par tous ceux qui ont accès CloudFront à votre distribution :
  - Votre compartiment n’est pas correctement configuré.
  - Les autorisations Amazon S3 sur le compartiment associé à votre distribution et sur les objets du compartiment accordent l’accès à quiconque.

  - Un utilisateur final accède à votre origine à l'aide de l'URL racine de votre origine.
- Liste des contenus privés de votre origine : si vous configurez votre origine en tant que distribution privée (vous êtes le seul à CloudFront y avoir accès), le contenu du compartiment Amazon S3 associé à votre distribution est visible par toute personne disposant des informations d'identification nécessaires pour accéder à votre distribution CloudFront. Dans ce cas, les utilisateurs ne peuvent pas accéder à vos contenus via l'URL racine de votre origine. Pour plus d'informations sur la distribution de contenus privés, consultez the section called "Restreindre le contenu avec des URL signées et des cookies signés".
- `Error 403 Forbidden`— CloudFront renvoie cette erreur si les autorisations sur le compartiment Amazon S3 associé à votre distribution ou les autorisations sur les objets de ce compartiment interdisent l'accès à CloudFront tout le monde.

Invalider des fichiers pour supprimer du contenu

Si vous devez supprimer un fichier des caches CloudFront Edge avant son expiration, vous pouvez effectuer l'une des opérations suivantes :

- Invalidez le fichier des caches périphériques. La prochaine fois qu'un utilisateur demande le fichier, il CloudFront retourne à l'origine pour récupérer la dernière version du fichier.
- Utilisez la gestion des versions de fichiers pour offrir une version différente du fichier dont le nom diffère. Pour plus d'informations, consultez Mettre à jour les fichiers existants à l'aide de noms de fichiers versionnés.

Rubriques

Choisissez entre l'invalidation des fichiers et l'utilisation de noms de fichiers versionnés

Pour contrôler les versions de fichiers qui sont offerts à partir de votre distribution, vous pouvez invalider des fichiers ou leur attribuer des noms de fichier versionnés. Si vous souhaitez mettre souvent vos fichiers à jour, nous vous recommandons d'utiliser principalement la gestion des versions de fichiers pour les raisons suivantes :

- La gestion des versions vous permet de contrôler quel fichier est renvoyé par une requête même lorsque l'utilisateur dispose d'une version en cache en local ou derrière un proxy de mise en cache d'entreprise. Si vous invalidez le fichier, l'utilisateur pourrait continuer de voir l'ancienne version tant qu'elle n'est pas arrivée à expiration dans ces caches.
- CloudFront les journaux d'accès incluent les noms de vos fichiers. La gestion des versions facilite donc l'analyse des résultats des modifications apportées aux fichiers.
- La gestion des versions offre un moyen d'offrir des versions différentes de fichiers à des utilisateurs différents.
- La gestion des versions simplifie la restauration par progression et la restauration entre les révisions de fichier.
- La gestion des versions est moins chère. Vous devez toujours payer pour CloudFront transférer les nouvelles versions de vos fichiers vers des emplacements périphériques, mais vous n'avez pas à payer pour invalider des fichiers.

Pour plus d'informations sur la gestion des versions de fichiers, consultez Mettre à jour les fichiers existants à l'aide de noms de fichiers versionnés.

Déterminez les fichiers à invalider

Si vous souhaitez invalider plusieurs fichiers, par exemple tous les fichiers d'un répertoire ou tous les fichiers commençant par les mêmes caractères, vous pouvez inclure le caractère générique * à la fin du chemin d'invalidation. Pour plus d'informations sur l'utilisation du caractère générique *, consultez Invalidation paths.

Pour invalider des fichiers, vous pouvez indiquer le chemin pour des fichiers individuels ou un chemin qui se termine par le caractère générique * qui peut s'appliquer à un ou plusieurs fichiers, comme illustré dans les exemples suivants :

- `/images/image1.jpg`

- `/images/image*`
- `/images/*`

Si vous souhaitez invalider des fichiers sélectionnés mais que vos utilisateurs n'accèdent pas nécessairement à tous les fichiers de votre origine, vous pouvez déterminer les fichiers que les utilisateurs ont demandés CloudFront et invalider uniquement ces fichiers. Pour déterminer les fichiers demandés par les utilisateurs, activez la journalisation des CloudFront accès. Pour plus d'informations sur les journaux d'accès, consultez Configuration et utilisation des journaux standard (journaux d'accès).

Ce que vous devez savoir lors de l'invalidation de fichiers

Lorsque vous spécifiez un fichier à invalider, reportez-vous aux informations suivantes :

Sensibilité à la casse

Les chemins d'invalidation distinguent les majuscules et minuscules. Par exemple, `/images/image.jpg` et `/images/Image.jpg` spécifiez deux fichiers différents.

Modification de l'URI à l'aide d'une fonction Lambda

Si votre CloudFront distribution déclenche une fonction Lambda lors des événements de demande du lecteur, et si la fonction modifie l'URI du fichier demandé, nous vous recommandons d'invalider les deux URI pour supprimer le fichier des caches périphériques : CloudFront

- L'URI de la demande utilisateur
- L'URI une fois que la fonction l'a modifié

Example Exemple

Supposons que votre fonction Lambda modifie l'URI d'un fichier à partir de :

`https://d111111abcdef8.cloudfront.net/index.html`

Vers un URI qui inclut un répertoire de langues :

`https://d111111abcdef8.cloudfront.net/en/index.html`

Pour invalider le fichier, vous devez spécifier les chemins suivants :

- `/index.html`
- `/en/index.html`

Pour de plus amples informations, veuillez consulter Invalidation paths.

Objet racine par défaut

Pour invalider l'objet racine (fichier) par défaut, spécifiez le chemin tout comme le chemin pour tout autre fichier. Pour plus d'informations, consultez Fonctionnement de l'objet racine par défaut.

Transmettre des cookies

Si vous avez configuré CloudFront pour transférer les cookies vers votre source, les caches CloudFront périphériques peuvent contenir plusieurs versions du fichier. Lorsque vous invalidez un fichier, toutes CloudFront les versions mises en cache du fichier sont invalidées, quels que soient les cookies associés. Vous ne pouvez pas invalider de façon sélective certaines versions et pas d'autres en fonction des cookies associés. Pour de plus amples informations, veuillez consulter Contenu du cache basé sur les cookies.

Transmettre des en-têtes

Si vous avez configuré CloudFront pour transférer une liste d'en-têtes vers votre origine et pour la mettre en cache en fonction des valeurs des en-têtes, les caches CloudFront périphériques peuvent contenir plusieurs versions du fichier. Lorsque vous invalidez un fichier, toutes CloudFront les versions mises en cache du fichier sont invalidées, quelles que soient les valeurs d'en-tête. Vous ne pouvez pas invalider de façon sélective certaines versions et pas d'autres en fonction de valeurs d'en-têtes. (Si vous configurez CloudFront pour transférer tous les en-têtes vers votre origine, vos fichiers CloudFront ne sont pas mis en cache.) Pour plus d'informations, consultez Contenu du cache basé sur les en-têtes des demandes.

Transmission de chaînes de requête

Si vous avez configuré CloudFront pour transférer les chaînes de requête vers votre origine, vous devez inclure les chaînes de requête lors de l'invalidation de fichiers, comme indiqué dans les exemples suivants :

- `/images/image.jpg?parameter1=a`
- `/images/image.jpg?parameter1=b`

Si les requêtes client incluent cinq chaînes de requête différentes pour le même fichier, vous pouvez soit invalider le fichier cinq fois (une fois par chaîne de requête), soit utiliser le caractère générique * dans le chemin d'invalidation, comme illustré dans l'exemple suivant :

```
/images/image.jpg*
```

Pour plus d'informations sur l'utilisation de caractères génériques dans le chemin d'invalidation, consultez Invalidation paths.

Pour plus d'informations sur les chaînes de requête, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

Pour déterminer les chaînes de requête utilisées, vous pouvez activer la CloudFront journalisation. Pour plus d'informations, consultez Configuration et utilisation des journaux standard (journaux d'accès).

Maximum autorisé

Pour plus d'informations sur le nombre maximal d'invalidations autorisées, consultez. Nombre maximum de requêtes d'invalidation simultanées

Fichiers Microsoft Smooth Streaming

Vous ne pouvez pas invalider les fichiers multimédia au format Microsoft Smooth Streaming lorsque vous avez activé Smooth Streaming pour le comportement de cache correspondant.

Caractères autres qu'ASCII ou caractères non sûrs dans le chemin

Si le chemin inclut des caractères autres qu'ASCII ou non sûrs, tels que définis dans la RFC 1738, encodez ces caractères dans l'URL. N'encodez pas d'URL pour les autres caractères du chemin, car cela CloudFront n'invalidera pas l'ancienne version du fichier mis à jour.

Chemins d'invalidation

Le chemin est relatif par rapport à la distribution. Par exemple, pour invalider le fichier à`https://d111111abcdef8.cloudfront.net/images/image2.jpg`, vous devez spécifier`/images/image2.jpg`.

> **Note**
>
> Dans la CloudFrontconsole, vous pouvez omettre la barre oblique principale dans le chemin, comme ceci :. `images/image2.jpg` Lorsque vous utilisez directement l' CloudFront API, les chemins d'invalidation doivent commencer par une barre oblique.

Vous pouvez également invalider simultanément plusieurs fichiers à l'aide du caractère générique *. Le caractère générique *, qui remplace 0 caractère ou plus, doit être le dernier caractère dans le chemin d'invalidation.

Si vous utilisez le AWS Command Line Interface (AWS CLI) pour invalider des fichiers et que vous spécifiez un chemin qui inclut le * caractère générique, vous devez utiliser des guillemets (") autour du chemin, par exemple. `"/*"`

Example Exemple : chemins d'invalidation

- Pour invalider tous les fichiers d'un répertoire :

  */chemin_répertoire/**

- Pour invalider un répertoire, tous ses sous-répertoires, ainsi que tous les fichiers qu'il contient, procédez comme suit :

  */chemin_répertoire**

- Pour invalider tous les fichiers qui ont le même nom mais des extensions de nom de fichier différentes, comme logo.jpg, logo.png et logo.gif :

  */chemin_répertoire/nom_fichier.**

- Pour invalider tous les fichiers d’un répertoire dont le nom de fichier commence par les mêmes caractères (par exemple, tous les fichiers pour une vidéo au format HLS), quelle que soit l’extension du nom de fichier :

  */nom-chemin du répertoire / initial-characters-in-file **

- Lorsque vous configurez CloudFront le cache en fonction des paramètres de chaîne de requête et que vous souhaitez invalider toutes les versions d'un fichier :

  */chemin_répertoire/nom_fichier.file-name-extension**

- Pour invalider tous les fichiers d'une distribution :

  /*

La longueur maximale d’un chemin est de 4 000 caractères. Vous ne pouvez pas utiliser de caractère générique dans le chemin. Il ne peut être ajouté qu'à la fin du chemin.

Pour plus d’informations sur l’invalidation de fichiers si vous utilisez une fonction Lambda pour modifier l’URI, consultez Changing the URI Using a Lambda Function.

Si le chemin d’invalidation est un répertoire et que vous n’avez pas adopté une méthode standardisée pour spécifier les répertoires, avec ou sans barre oblique de fin (/), nous vous recommandons d’invalider le répertoire avec et sans barre oblique de fin, par exemple, `/images` et `/images/`.

URL signées

Si vous utilisez des URL signées, invalidez un fichier en n’incluant que la portion de l’URL avant le point d’interrogation (?).

Invalider des fichiers

Vous pouvez utiliser la CloudFront console pour créer et exécuter une invalidation, afficher la liste des invalidations que vous avez soumises précédemment et afficher des informations détaillées sur une invalidation individuelle. Vous pouvez également copier une invalidation existante, modifier la liste des chemins de fichier et exécuter l'invalidation modifiée. Vous ne pouvez pas supprimer d'invalidations de la liste.

Table des matières

Invalider des fichiers

Pour invalider des fichiers à l'aide de la CloudFront console, procédez comme suit.

Console

Pour invalider des fichiers (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution pour laquelle vous voulez invalider des fichiers.
3. Choisissez l'onglet Invalidations.
4. Choisissez Créer une invalidation.
5. Pour les fichiers que vous voulez invalider, entrez un chemin d'invalidation par ligne. Pour plus d'informations sur la spécification de chemins d'invalidation, consultez Ce que vous devez savoir lors de l'invalidation de fichiers.

> **Important**
>
> Indiquez les chemins de fichier avec soin. Vous ne pouvez pas annuler une demande d'invalidation après l'avoir commencée.

6. Choisissez Créer une invalidation.

CloudFront API

Pour en savoir plus sur l'invalidation d'objets et l'affichage d'informations sur les invalidations, consultez les rubriques suivantes dans le manuel Amazon API Reference : CloudFront

- CreateInvalidation
- ListInvalidations
- GetInvalidation

> **Note**
>
> Si vous utilisez le AWS Command Line Interface (AWS CLI) pour invalider des fichiers et que vous spécifiez un chemin qui inclut le * caractère générique, vous devez placer le chemin entre guillemets (''), comme dans l'exemple suivant :
>
> ```
> aws cloudfront create-invalidation --distribution-id distribution_ID --paths
>  "/*"
> ```

Copier, modifier et réexécuter une invalidation existante

Vous pouvez copier une invalidation que vous avez créée précédemment, mettre à jour la liste des chemins d'invalidation d'objet et exécuter l'invalidation mise à jour. Vous ne pouvez pas copier une invalidation existante, mettre à jour les chemins d'invalidation, puis enregistrer l'invalidation mise à jour sans l'exécuter.

> **Important**
>
> Si vous copiez une invalidation toujours en cours, si vous mettez à jour la liste des chemins d'invalidation, puis si vous exécutez l'invalidation mise à jour, cela n'arrêtera ni CloudFront ne supprimera l'invalidation que vous avez copiée. Si des chemins d'invalidation apparaissent dans l'original et dans la copie, CloudFront nous essaierons d'invalider les fichiers deux fois, et les deux invalidations seront prises en compte dans votre nombre maximum d'invalidations gratuites pour le mois. Si vous avez déjà atteint le nombre maximum d'invalidations gratuites,

les deux invalidations de chaque fichier vous seront facturées. Pour plus d'informations, consultez Nombre maximum de requêtes d'invalidation simultanées.

Pour copier, modifier et réexécuter une invalidation existante

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution qui contient l'invalidation à copier.
3. Choisissez l'onglet Invalidations.
4. Sélectionnez l'invalidation que vous souhaitez copier.

   Si vous ne savez pas quelle invalidation vous souhaitez copier, vous pouvez choisir une invalidation et choisir Afficher les détails pour afficher des informations détaillées sur cette invalidation.
5. Choisissez Copier vers un nouveau.
6. Mettez à jour la liste des chemins d'invalidation la cas échéant.
7. Choisissez Créer une invalidation.

Annuler les invalidations

Lorsque vous soumettez une demande d'invalidation à CloudFront, CloudFront transfère la demande à tous les emplacements périphériques en quelques secondes, et chaque emplacement périphérique commence immédiatement à traiter l'invalidation. De ce fait, vous ne pouvez pas annuler une invalidation après l'avoir soumise.

Répertorier les invalidations

Vous pouvez afficher la liste des 100 dernières invalidations que vous avez créées et exécutées pour une distribution à l'aide de la CloudFront console. Si vous souhaitez obtenir une liste de plus de 100 invalidations, utilisez l'opération `ListInvalidations` API. Pour plus d'informations, consultez ListInvalidationsle Amazon CloudFront API Reference.

Pour répertorier des invalidations

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Sélectionnez la distribution pour laquelle vous voulez afficher une liste d'invalidations.
3. Choisissez l'onglet Invalidations.

> **Note**
>
> Vous ne pouvez pas supprimer d'invalidations de la liste.

Afficher les informations relatives à une invalidation

Vous pouvez afficher des informations détaillées sur une invalidation, notamment l'ID de distribution, l'ID d'invalidation, le statut de l'invalidation, la date et l'heure auxquelles l'invalidation a été créée, et une liste complète des chemins d'invalidation.

Pour afficher des informations sur une invalidation

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution qui contient l'invalidation pour laquelle vous souhaitez afficher des informations détaillées.
3. Choisissez l'onglet Invalidations.
4. Choisissez l'ID d'invalidation applicable ou sélectionnez l'ID d'invalidation, puis choisissez Afficher les détails.

Nombre maximum de requêtes d'invalidation simultanées

Si vous invalidez des fichiers individuellement, il est possible que des demandes d'invalidation concernant jusqu'à 3 000 fichiers par distribution soient en cours en même temps. Il peut s'agir d'une demande d'invalidation concernant jusqu'à 3 000 fichiers, de 3 000 demandes concernant chacune un fichier, ou d'une autre combinaison ne dépassant pas 3 000 fichiers. Par exemple, vous pouvez soumettre 30 demandes d'invalidation invalidant 100 fichiers chacune. Tant que toutes les 30 demandes d'invalidation sont encore en cours, vous ne pouvez pas soumettre d'autres demandes d'invalidation. Si vous dépassez le maximum, CloudFront renvoie un message d'erreur.

Si vous utilisez le caractère générique *, vous pouvez lancer en même temps des demandes concernant jusqu'à 15 chemins d'invalidation. Vous pouvez également lancer en même temps des demandes d'invalidation concernant jusqu'à 3 000 fichiers individuels par distribution, la limite

concernant les demandes d'invalidation avec caractères génériques autorisées étant indépendante de la limite applicable à l'invalidation de fichiers individuels.

Payer pour l'invalidation du fichier

Les premiers 1 000 chemins d'invalidation que vous soumettez par mois sont gratuits ; vous paierez pour chaque chemin d'invalidation au-delà de 1 000 au cours d'un mois. Un chemin d'invalidation peut être un fichier unique (comme `/images/logo.jpg`) ou plusieurs fichiers (comme `/images/*`). Un chemin qui inclut le `*` caractère générique est considéré comme un chemin, même s'il entraîne CloudFront l'invalidation de milliers de fichiers.

Le maximum de 1 000 chemins d'invalidation gratuits par mois s'applique au nombre total de chemins d'invalidation pour toutes les distributions que vous créez avec un compte AWS . Par exemple, si vous utilisez le Compte AWS `john@example.com` pour créer trois distributions et que vous soumettez 600 chemins d'invalidation pour chaque distribution au cours d'un mois donné (pour un total de 1 800 chemins d'invalidation), 800 chemins d'invalidation vous AWS seront facturés au cours de ce mois.

Les frais pour soumettre un chemin d'invalidation sont les mêmes quel que soit le nombre de fichiers que vous invalidez : un seul fichier (`/images/logo.jpg`) ou tous les fichiers associés à une distribution (`/*`). Comme vous êtes facturé par chemin dans votre demande d'invalidation, même si vous regroupez plusieurs chemins en une seule demande, chaque chemin est toujours compté individuellement à des fins de facturation.

Pour plus d'informations sur les tarifs d'invalidation, consultez Amazon CloudFront Pricing. Pour plus d'informations sur les chemins d'invalidation, consultez Invalidation paths.

Servir des fichiers compressés

Vous pouvez l'utiliser CloudFront pour compresser automatiquement certains types d'objets (fichiers) et distribuer les objets compressés lorsque les utilisateurs (navigateurs Web ou autres clients) les prennent en charge. Les utilisateurs indiquent leur prise en charge des objets compressés avec l'en-tête `Accept-Encoding` HTTP.

CloudFront peut compresser des objets en utilisant les formats de compression Gzip et Brotli. Lorsque le lecteur prend en charge les deux formats et que les deux sont présents sur le serveur de cache atteint, il CloudFront préfère Brotli. Si un seul format de compression est présent dans le serveur de cache, il le CloudFront renvoie.

> **Note**
>
> Les navigateurs web Chrome et Firefox prennent en charge la compression Brotli uniquement lorsque la demande est envoyée en HTTPS. Ces navigateurs ne prennent pas en charge Brotli avec les demandes HTTP.

Lorsque les objets demandés sont compressés, les téléchargements peuvent être plus rapides, parce que les objets sont plus petits (dans certains cas, inférieurs à un quart de la taille de l'objet original). En particulier pour JavaScript les fichiers CSS, des téléchargements plus rapides peuvent accélérer le rendu des pages Web pour vos utilisateurs. En outre, étant donné que le coût du transfert de CloudFront données est basé sur la quantité totale de données diffusées, le service d'objets compressés peut être moins coûteux que de les servir non compressés.

Certaines origines personnalisées peuvent également compresser des objets. Votre origine est peut-être en mesure de compresser des objets qui CloudFront ne le sont pas (voirTypes de fichier que CloudFront compresse). Si votre origine renvoie un objet compressé à CloudFront, CloudFront détecte que l'objet est compressé en fonction de la présence d'un `Content-Encoding` en-tête et ne le compresse pas à nouveau.

Configurer CloudFront pour compresser des objets

CloudFront Pour configurer la compression des objets, mettez à jour le comportement du cache que vous souhaitez appliquer aux objets compressés en procédant comme suit :

1. Assurez-vous que le paramètre Compress objects automatically (Compresser automatiquement les objets) est défini sur Yes (Oui). (Dans AWS CloudFormation ou dans l' CloudFront API, défini `Compress` sur`true`.)
2. Utilisez une stratégie de cache pour spécifier les paramètres de mise en cache et assurez-vous que les paramètres Gzip et Brotli sont tous les deux activés. (Dans AWS CloudFormation ou dans l' CloudFrontAPI, définissez `EnableAcceptEncodingGzip` et `EnableAcceptEncodingBrotli` à`true`.)
3. Assurez-vous que les valeurs TTL dans la stratégie de cache sont définies sur une valeur supérieure à zéro. Lorsque vous définissez les valeurs TTL sur zéro, la mise en cache est désactivée et CloudFront ne compresse pas les objets.

Pour mettre à jour un comportement de cache, vous pouvez utiliser l'un des outils suivants :

- La CloudFront console
- AWS CloudFormation
- Les kits SDK AWS et les outils de ligne de commande

Comment fonctionne CloudFront la compression

Lorsque vous configurez CloudFront pour compresser des objets (voir la section précédente), voici comment cela fonctionne :

1. Un utilisateur demande un objet. L'utilisateur inclut l'en-tête HTTP `Accept-Encoding` dans la demande et les valeurs d'en-tête incluent `gzip`, `br` ou les deux. Cela signifie qu'il prend en charge les objets compressés. Lorsque le lecteur supporte à la fois Gzip et Brotli, CloudFront il préfère Brotli.

   > **Note**
   >
   > Les navigateurs web Chrome et Firefox prennent en charge la compression Brotli uniquement lorsque la demande est envoyée en HTTPS. Ces navigateurs ne prennent pas en charge Brotli avec les demandes HTTP.

2. À l'emplacement périphérique, CloudFront recherche dans le cache une copie compressée de l'objet demandé.
3. Si l'objet compressé se trouve déjà dans le cache, il l' CloudFront envoie au visualiseur et ignore les étapes restantes.

   Si l'objet compressé n'est pas dans le cache, CloudFront transmet la demande à l'origine.

   > **Note**
   >
   > Si une copie non compressée de l'objet se trouve déjà dans le cache, vous CloudFront pouvez l'envoyer au visualiseur sans transmettre la demande à l'origine. Par exemple, cela peut se produire lorsque la compression a CloudFront été précédemment ignorée. Dans ce cas, met en CloudFront cache l'objet non compressé et continue de le servir jusqu'à ce que l'objet expire, soit expulsé ou soit invalidé.

4. Si l'origine renvoie un objet compressé, comme indiqué par la présence d'un `Content-Encoding` en-tête dans la réponse HTTP, CloudFront envoie l'objet compressé au visualiseur, l'ajoute au cache et ignore l'étape restante. CloudFront ne compresse pas à nouveau l'objet.

   Si l'origine renvoie un objet non compressé à CloudFront (il n'y a aucun `Content-Encoding` en-tête dans la réponse HTTP), CloudFront détermine si l'objet est compressible. Pour plus d'informations sur la manière de CloudFront déterminer si un objet est compressible, consultez la section suivante.
5. Si l'objet est compressible, CloudFront compressez-le, envoyez-le au visualiseur et ajoutez-le au cache. (Dans de rares cas, CloudFront cela peut ignorer la compression et envoyer l'objet décompressé au visualiseur.)

Quand CloudFront compresse des objets

La liste suivante fournit plus d'informations sur les circonstances dans lesquelles CloudFront des objets sont compressés.

La demande utilise HTTP 1.0

Si une demande CloudFront utilise le protocole HTTP 1.0, CloudFront supprime l'`Accept-Encoding`en-tête et ne compresse pas l'objet dans la réponse.

En-tête de demande **`Accept-Encoding`**

Si l'`Accept-Encoding`en-tête est absent de la demande du visualiseur, ou s'il ne contient pas `gzip` ou `br` ne contient pas de valeur, l'objet CloudFront n'est pas compressé dans la réponse. Si l'`Accept-Encoding`en-tête inclut des valeurs supplémentaires telles que`deflate`, les CloudFront supprime avant de transmettre la demande à l'origine.

Lorsqu'il CloudFront est configuré pour compresser des objets, il inclut automatiquement l'`Accept-Encoding`en-tête dans la clé de cache et dans les demandes d'origine.

Contenu dynamique

CloudFront ne compresse pas toujours le contenu dynamique. Les réponses pour le contenu dynamique sont parfois compressées, et parfois elles ne le sont pas.

Le contenu est déjà mis en cache lorsque vous configurez CloudFront pour compresser des objets

CloudFront compresse les objets lorsqu'il les extrait de l'origine. Lorsque vous configurez CloudFront pour compresser des objets, CloudFront cela ne compresse pas les objets déjà mis

en cache dans des emplacements périphériques. En outre, lorsqu'un objet mis en cache expire dans un emplacement périphérique et CloudFront transmet une autre demande pour l'objet à votre origine, CloudFront cela ne compresse pas l'objet lorsque votre origine renvoie un code d'état HTTP 304, ce qui signifie que l'emplacement périphérique possède déjà la dernière version de l'objet. Si vous souhaitez CloudFront compresser des objets déjà mis en cache dans des emplacements périphériques, vous devez invalider ces objets. Pour plus d'informations, consultez Invalider des fichiers pour supprimer du contenu.

L'origine est déjà configurée pour compresser les objets

Si vous configurez CloudFront pour compresser des objets et que l'origine compresse également des objets, l'origine doit inclure un `Content-Encoding` en-tête indiquant CloudFront que l'objet est déjà compressé. Lorsqu'une réponse provenant d'une origine inclut l'`Content-Encoding`en-tête, CloudFront elle ne compresse pas l'objet, quelle que soit la valeur de l'en-tête. CloudFront envoie la réponse au spectateur et met en cache l'objet à l'emplacement périphérique.

Types de fichiers qui CloudFront compressent

Pour obtenir la liste complète des types de fichiers CloudFront compressés, consultezTypes de fichier que CloudFront compresse.

Taille des objets qui CloudFront compressent

CloudFront compresse les objets dont la taille est comprise entre 1 000 et 10 000 000 octets.

En-tête **`Content-Length`**

L'origine doit inclure un `Content-Length` en-tête dans la réponse, qui CloudFront permet de déterminer si la taille de l'objet se situe dans la plage de CloudFront compression. Si l'`Content-Length`en-tête est absent, contient une valeur non valide ou contient une valeur en dehors de la plage de tailles qui CloudFront compresse, CloudFront ne compresse pas l'objet.

Code d'état HTTP de la réponse

CloudFront compresse les objets uniquement lorsque le code d'état HTTP de la réponse est `200`403, ou`404`.

La réponse n'a pas de corps

Lorsque la réponse HTTP de l'origine n'a pas de corps, il n'y a rien CloudFront à compresser.

En-tête **`ETag`**

CloudFront modifie parfois l'`ETag`en-tête de la réponse HTTP lorsqu'elle compresse des objets. Pour plus d'informations, consultez the section called "Conversion de l'en-tête `ETag`".

CloudFront ignore la compression

CloudFront compresse les objets au mieux. Dans de rares cas, CloudFront ignore la compression. CloudFront prend cette décision en fonction de divers facteurs, y compris la capacité de l'hôte. Si la compression CloudFront d'un objet est ignorée, il met en cache l'objet non compressé et continue de le servir aux utilisateurs jusqu'à ce que l'objet expire, soit expulsé ou soit invalidé.

Types de fichier que CloudFront compresse

Si vous configurez CloudFront pour compresser des objets, compresse CloudFront uniquement les objets dont l'en-tête de `Content-Type` réponse contient l'une des valeurs suivantes :

- `application/dash+xml`
- `application/eot`
- `application/font`
- `application/font-sfnt`
- `application/javascript`
- `application/json`
- `application/opentype`
- `application/otf`
- `application/pdf`
- `application/pkcs7-mime`
- `application/protobuf`
- `application/rss+xml`
- `application/truetype`
- `application/ttf`
- `application/vnd.apple.mpegurl`
- `application/vnd.mapbox-vector-tile`
- `application/vnd.ms-fontobject`
- `application/wasm`
- `application/xhtml+xml`
- `application/xml`

- application/x-font-opentype
- application/x-font-truetype
- application/x-font-ttf
- application/x-httpd-cgi
- application/x-javascript
- application/x-mpegurl
- application/x-opentype
- application/x-otf
- application/x-perl
- application/x-ttf
- font/eot
- font/opentype
- font/otf
- font/ttf
- image/svg+xml
- text/css
- text/csv
- text/html
- text/javascript
- text/js
- text/plain
- text/richtext
- text/tab-separated-values
- text/xml
- text/x-component
- text/x-java-source
- text/x-script
- vnd.apple.mpegurl

Conversion de l'en-tête **ETag**

Lorsque l'objet décompressé depuis l'origine inclut un en-tête ETag HTTP valide et fort, et qu'il CloudFront compresse l'objet, convertit CloudFront également la valeur d'ETagen-tête forte en valeur faible ETag et renvoie la ETag valeur faible au visualiseur. Les utilisateurs peuvent stocker la valeur ETag faible et l'utiliser pour envoyer des demandes conditionnelles avec l'en-tête HTTP If-None-Match. Cela permet aux utilisateurs et à l'origine de traiter les versions compressées et non compressées d'un objet comme sémantiquement équivalentes, ce qui réduit les transferts de données inutiles. CloudFront

Une valeur d'en-tête ETag valide et forte commence par des guillemets doubles ("). Pour convertir la ETag valeur forte en valeur faible, CloudFront ajoute les caractères W/ au début de la ETag valeur forte.

Lorsque l'objet de l'origine inclut une faible valeur d'ETagen-tête (une valeur qui commence par les caractèresW/), CloudFront ne modifie pas cette valeur et la renvoie au visualiseur telle qu'elle a été reçue de l'origine.

Lorsque l'objet de l'origine inclut une valeur d'ETagen-tête non valide (la valeur ne commence pas par " ou parW/), CloudFront supprime l'ETagen-tête et renvoie l'objet au visualiseur sans l'en-tête de ETag réponse.

Pour de plus amples informations, veuillez consulter les pages suivantes dans les documents web MDN :

- Directives (en-tête HTTP ETag)
- Validation faible (requêtes conditionnelles HTTP)
- En-tête HTTP If-None-Match

Utilisez des AWS WAF protections

Vous pouvez l'utiliser AWS WAFpour protéger vos CloudFront distributions et vos serveurs d'origine. AWS WAF est un pare-feu pour applications Web qui permet de sécuriser vos applications Web et vos API en bloquant les demandes avant qu'elles n'atteignent vos serveurs. Pour plus de détails, consultez Accélérez et protégez vos sites Web à l'aide de CloudFront et AWS WAF.

Pour activer AWS WAF les protections, vous pouvez :

- Utilisez la protection en un clic dans la CloudFront console. La protection en un clic crée une liste de contrôle d'accès AWS WAF Web (ACL Web), configure des règles pour protéger vos serveurs contre les menaces Web courantes et associe l'ACL Web à la CloudFront distribution pour vous. Les rubriques de cette section supposent l'utilisation de protections en un clic.
- Utilisez une ACL (liste de contrôle d'accès) Web préconfigurée que vous créez dans la AWS WAF console ou à l'aide des AWS WAF API. Pour plus d'informations, consultez les listes de contrôle d'accès Web (ACL) dans le guide du AWS WAF développeur et les listes AssociateWebACL dans le guide de référence des AWS WAF API

Vous pouvez l'activer AWS WAF lorsque vous :

- Créer une distribution
- Utilisation du tableau de bord Sécurité pour modifier les paramètres de sécurité d'une distribution existante

Lorsque vous utilisez la protection en un clic, CloudFront applique un ensemble de protections AWS recommandé qui :

- Bloquer les adresses IP contre les menaces potentielles en vous basant sur les informations internes d'Amazon sur les menaces.
- Vous protéger contre les vulnérabilités les plus courantes détectées dans les applications Web, comme décrit dans le Top 10 de l'OWASP.
- Vous défendre contre les acteurs malveillants qui découvrent des vulnérabilités dans les applications.

> **Important**
>
> Vous devez l'activer AWS WAF si vous souhaitez afficher les métriques de sécurité dans le tableau de bord CloudFront de sécurité. Si cette option n'est pas activée AWS WAF, vous ne pouvez utiliser le tableau de bord de sécurité que pour activer AWS WAF ou configurer les restrictions CloudFront géographiques. Pour plus d'informations sur le tableau de bord, consultez Gérez les protections AWS WAF de sécurité dans le tableau CloudFront de bord de sécurité plus loin dans cette section.

Rubriques

Activer AWS WAF pour les distributions

Vous pouvez l'activer AWS WAF lorsque vous créez une distribution, ou vous pouvez activer les protections de sécurité pour une liste de contrôle d'accès (ACL) existante.

Si vous l'activez AWS WAF pour votre CloudFront distribution, vous pouvez également activer le contrôle des robots et configurer la protection de sécurité par catégorie de bot.

Rubriques

Activer AWS WAF une nouvelle distribution

La procédure suivante explique comment l'activer AWS WAF lorsque vous créez une nouvelle CloudFront distribution.

AWS WAF Pour activer une nouvelle distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Distributions, puis Create distribution.
3. Au besoin, suivez les étapes décrites dans Créer une distribution.
4. Dans la section Web Application Firewall, choisissez Modifier, puis sélectionnez Activer les protections de sécurité.
5. Renseignez les champs suivants :

   - Utiliser le mode surveillance : vous activez le mode surveillance lorsque vous souhaitez d'abord collecter des données afin de tester le fonctionnement de la protection. Lorsque vous activez le mode de surveillance, les demandes ne sont pas bloquées si les protections étaient actives. À la place, le mode de surveillance collecte des données sur les demandes qui seraient bloquées si les protections étaient actives. Lorsque vous êtes prêt à commencer le blocage, vous pouvez activer le blocage sur la page Sécurité.
   - Protections supplémentaires — Choisissez les options que vous souhaitez activer. Si vous activez la limitation de débit, consultez the section called “Configuration de la limitation du débit” pour plus d'informations.
   - Estimation du prix — Vous pouvez ouvrir la section pour afficher un champ dans lequel vous entrez un nombre différent de demandes par mois et voyez une nouvelle estimation.
6. Vérifiez les autres paramètres de distribution, puis choisissez Créer une distribution.

Après avoir créé une distribution, CloudFront crée un tableau de bord de sécurité. Vous pouvez utiliser ce tableau de bord pour activer ou désactiver AWS WAF. Si vous ne l'avez pas AWS WAF encore activé, les tableaux et graphiques du tableau de bord restent vides.

Utilisation d'une ACL Web existante

Si vous possédez déjà une ACL Web, vous pouvez l'utiliser à la place de la protection offerte par AWS WAF.

Pour utiliser une AWS WAF configuration existante

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Effectuez l’une des actions suivantes :

a. Choisissez Créer une distribution et suivez les étapes indiquées dans Créer une distribution, puis revenez à cette rubrique.

b. Choisissez une configuration existante, puis cliquez sur l'onglet Sécurité.

3. Dans la section Web Application Firewall (WAF), choisissez Modifier, puis Activer les protections de sécurité.
4. Choisissez Utiliser la configuration WAF existante. Cette option apparaît uniquement si des ACL Web sont configurées.
5. Choisissez votre ACL Web existante dans le tableau Choisir une ACL Web.
6. Passez en revue les autres paramètres de distribution, puis choisissez Créer une distribution.

Activer le contrôle des robots

Si vous activez AWS WAF votre CloudFront distribution, vous pouvez consulter les demandes de bot pour une période donnée dans le tableau de bord de sécurité de la CloudFront console. Vous pouvez également activer ou désactiver le contrôle des robots ici.

Vous encourez des frais lorsque vous activez le contrôle des robots. Le tableau de bord de sécurité fournit une estimation des coûts.

Si vous activez le contrôle des bots, le tableau de bord de sécurité affiche le trafic des bots par type et catégorie de bot. Si vous désactivez le contrôle des robots, le trafic des robots est affiché en fonction de l'échantillonnage des demandes.

Pour activer le contrôle des bots

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l’onglet Security (Sécurité).
4. Faites défiler la page jusqu'à la section Demandes de bots pour une plage de temps donnée et choisissez Activer le contrôle des bots.
5. Dans la boîte de dialogue Contrôle des robots, sous Configuration, cochez la case Activer le contrôle des robots pour les robots courants.
6. Sélectionnez Enregistrer les modifications.

Configuration de la protection par catégorie de bot

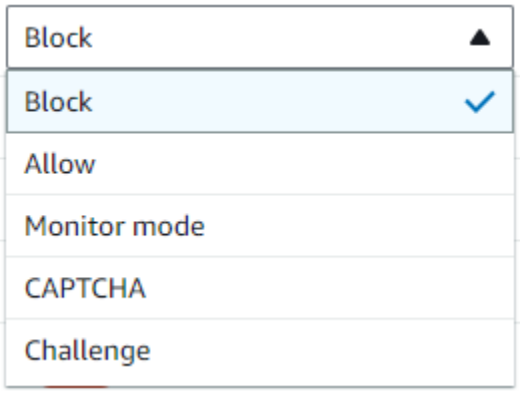
Lorsque vous activez le contrôle des robots, vous pouvez configurer la façon dont chaque bot non vérifié est traité par catégorie de bot. Par exemple, vous pouvez configurer un bot de bibliothèque HTTP en mode Surveillance et attribuer un défi à un vérificateur de liens.

> **Note**
>
> Les robots connus AWS pour être courants et vérifiables, tels que les robots d'exploration connus des moteurs de recherche, ne sont pas soumis aux actions que vous définissez ici. Le contrôle des bots confirme que les bots validés proviennent de la source indiquée avant de les marquer comme vérifiés.

Pour configurer la protection d'une catégorie de bot

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l’onglet Security (Sécurité).
4. Dans le graphique Catégories de demandes par bot, pointez sur l'un des éléments de la colonne Action de bot non vérifiée et cliquez sur l'icône de modification.

5. Ouvrez la liste obtenue et choisissez l'un des éléments suivants :
   - Bloc
   - Autorisation
   - Mode de surveillance
   - CAPTCHA
   - Défi



6. Cochez la case à côté de la liste pour valider votre modification.

Gérez les protections AWS WAF de sécurité dans le tableau CloudFront de bord de sécurité

CloudFront crée un tableau de bord de sécurité pour chacune de vos distributions. Vous utilisez les tableaux de bord de la CloudFront console. Grâce aux tableaux de bord, vous pouvez les utiliser CloudFront et les AWS WAF regrouper en un seul endroit pour surveiller et gérer les protections de sécurité communes pour vos applications Web. Les tableaux de bord fournissent les tâches et les données suivantes :

- Configuration de la sécurité : vous pouvez activer et désactiver les AWS WAF protections, et consulter toutes les protections spécifiques à l'application, telles que WordPress les protections.
- Tendances en matière de sécurité : il s'agit notamment des demandes autorisées et bloquées, des requêtes de type challenge et CAPTCHA, ainsi que des principaux types d'attaques. Vous pouvez voir les ratios de trafic et leur évolution au fil du temps. Par exemple, si toutes les demandes augmentent de 3 %, mais que les demandes autorisées augmentent de 14 %, cela signifie que vous avez autorisé une plus grande partie de votre trafic au cours de la période en cours.
- Demandes de robots : vous pouvez voir le volume de trafic provenant des robots, quels types de robots (vérifiés ou non vérifiés) et comment les pourcentages d'allocation des types de robots (vérifiés ou non vérifiés) évoluent au fil du temps. Pour plus d'informations sur l'activation du contrôle des robots, consultezActiver le contrôle des robots.

- Journaux des demandes : les données des journaux peuvent aider à répondre aux questions concernant les tendances en matière de sécurité ou les demandes de robots. Vous pouvez effectuer des recherches dans vos journaux sans écrire de requêtes et consulter des graphiques agrégés pour déterminer si un ensemble de journaux filtré est principalement piloté par un sous-ensemble de méthodes HTTP, d'adresses IP, de chemins d'URI ou de pays. Vous pouvez survoler les valeurs des graphiques et bloquer les adresses IP et les pays. Pour plus d'informations, consultez Activer AWS WAF les journaux.
- Gestion des restrictions géographiques — CloudFront et AWS WAF fourniture de fonctionnalités de restriction géographique. CloudFront fournit des restrictions géographiques gratuitement, mais les mesures relatives aux restrictions CloudFront géographiques ne sont pas affichées dans le tableau de bord de sécurité. Pour consulter les statistiques relatives aux demandes par pays bloquées, vous devez utiliser les restrictions AWS WAF géographiques. Pour ce faire, survolez une barre de pays dans le tableau de bord de sécurité et bloquez le pays. Pour plus d'informations, consultez Utiliser les restrictions CloudFront géographiques.
  - L'option Bloquer n'est peut-être pas disponible si vous avez déjà créé une AWS WAF règle personnalisée en dehors de la CloudFront console pour bloquer des pays.

Rubriques

Prérequis

Vous devez l'activer AWS WAF si vous souhaitez afficher les métriques de sécurité dans le tableau de bord CloudFront de sécurité. Si vous ne l'activez pas AWS WAF, vous ne pouvez utiliser le tableau de bord de sécurité que pour activer AWS WAF ou configurer les restrictions CloudFront géographiques.

Pour plus d'informations sur l'activation AWS WAF, consultezActiver AWS WAF pour les distributions.

Activer AWS WAF les journaux

AWS WAF les données du journal peuvent vous aider à isoler des modèles de trafic spécifiques. Par exemple, les journaux peuvent vous indiquer d'où provient un certain trafic ou ce qu'il fait.

Si vous activez la AWS WAF connexion à CloudWatch, le tableau CloudFront de bord de sécurité interroge, agrège et affiche les informations issues des CloudWatch journaux. L'utilisation du tableau

de bord de sécurité est gratuite, mais la CloudWatch tarification s'applique aux journaux consultés via le tableau de bord. Pour plus d'informations, consultez Amazon CloudWatch Pricing.

Pour activer la journalisation

1. Saisissez le volume de demandes prévu dans le champ Nombre de demandes/mois pour estimer les coûts liés à l'activation des journaux.
2. Cochez la case Activer les AWS WAF journaux.
3. Sélectionnez Activer.

CloudFront crée un groupe de CloudWatch journaux et met à jour votre AWS WAF configuration pour commencer à vous connecter à CloudWatch. Lors de la première utilisation, plusieurs minutes peuvent s'écouler avant que les données du journal s'affichent. La section Demandes du graphique répertorie chaque demande. Sous les demandes individuelles, le graphique à barres regroupe les données par méthode HTTP, les principaux chemins d'URI, les principales adresses IP et les principaux pays. Les graphiques peuvent vous aider à repérer des schémas. Par exemple, vous pouvez voir un volume disproportionné de demandes provenant d'une seule adresse IP ou de données provenant d'un pays que vous n'avez encore jamais vu dans vos journaux. Vous pouvez filtrer les demandes en fonction du pays, de l'en-tête de l'hôte et d'autres attributs afin de détecter le trafic indésirable. Une fois que vous avez identifié ce trafic, passez le curseur sur une demande individuelle ou un élément du graphique et bloquez une adresse IP ou un pays.

> **Note**
>
> Les métriques affichées sont basées sur l'ACL Web. Par conséquent, si vous associez la même ACL Web à plusieurs distributions, vous verrez toutes les métriques de votre ACL Web, et pas seulement les AWS WAF demandes traitées pour cette distribution.

Configuration de la limitation du débit

La limitation du débit fait partie des recommandations que vous pouvez recevoir lors de la configuration des protections de sécurité.

CloudFront active toujours la limitation du débit en mode moniteur. Lorsque le mode moniteur est activé, CloudFront capture des mesures qui vous indiquent si le taux que vous avez configuré dans le champ Limitation du débit a été dépassé, à quelle fréquence et dans quelle mesure.

Après avoir enregistré la distribution, CloudFront commence à collecter des données en fonction du nombre indiqué dans le champ Limitation du débit.

Vous pouvez gérer les paramètres de limitation de débit dans la section Sécurité - Web Application Firewall (WAF) de l'onglet Sécurité de n'importe quelle CloudFront distribution.

Pour configurer la limitation du débit

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l'onglet Security (Sécurité).
4. Dans la section Web Application Firewall (WAF), à côté de Limitation du débit, choisissez le message du mode Surveillance pour afficher une boîte de dialogue contenant des détails sur les données collectées. Vous pouvez éventuellement modifier la limite de taux. Une fois le taux réglé avec précision, vous pouvez choisir Activer le blocage (dans la boîte de dialogue) pour désactiver le mode moniteur. CloudFront commencera à bloquer les demandes qui dépassent la limite de débit spécifiée.

Désactiver les protections AWS WAF de sécurité

Si votre distribution n'a pas besoin AWS WAF de protections de sécurité, vous pouvez désactiver cette fonctionnalité à l'aide de la CloudFront console.

Si vous avez précédemment activé AWS WAF la protection et que vous n'avez pas choisi de configuration WAF existante (également appelée protection en un clic), vous avez CloudFront automatiquement créé une ACL Web pour vous. Pour les ACL Web créées de cette manière, la CloudFront console dissociera la ressource et supprimera l'ACL Web.

Dissocier un ACL Web est différent de le supprimer. La dissociation supprime l'ACL Web de votre distribution, mais elle n'est pas supprimée de votre Compte AWS. Pour plus d'informations, consultez les sections Associer ou dissocier une ACL Web à une AWS ressource dans le AWS WAF et AWS Firewall Manager le Guide du AWS Shield Advanced développeur.

Consultez la procédure suivante pour désactiver les AWS WAF protections et dissocier l'ACL Web de votre distribution.

Pour désactiver les protections AWS WAF de sécurité dans CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l'onglet Sécurité, puis sélectionnez Modifier.
4. Dans la section Web Application Firewall (WAF), choisissez Désactiver AWS WAF la protection.
5. Sélectionnez Enregistrer les modifications.

Remarques

- Si vous avez désactivé AWS WAF la protection de sécurité et que vous souhaitez toujours supprimer l'ACL Web de votre Compte AWS compte, vous pouvez la supprimer manuellement. Suivez la procédure pour supprimer une ACL Web. Dans la console AWS WAF & Shield, pour la page Web ACL, vous devez choisir la liste Global (CloudFront) pour trouver les ACL Web.
- Lorsque vous supprimez une distribution de la CloudFront console, il CloudFront essaiera également de supprimer l'ACL Web si vous avez choisi la protection en un clic. C'est le meilleur effort possible et ce n'est pas toujours garanti. Pour plus d'informations, voir Supprimer une distribution .

Configuration de l'accès sécurisé et restriction de l'accès au contenu

CloudFront propose plusieurs options pour sécuriser le contenu qu'il diffuse. Vous pouvez utiliser les méthodes suivantes CloudFront pour sécuriser et restreindre l'accès au contenu :

- Configurer les connexions HTTPS.
- Empêcher les utilisateurs situés dans des points géographiques spécifiques d’accéder au contenu
- Obliger les utilisateurs à accéder au contenu à l'aide d'URL CloudFront signées ou de cookies signés
- Configurer le chiffrement au niveau du champ pour des champs de contenu spécifiques
- AWS WAF À utiliser pour contrôler l'accès à votre contenu

Rubriques

Utilisez le protocole HTTPS avec CloudFront

Vous pouvez configurer CloudFront pour obliger les utilisateurs à utiliser le protocole HTTPS afin que les connexions soient chiffrées lors des CloudFront communications avec les spectateurs. Vous pouvez également CloudFront configurer l'utilisation du protocole HTTPS avec votre origine afin que les connexions soient cryptées lorsque CloudFront vous communiquez avec votre origine.

Si vous configurez CloudFront pour exiger le protocole HTTPS à la fois pour communiquer avec les spectateurs et pour communiquer avec votre origine, voici ce qui se passe lorsque CloudFront vous recevez une demande :

1. Un utilisateur envoie une demande HTTPS à CloudFront. Il y a ici une négociation SSL/TLS entre le spectateur et. CloudFront La visionneuse finit par envoyer la requête dans un format chiffré.
2. Si l'emplacement CloudFront périphérique contient une réponse mise en cache, CloudFront chiffre la réponse et la renvoie au visualiseur, qui la déchiffre.
3. Si l'emplacement CloudFront périphérique ne contient pas de réponse mise en cache, CloudFront effectue une négociation SSL/TLS avec votre origine et, une fois la négociation terminée, transmet la demande à votre origine dans un format crypté.
4. Votre origine déchiffre la demande, la traite (génère une réponse), chiffre la réponse et renvoie la réponse à. CloudFront
5. CloudFront déchiffre la réponse, la chiffre à nouveau et la transmet au lecteur. CloudFrontmet également en cache la réponse dans l'emplacement périphérique afin qu'elle soit disponible la prochaine fois qu'elle sera demandée.
6. La visionneuse déchiffre la réponse.

Le processus fonctionne essentiellement de la même manière, MediaStore que votre origine soit un compartiment Amazon S3 ou une origine personnalisée telle qu'un serveur HTTP/S.

> **Note**
>
> Pour aider à contrecarrer les attaques de type renégociation SSL, CloudFront ne prend pas en charge la renégociation pour les demandes du destinataire et de l'origine.

Pour savoir comment exiger le protocole HTTPS entre les spectateurs et CloudFront, entre CloudFront et votre origine, consultez les rubriques suivantes.

Rubriques

- Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront
- Exigez le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée
- Exiger le protocole HTTPS pour la communication entre votre Amazon S3 CloudFront et votre point d'origine
- Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront
- Protocoles et chiffrements pris en charge entre CloudFront et l'origine

Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront

Vous pouvez configurer un ou plusieurs comportements de cache dans votre CloudFront distribution afin d'exiger le protocole HTTPS pour la communication entre les utilisateurs et CloudFront. Vous pouvez également configurer un ou plusieurs comportements de cache pour autoriser à la fois le HTTP et le HTTPS, ce qui CloudFront nécessite le protocole HTTPS pour certains objets mais pas pour d'autres. Les étapes de configuration dépendent du nom de domaine que vous utilisez dans les URL d'objet :

- Si vous utilisez le nom de domaine CloudFront attribué à votre distribution, tel que d111111abcdef8.cloudfront.net, vous modifiez le paramètre Viewer Protocol Policy pour un ou plusieurs comportements de cache afin d'exiger une communication HTTPS. Dans cette configuration, CloudFront fournit le certificat SSL/TLS.

  Pour modifier la valeur de Viewer Protocol Policy à l'aide de la CloudFront console, reportez-vous à la procédure décrite plus loin dans cette section.

  Pour plus d'informations sur l'utilisation de l' CloudFront API pour modifier la valeur de l'`ViewerProtocolPolicy`élément, consultez UpdateDistributionle Amazon CloudFront API Reference.
- Si vous utilisez votre propre nom de domaine, tel que exemple.com, vous devez modifier plusieurs CloudFront paramètres. Vous devez également utiliser un certificat SSL/TLS fourni par AWS Certificate Manager (ACM), ou importer un certificat d'une autorité de certification tierce dans ACM ou du magasin de certificats IAM. Pour plus d’informations, consultez Utiliser des noms de domaine alternatifs et le protocole HTTPS.

> **Note**
>
> Si vous voulez vous assurer que les objets que les spectateurs obtiennent CloudFront étaient chiffrés lorsqu'ils CloudFront sont arrivés de chez vous, utilisez toujours le protocole HTTPS entre CloudFront et votre origine. Si vous êtes récemment passé du protocole HTTP au protocole HTTPS entre CloudFront et votre origine, nous vous recommandons d'invalider les objets situés dans des emplacements CloudFront périphériques. CloudFront renverra un objet à un visualiseur, que le protocole utilisé par le visualiseur (HTTP ou HTTPS) corresponde ou non au protocole CloudFront utilisé pour obtenir l'objet. Pour plus

d'informations sur la suppression ou le remplacement des objets dans une distribution, consultez Ajouter, supprimer ou remplacer du contenu CloudFront diffusé.

Exiger le protocole HTTPS pour les utilisateurs

Pour exiger le protocole HTTPS entre les utilisateurs et CloudFront pour un ou plusieurs comportements de cache, effectuez la procédure suivante.

Pour configurer CloudFront afin d'exiger le protocole HTTPS entre les spectateurs et CloudFront

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Dans l'onglet Comportements, sélectionnez le comportement du cache que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Spécifiez l'une des valeurs suivantes pour la politique du protocole Viewer :

   Redirect HTTP to HTTPS

   Les visionneuses peuvent utiliser les deux protocoles. Le protocole HTTP `GET` et les `HEAD` requêtes sont automatiquement redirigés vers les requêtes HTTPS. CloudFront renvoie le code d'état HTTP 301 (déplacé définitivement) ainsi que la nouvelle URL HTTPS. Le téléspectateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

   > **Important**
   >
   > Si vous envoyez`POST`,`PUT`, `DELETE``OPTIONS`, ou `PATCH` via HTTP avec un comportement de cache HTTP vers HTTPS et une version du protocole de requête HTTP 1.1 ou supérieure, CloudFront redirige la demande vers un emplacement HTTPS avec un code d'état HTTP 307 (redirection temporaire). Cette approche garantit le nouvel envoi de la demande vers le nouvel emplacement à l'aide de la même méthode et de la même charge utile du corps.
   > Si vous envoyez`POST`, `PUT` `DELETE``OPTIONS`, ou des `PATCH` requêtes via HTTP vers HTTPS, le comportement du cache avec une version du protocole de requête inférieure à HTTP 1.1 CloudFront renvoie un code d'état HTTP 403 (interdit).

Lorsqu'un utilisateur fait une requête HTTP qui est redirigée vers une requête HTTPS, les deux requêtes sont CloudFront facturées. Pour la requête HTTP, les frais concernent uniquement la demande et les en-têtes CloudFront renvoyés au lecteur. Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et à l'objet renvoyés par votre origine.

HTTPS uniquement

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code d'état HTTP 403 (Interdit) et ne renvoie pas l'objet.

5. Sélectionnez Enregistrer les modifications.
6. Répétez les étapes 3 à 5 pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger le protocole HTTPS entre les utilisateurs et CloudFront.
7. Vérifiez les éléments suivants avant d'utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s'applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d'informations, consultez Modèle de chemin d'accès.
   - Les comportements de cache acheminent les requêtes vers les origines correctes.

Exigez le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée

Vous pouvez exiger le protocole HTTPS pour la communication entre CloudFront et votre origine.

> **Note**
>
> Si votre origine est un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous ne pouvez pas le configurer CloudFront pour utiliser le protocole HTTPS avec votre origine, car Amazon S3 ne prend pas en charge le protocole HTTPS pour les points de terminaison de sites Web.

Pour exiger le protocole HTTPS entre CloudFront et votre origine, suivez les procédures décrites dans cette rubrique pour effectuer les opérations suivantes :

1. Dans votre distribution, modifiez le paramètre Stratégie de protocole d'origine pour l'origine.
2. Installez un certificat SSL/TLS sur votre serveur d'origine (cela n'est pas obligatoire lorsque vous utilisez une origine Amazon S3 ou certaines autres AWS origines).

Rubriques

Exiger le protocole HTTPS pour les origines personnalisées

La procédure suivante explique comment configurer l'utilisation du protocole HTTPS CloudFront pour communiquer avec un équilibreur de charge Elastic Load Balancing, une instance Amazon EC2 ou une autre origine personnalisée. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

Pour configurer CloudFront afin d'exiger le protocole HTTPS entre CloudFront et votre origine personnalisée

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Dans l'onglet Comportements, sélectionnez l'origine que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Modifiez les paramètres suivants :

   Origin Protocol Policy

   Modifiez le paramètre Stratégie de protocole d'origine pour les origines concernées de votre distribution :

   - HTTPS uniquement : CloudFront utilise uniquement le protocole HTTPS pour communiquer avec votre origine personnalisée.

- Match Viewer : CloudFront communique avec votre origine personnalisée via HTTP ou HTTPS, selon le protocole de la demande du spectateur. Par exemple, si vous choisissez Match Viewer for Origin Protocol Policy et que le lecteur utilise le protocole HTTPS pour demander un objet CloudFront, il utilise CloudFront également le protocole HTTPS pour transférer la demande à votre source.

  Ne sélectionnez Identique à l'utilisateur que si vous affectez la valeur Rediriger HTTP vers HTTPS ou HTTPS uniquement au paramètre Stratégie de protocole d'utilisateur.

  CloudFront ne met en cache l'objet qu'une seule fois, même si les utilisateurs font des demandes à l'aide des protocoles HTTP et HTTPS.

Origin SSL Protocols

Choisissez les Protocoles SSL d'origine pour les origines concernées de votre distribution. Le protocole SSLv3 étant moins sécurisé, nous vous recommandons de choisir SSLv3 uniquement si votre origine ne prend pas en charge TLSv1 ou version ultérieure. La poignée de main TLSv1 est à la fois rétrocompatible avec SSLv3, mais TLSv1.1 et versions ultérieures ne le sont pas. Lorsque vous choisissez SSLv3, envoie CloudFront uniquement des demandes de poignée de main SSLv3.

5. Sélectionnez Enregistrer les modifications.
6. Répétez les étapes 3 à 5 pour chaque origine supplémentaire pour laquelle vous souhaitez exiger le protocole HTTPS entre CloudFront et votre origine personnalisée.
7. Vérifiez les éléments suivants avant d’utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s’applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d’informations, consultez Modèle de chemin d’accès.
   - Les comportements de cache acheminent les requêtes vers les origines pour lesquelles vous avez modifié le paramètre Stratégie de protocole d'origine.

Installez un certificat SSL/TLS sur votre origine personnalisée

Vous pouvez utiliser un certificat SSL/TLS provenant des sources suivantes sur votre origine personnalisée :

- Si votre origine est un équilibreur de charge Elastic Load Balancing, vous pouvez utiliser un certificat fourni par AWS Certificate Manager (ACM). Vous pouvez également utiliser un certificat signé par une autorité de certification tierce reconnue et importé dans ACM.
- Pour les origines autres que les équilibreurs de charge Elastic Load Balancing, vous devez utiliser un certificat signé par une autorité de certification (CA) tierce de confiance, par exemple Comodo ou DigiCert Symantec.

Le certificat renvoyé depuis l'origine doit comprendre l'un des noms de domaine suivants :

- Le nom de domaine dans le champ du domaine Origin de l'origine (le `DomainName` champ de l' CloudFront API).
- Nom du domaine dans l'en-tête `Host`, si le comportement du cache est configuré pour transférer l'en-tête `Host` de l'origine.

Lorsque CloudFront vous utilisez le protocole HTTPS pour communiquer avec votre origine, CloudFront vérifie que le certificat a été émis par une autorité de certification fiable. CloudFront prend en charge les mêmes autorités de certification que Mozilla. Pour obtenir la liste actuelle, consultez la Liste des certificats de CA inclus dans Mozilla. Vous ne pouvez pas utiliser de certificat auto-signé pour les communications HTTPS entre CloudFront et votre origine.

> **Important**
>
> Si le serveur d'origine renvoie un certificat expiré, un certificat non valide ou un certificat auto-signé, ou s'il renvoie la chaîne de certificats dans le mauvais ordre, CloudFront abandonne la connexion TCP, renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur et définit l'`X-Cache`en-tête sur. `Error from cloudfront` De même, si la chaîne complète de certificats, y compris le certificat intermédiaire, n'est pas présente, CloudFront supprime la connexion TCP.

Exiger le protocole HTTPS pour la communication entre votre Amazon S3 CloudFront et votre point d'origine

Lorsque votre origine est un compartiment Amazon S3, les options d'utilisation du protocole HTTPS pour les communications avec ce CloudFront dernier dépendent de la manière dont vous utilisez le compartiment. Si votre compartiment Amazon S3 est configuré comme point de terminaison

de site Web, vous ne pouvez pas le configurer CloudFront pour utiliser le protocole HTTPS pour communiquer avec votre origine, car Amazon S3 ne prend pas en charge les connexions HTTPS dans cette configuration.

Lorsque votre origine est un compartiment Amazon S3 qui prend en charge les communications HTTPS, il transmet CloudFront toujours les demandes à S3 en utilisant le protocole utilisé par les utilisateurs pour envoyer les demandes. La valeur par défaut du paramètre Protocole (origines personnalisées uniquement) est Match Viewer (Identique à l'utilisateur) et elle ne peut pas être modifiée.

Si vous souhaitez exiger le protocole HTTPS pour les communications entre Amazon S3 CloudFront et Amazon S3, vous devez modifier la valeur de Viewer Protocol Policy pour rediriger le HTTP vers HTTPS ou HTTPS uniquement. La procédure décrite plus loin dans cette section explique comment utiliser la CloudFront console pour modifier la politique du protocole Viewer. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour l'`ViewerProtocolPolicy`élément d'une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

Lorsque vous utilisez HTTPS avec un compartiment Amazon S3 qui prend en charge les communications HTTPS, Amazon S3 fournit le certificat SSL/TLS. Vous n'avez donc pas à vous en préoccuper.

Exiger le protocole HTTPS pour une origine Amazon S3

La procédure suivante explique comment configurer CloudFront pour exiger le protocole HTTPS sur votre origine Amazon S3.

Pour configurer CloudFront afin d'exiger le protocole HTTPS pour votre origine Amazon S3

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Sous l’onglet Comportements, choisissez le comportement de cache à mettre à jour, puis cliquez sur Modifier.
4. Spécifiez l'une des valeurs suivantes pour Stratégie de protocole d'utilisateur :

Redirect HTTP to HTTPS

Les utilisateurs peuvent utiliser les deux protocoles, mais les requêtes HTTP sont automatiquement redirigées vers les requêtes HTTPS. CloudFront renvoie le code d'état HTTP 301 (déplacé définitivement) ainsi que la nouvelle URL HTTPS. Le téléspectateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

> **Important**
>
> CloudFront ne redirige pas `DELETEOPTIONS`,`PATCH`,`POST`, ou les `PUT` requêtes de HTTP vers HTTPS. Si vous configurez un comportement de cache pour rediriger vers HTTPS, vous CloudFront répondez au `HTTPDELETE`,`OPTIONS`, `PATCHPOST`, ou aux `PUT` demandes relatives à ce comportement de cache avec le code d'état HTTP 403 (Interdit).

Lorsqu'un utilisateur fait une requête HTTP qui est redirigée vers une requête HTTPS, les deux requêtes sont CloudFront facturées. Pour la requête HTTP, les frais concernent uniquement la demande et les en-têtes CloudFront renvoyés au lecteur. Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et à l'objet renvoyés par votre origine.

HTTPS Only

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code d'état HTTP 403 (Interdit) et ne renvoie pas l'objet.

5. Choisissez Oui, Modifier.
6. Répétez les étapes 3 à 5 pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger le protocole HTTPS entre les utilisateurs et CloudFront entre CloudFront et S3.
7. Vérifiez les éléments suivants avant d’utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s’applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d’informations, consultez Modèle de chemin d’accès.

- Les comportements de cache acheminent les requêtes vers les origines correctes.

Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront

Lorsque vous avez besoin du protocole HTTPS entre les spectateurs et votre CloudFront distribution, vous devez choisir une politique de sécurité qui détermine les paramètres suivants :

- Protocole SSL/TLS minimal CloudFront utilisé pour communiquer avec les utilisateurs.
- Les chiffrements qui CloudFront peuvent être utilisés pour chiffrer la communication avec les spectateurs.

Pour choisir une stratégie de sécurité, spécifiez la valeur applicable pour Politique de sécurité (version SSL/TLS minimale). Le tableau suivant répertorie les protocoles et les chiffrements qui CloudFront peuvent être utilisés pour chaque politique de sécurité.

Un utilisateur doit prendre en charge au moins l'un des chiffrements pris en charge pour établir une connexion HTTPS avec. CloudFront CloudFront choisit un chiffre dans l'ordre indiqué parmi les chiffrements pris en charge par le lecteur. Voir aussi Noms de chiffrement OpenSSL, s2n et RFC.

	Stratégie de sécurité						
	SSLv3	TLSv1	TLSv1_26	TLSv1.1_016	TLSv1.2_018	TLSV1.2019	TLSv1.2_2021
Protocoles SSL/TLS pris en charge							
TLSv1.3	♦	♦	♦	♦	♦	♦	♦
TLSv1.2	♦	♦	♦	♦	♦	♦	♦
TLSv1.1	♦	♦	♦	♦			
TLSv1	♦	♦	♦				
SSLv3	♦						
Chiffrements TLSv1.3 pris en charge							

	Stratégie de sécurité						
	SSLv3	TLSv1	TLSv1_2016	TLSv1.1_2016	TLSv1.2_2018	TLSV1.2_2019	TLSv1.2_2021
TLS_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦
TLS_CHACHA20_POLY1305_SHA256	♦	♦	♦	♦	♦	♦	♦
Chiffrements ECDSA pris en charge							
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES128-SHA	♦	♦	♦	♦			
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES256-SHA	♦	♦	♦	♦			
Chiffrements RSA pris en charge							

	Stratégie de sécurité						
	SSLv3	TLSv1	TLSv1_26	TLSv1.1_016	TLSv1.2_018	TLSV1.2019	TLSv1.2_2021
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES128-SHA	♦	♦	♦	♦			
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦			
AES128-GCM-SHA256	♦	♦	♦	♦	♦		
AES256-GCM-SHA384	♦	♦	♦	♦	♦		
AES128-SHA256	♦	♦	♦	♦	♦		
AES256-SHA	♦	♦	♦	♦			
AES128-SHA	♦	♦	♦	♦			
DES-CBC3-SHA	♦	♦					
RC4-MD5	♦						

Noms de chiffrement OpenSSL, s2n et RFC

OpenSSL et s2n utilisent des noms de chiffrement différents de ceux utilisés par les standards TLS (RFC 2246, RFC 4346, RFC 5246, et RFC 8446). Le tableau suivant met en correspondance les noms OpenSSL et s2n avec le nom RFC pour chaque chiffrement.

Pour les chiffrements utilisant des algorithmes d'échange de clés à courbe elliptique, CloudFront prend en charge les courbes elliptiques suivantes :

- prime256v1
- secp384r1
- X25519

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
Chiffrements TLSv1.3 pris en charge	
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
Chiffrements ECDSA pris en charge	
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Chiffrements RSA pris en charge	
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schémas de signature pris en charge entre les spectateurs et CloudFront

CloudFront prend en charge les schémas de signature suivants pour les connexions entre les spectateurs etCloudFront.

- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SHA384
- TLS_SIGNATURE_SCHEME_ECDSA_SHA512
- TLS_SIGNATURE_SCHEME_ECDSA_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SECP256R1_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SECP384R1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1
- TLS_SIGNATURE_SCHEME_ECDSA_SHA1

Protocoles et chiffrements pris en charge entre CloudFront et l'origine

Si vous choisissez d'exiger le protocole HTTPS entre CloudFront et votre origine, vous pouvez décider quel protocole SSL/TLS autoriser la connexion sécurisée, et vous CloudFront pouvez vous connecter à l'origine à l'aide de l'un des chiffrements ECDSA ou RSA répertoriés dans le tableau suivant. Votre origine doit prendre en charge au moins un de ces chiffrements pour CloudFront établir une connexion HTTPS avec votre origine.

OpenSSL et s2n utilisent des noms de chiffrement différents de ceux utilisés par les standards TLS (RFC 2246, RFC 4346, RFC 5246, et RFC 8446). Le tableau suivant inclut les noms OpenSSL et s2n avec le nom RFC pour chaque chiffrement.

Pour les chiffrements utilisant des algorithmes d'échange de clés à courbe elliptique, CloudFront prend en charge les courbes elliptiques suivantes :

- prime256v1
- secp384r1
- X25519

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
Chiffrements ECDSA pris en charge	
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
Chiffrements RSA pris en charge	
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schémas de signature pris en charge entre CloudFront et l'origine

CloudFront prend en charge les schémas de signature suivants pour les connexions entre CloudFront et l'origine.

- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384

- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SHA384
- TLS_SIGNATURE_SCHEME_ECDSA_SHA512
- TLS_SIGNATURE_SCHEME_ECDSA_SHA224
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1
- TLS_SIGNATURE_SCHEME_ECDSA_SHA1

Utiliser des noms de domaine alternatifs et le protocole HTTPS

Si vous souhaitez employer votre propre nom de domaine dans les URL de vos fichiers (comme `https://www.example.com/image.jpg`) et que vous voulez que vos utilisateurs utilisent le protocole HTTPS, vous devez réaliser les étapes décrites dans les rubriques suivantes. (Si vous utilisez le nom de domaine de CloudFront distribution par défaut dans vos URL, par exemple`https://d111111abcdef8.cloudfront.net/image.jpg`, suivez plutôt les instructions de la rubrique suivante :Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.)

> **Important**
>
> Lorsque vous ajoutez un certificat à votre distribution, le certificat est CloudFront immédiatement propagé à tous ses emplacements périphériques. Au fur et à mesure que de nouveaux emplacements périphériques sont disponiblesCloudFront , le certificat est également propagé vers ces emplacements. Vous ne pouvez pas restreindre les emplacements périphériques vers lesquels les certificats sont CloudFront propagés.

Rubriques

- Choisissez le mode de CloudFront traitement des requêtes HTTPS
- Exigences relatives à l'utilisation de certificats SSL/TLS avec CloudFront
- Quotas d'utilisation des certificats SSL/TLS avec CloudFront (HTTPS entre utilisateurs et uniquement) CloudFront
- Configuration des noms de domaine alternatifs et du protocole HTTPS

- Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA
- Augmenter les quotas pour les certificats SSL/TLS
- Rotation des certificats SSL/TLS
- Revenir d'un certificat SSL/TLS personnalisé au certificat par défaut CloudFront
- Passez d'un certificat SSL/TLS personnalisé avec adresses IP dédiées à un certificat SNI

Choisissez le mode de CloudFront traitement des requêtes HTTPS

Si vous souhaitez que vos utilisateurs utilisent le protocole HTTPS et utilisent des noms de domaine alternatifs pour vos fichiers, choisissez l'une des options suivantes pour le traitement CloudFront des requêtes HTTPS :

- Utilisation de Server Name Indication (SNI) – recommandée
- Utilisez une adresse IP dédiée dans chaque emplacement périphérique

Cette section explique le mode de fonctionnement de chaque option.

Utiliser le SNI pour répondre aux requêtes HTTPS (fonctionne pour la plupart des clients)

Server Name Indication (SNI) est une extension du protocole TLS prise en charge par les navigateurs et les clients lancés après 2010. Si vous configurez CloudFront pour répondre aux demandes HTTPS à l'aide du SNI, CloudFront associez votre nom de domaine alternatif à une adresse IP pour chaque emplacement périphérique. Lorsqu'un utilisateur envoie une demande HTTPS pour votre contenu, DNS achemine la demande vers l'adresse IP de l'emplacement périphérique correct. L'adresse IP vers votre nom de domaine est déterminée au cours de la négociation de la liaison SSL/TLS. L'adresse IP n'est pas dédiée à votre distribution.

La négociation SSL/TLS se produit tôt dans le processus d'établissement de connexion HTTPS. S'il n'est pas CloudFront possible de déterminer immédiatement à quel domaine la demande est destinée, la connexion est interrompue. Lorsqu'une visionneuse prenant en charge SNI envoie une requête HTTPS pour obtenir votre contenu, voici ce qui se passe :

1. Le visualiseur obtient automatiquement le nom de domaine à partir de l'URL de demande et l'ajoute à l'extension SNI du message d'accueil du client TLS.

2. Lorsqu'il CloudFront reçoit le client TLS hello, il utilise le nom de domaine de l'extension SNI pour trouver la CloudFront distribution correspondante et renvoie le certificat TLS associé.
3. Le visualiseur et CloudFront exécutent la négociation SSL/TLS.
4. CloudFront renvoie le contenu demandé au spectateur.

Pour une liste actuelle des navigateurs qui prennent en charge l'extension SNI, consultez l'entrée Server Name Indication de Wikipedia.

Si vous souhaitez utiliser l'extension SNI mais que certains navigateurs de vos utilisateurs ne la prennent pas en charge, vous disposez des solutions suivantes :

- Configurez CloudFront pour répondre aux requêtes HTTPS en utilisant des adresses IP dédiées au lieu du SNI. Pour plus d'informations, consultez Utiliser une adresse IP dédiée pour répondre aux requêtes HTTPS (fonctionne pour tous les clients).
- Utilisez le certificat CloudFront SSL/TLS au lieu d'un certificat personnalisé. Cela nécessite que vous utilisiez le nom de CloudFront domaine de votre distribution dans les URL de vos fichiers, par exemple,`https://d111111abcdef8.cloudfront.net/logo.png`.

  Si vous utilisez le CloudFront certificat par défaut, les utilisateurs doivent prendre en charge le protocole SSL TLSv1 ou version ultérieure. CloudFront ne prend pas en charge le protocole SSLv3 avec le certificat par défautCloudFront .

  Vous devez également remplacer le certificat SSL/TLS utilisé par un certificat personnalisé par le certificat par défaut : CloudFront CloudFront

  - Si vous n'avez pas utilisé votre distribution pour transmettre votre contenu, vous pouvez juste modifier la configuration. Pour plus d'informations, consultez Mettre à jour une distribution.
  - Si vous avez utilisé votre distribution pour distribuer votre contenu, vous devez créer une nouvelle CloudFront distribution et modifier les URL de vos fichiers afin de réduire ou d'éliminer la durée pendant laquelle votre contenu n'est pas disponible. Pour plus d'informations, consultez Revenir d'un certificat SSL/TLS personnalisé au certificat par défaut CloudFront .
- Si vous pouvez contrôler le navigateur employé par vos utilisateurs, demandez-leur de mettre leur navigateur à niveau afin qu'il accepte l'extension SNI.
- Utilisez HTTP au lieu de HTTPS.

Utiliser une adresse IP dédiée pour répondre aux requêtes HTTPS (fonctionne pour tous les clients)

L'utilisation d'une extension SNI (Server Name Indication) est une façon d'associer une demande à un domaine. Une autre méthode consiste à utiliser une adresse IP dédiée. Si vous avez des utilisateurs qui ne peuvent pas effectuer une mise à niveau vers un navigateur ou un client lancé après 2010, vous pouvez utiliser une adresse IP dédiée pour servir les demandes HTTPS. Pour une liste actuelle des navigateurs qui prennent en charge l'extension SNI, consultez l'entrée Server Name Indication de Wikipedia.

> **Important**
>
> Si vous configurez CloudFront pour répondre aux requêtes HTTPS à l'aide d'adresses IP dédiées, vous devrez payer des frais mensuels supplémentaires. Ces frais commencent lors de l'association de votre certificat SSL/TLS à une distribution et de l'activation de cette distribution. Pour plus d'informations sur CloudFront les tarifs, consultez Amazon CloudFront Pricing. Consultez également Using the Same Certificate for Multiple CloudFront Distributions.

Lorsque vous configurez CloudFront pour répondre aux demandes HTTPS à l'aide d'adresses IP dédiées, CloudFront associez votre certificat à une adresse IP dédiée dans chaque emplacement CloudFront périphérique. Lorsqu'une visionneuse envoie une requête HTTPS pour obtenir votre contenu, voici ce qui se passe :

1. DNS achemine la requête à l'adresse IP de votre distribution dans l'emplacement périphérique concerné.
2. Si une demande du client fournit l'extension SNI dans le `ClientHello` message, CloudFront recherche une distribution associée à ce SNI.
   - S'il y a une correspondance, CloudFront répond à la demande avec le certificat SSL/TLS.
   - S'il n'y a pas de correspondance, CloudFront utilise plutôt l'adresse IP pour identifier votre distribution et pour déterminer le certificat SSL/TLS à renvoyer au lecteur.
3. Le visualiseur et CloudFront exécutent la négociation SSL/TLS à l'aide de votre certificat SSL/TLS.
4. CloudFront renvoie le contenu demandé au spectateur.

Cette méthode fonctionne pour toutes les requêtes HTTPS, quel que soit le navigateur ou autre client employé par l'utilisateur.

Demande l'autorisation d'utiliser au moins trois certificats IP SSL/TLS dédiés

Si vous avez besoin d'une autorisation pour associer de manière permanente au moins trois certificats IP dédiés SSL/TLS CloudFront, effectuez la procédure suivante. Pour de plus amples informations sur les requêtes HTTPS, consultez Choisissez le mode de CloudFront traitement des requêtes HTTPS.

> **Note**
>
> Cette procédure permet d'utiliser au moins trois certificats IP dédiés dans vos CloudFront distributions. La valeur par défaut est 2. N'oubliez pas que vous ne pouvez pas lier plusieurs certificats SSL à une distribution.
> Vous ne pouvez associer qu'un seul certificat SSL/TLS à une CloudFront distribution à la fois. Ce nombre correspond au nombre total de certificats IP SSL dédiés que vous pouvez utiliser dans toutes vos CloudFront distributions.

Pour demander l'autorisation d'utiliser trois certificats ou plus avec une CloudFront distribution

1. Accédez au Centre de support et créez une demande.
2. Indiquez le nombre de certificats dont vous avez besoin et décrivez les circonstances de votre demande. Nous mettrons votre compte à jour dès que possible.
3. Poursuivez avec la procédure suivante.

Exigences relatives à l'utilisation de certificats SSL/TLS avec CloudFront

Les exigences relatives à l'utilisation des certificats SSL/TLS sont décrites dans cette rubrique. Elles s'appliquent, sauf indication contraire, aux deux certificats suivants :

- Certificats pour l'utilisation du protocole HTTPS entre les utilisateurs et CloudFront
- Certificats pour l'utilisation du protocole HTTPS entre CloudFront et votre origine

Rubriques

- Auteur du certificat

- Région AWS pour AWS Certificate Manager
- Format du certificat
- Certificats intermédiaires
- Type de clé
- Clé privée
- Autorisations
- Taille de la clé de certificat
- Types de certificats pris en charge
- Date d'expiration de certificat et renouvellement
- Noms de domaine dans la CloudFront distribution et dans le certificat
- Version minimale du protocole SSL/TLS
- Versions de HTTP prises en charge

Auteur du certificat

Nous vous recommandons d'utiliser un certificat délivré parAWS Certificate Manager (ACM). Pour plus d'informations sur l'obtention d'un certificat auprès d'ACM, reportez-vous au Guide de l'utilisateur AWS Certificate Manager. Pour utiliser un certificat ACM avec CloudFront, assurez-vous de demander (ou d'importer) le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).

CloudFront prend en charge les mêmes autorités de certification (CA) que Mozilla. Par conséquent, si vous n'utilisez pas ACM, utilisez un certificat émis par une autorité de certification figurant sur la liste des certificats d'autorité de certification inclus par Mozilla. Pour plus de détails sur l'obtention et l'installation d'un certificat, consultez la documentation du logiciel de votre serveur HTTP et celle de l'autorité de certification.

Région AWS pour AWS Certificate Manager

Pour utiliser un certificat dans AWS Certificate Manager (ACM) afin d'exiger le protocole HTTPS entre les utilisateursCloudFront, assurez-vous de demander (ou d'importer) le certificat dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`).

Si vous souhaitez exiger le protocole HTTPS entre CloudFront et votre origine, et que vous utilisez un équilibreur de charge dans Elastic Load Balancing comme origine, vous pouvez demander ou importer le certificat dans n'importe quel Région AWS système.

Format du certificat

Le certificat doit être au format PEM X.509. Il s'agit du format par défaut si vous utilisez AWS Certificate Manager.

Certificats intermédiaires

Si vous utilisez une autorité de certification tierce, indiquez tous les certificats intermédiaires dans la chaîne de certificats du fichier `.pem`, en commençant par celui de l'autorité de certification qui a signé le certificat de votre domaine. En règle générale, vous trouverez sur le site web de votre autorité de certification un fichier répertoriant les certificats racines et intermédiaires dans l'ordre approprié pour la chaîne.

> **Important**
>
> N'incluez par les éléments suivants : le certificat racine, les certificats intermédiaires non approuvés ou le certificat de la clé publique de votre autorité de certification.

Voici un exemple :

```
-----BEGIN CERTIFICATE-----
Intermediate certificate 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate certificate 1
-----END CERTIFICATE-----
```

Type de clé

CloudFront prend en charge les paires de clés publiques-privées RSA et ECDSA.

CloudFront prend en charge les connexions HTTPS aux utilisateurs et aux origines à l'aide de certificats RSA et ECDSA. Avec AWS Certificate Manager (ACM), vous pouvez demander et importer des certificats RSA ou ECDSA, puis les associer à votre distribution. CloudFront

Pour obtenir la liste des chiffrements RSA et ECDSA pris en charge par ces protocoles CloudFront que vous pouvez négocier dans le cadre de connexions HTTPS, consultez et. the section called "Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront" the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine"

Clé privée

Si vous utilisez un certificat d'une autorité de certification tierce, notez les points suivants :

- La clé privée doit correspondre à la clé publique qui se trouve dans le certificat.
- La clé privée doit être au format PEM.
- La clé privée ne peut pas être chiffrée avec un mot de passe.

Si AWS Certificate Manager (ACM) a fourni le certificat, ACM ne libère pas la clé privée. La clé privée est stockée dans ACM pour être utilisée par les AWS services intégrés à ACM.

Autorisations

Vous devez avoir l'autorisation d'utiliser et d'importer le certificat SSL/TLS. Si vous utilisez AWS Certificate Manager (ACM), nous vous recommandons d'utiliser AWS Identity and Access Management des autorisations pour restreindre l'accès aux certificats. Pour plus d'informations, consultez see Identity and Access Management dans le Guide de l'utilisateur AWS Certificate Manager .

Taille de la clé de certificat

La taille de clé de certificat CloudFront prise en charge dépend du type de clé et de certificat.

Pour les certificats RSA :

CloudFront prend en charge les clés RSA 1024 bits, 2048 bits, 3072 bits et 4096 bits. La longueur de clé maximale pour un certificat RSA que vous utilisez CloudFront est de 4 096 bits.

Notez qu'ACM émet des certificats RSA avec des clés allant jusqu'à 2 048 bits. Pour utiliser un certificat RSA 3072 bits ou 4096 bits, vous devez obtenir le certificat en externe et l'importer dans ACM, après quoi vous pourrez l'utiliser. CloudFront

Pour en savoir plus sur la façon de déterminer la taille d'une clé RSA, consultez Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA.

Pour les certificats ECDSA :

CloudFront prend en charge les clés 256 bits. Pour utiliser un certificat ECDSA dans ACM afin d'exiger le protocole HTTPS entre les utilisateurs CloudFront, utilisez la courbe elliptique prime256v1.

Types de certificats pris en charge

CloudFront prend en charge tous les types de certificats émis par une autorité de certification fiable.

Date d'expiration de certificat et renouvellement

Si vous utilisez des certificats que vous obtenez d'une autorité de certification (CA) tierce, vous devez surveiller les dates d'expiration des certificats et renouveler les certificats que vous importez dans AWS Certificate Manager (ACM) ou que vous téléchargez dans le magasin de AWS Identity and Access Management certificats avant leur expiration.

Si vous utilisez des certificats fournis par ACM, ACM gère automatiquement le renouvellement des certificats. Pour plus d'informations, consultez Renouvellement géré dans le Guide de l'utilisateur AWS Certificate Manager .

Noms de domaine dans la CloudFront distribution et dans le certificat

Lorsque vous utilisez une origine personnalisée, le certificat SSL/TLS de votre origine inclut un nom de domaine dans le champ Common Name (Nom commun) et éventuellement plusieurs autres dans le champ Subject Alternative Names (Noms SAN). (CloudFront prend en charge les caractères génériques dans les noms de domaine des certificats.)

L'un des noms de domaines du certificat doit correspondre au nom de domaine spécifié pour le nom du domaine d'origine. Si aucun nom de domaine ne correspond, CloudFront renvoie le code `502 (Bad Gateway)` d'état HTTP au lecteur.

> **Important**
>
> Lorsque vous ajoutez un autre nom de domaine à une distribution, CloudFront vérifiez que le nom de domaine alternatif est couvert par le certificat que vous avez joint. Le certificat doit couvrir le nom de domaine alternatif dans le champ SAN du certificat. Cela signifie que le champ SAN doit contenir une correspondance exacte pour le nom de domaine alternatif ou un caractère générique au même niveau que le nom de domaine alternatif que vous ajoutez. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs.

Version minimale du protocole SSL/TLS

Si vous utilisez des adresses IP dédiées, définissez la version minimale du protocole SSL/TLS pour la connexion entre les utilisateurs et choisissez une politique CloudFront de sécurité.

Pour plus d'informations, consultez Politique de sécurité (version SSL/TLS minimale) dans la rubrique Référence des paramètres de distribution.

Versions de HTTP prises en charge

Si vous associez un certificat à plusieurs CloudFront distributions, toutes les distributions associées au certificat doivent utiliser la même option pourVersions de HTTP prises en charge. Vous spécifiez cette option lorsque vous créez ou mettez à jour une CloudFront distribution.

Quotas d'utilisation des certificats SSL/TLS avec CloudFront (HTTPS entre utilisateurs et uniquement) CloudFront

Notez les quotas suivants concernant l'utilisation de certificats SSL/TLS avec. CloudFront Ces quotas s'appliquent uniquement aux certificats SSL/TLS que vous fournissez à l'aide de AWS Certificate Manager (ACM), que vous importez dans ACM ou que vous téléchargez dans le magasin de certificats IAM pour les communications HTTPS entre les utilisateurs et. CloudFront

Pour plus d'informations, consultez Augmenter les quotas pour les certificats SSL/TLS.

Nombre maximum de certificats par CloudFront distribution

Vous pouvez associer au maximum un certificat SSL/TLS à chaque distribution. CloudFront

Nombre maximal de certificats que vous pouvez importer dans ACM ou télécharger dans le magasin de certificats IAM

Si vous avez obtenu vos certificats SSL/TLS auprès d'une autorité de certification tierce, vous devez stocker les certificats dans l'un des emplacements suivants :

- AWS Certificate Manager – Pour connaître le quota actuel sur le nombre de certificats ACM, consultez Quotas dans le Guide de l'utilisateur AWS Certificate Manager . Le quota indiquée est un total qui inclut les certificats que vous mettez en service à l'aide d'ACM et les certificats que vous importez dans ACM.
- Magasin de certificats IAM : pour connaître le quota actuel (anciennement connu sous le nom de limite) du nombre de certificats que vous pouvez télécharger vers le magasin de certificats

IAM pour un AWS compte, consultez la section Limites IAM et STS dans le guide de l'utilisateur IAM. Vous pouvez demander un quota plus élevé dans AWS Management Console.

Nombre maximum de certificats par AWS compte (adresses IP dédiées uniquement)

Si vous souhaitez diffuser des requêtes HTTPS en utilisant des adresses IP dédiées, notez les points suivants :

- Par défaut, vous CloudFront autorise à utiliser deux certificats avec votre AWS compte, l'un pour un usage quotidien et l'autre lorsque vous devez alterner les certificats pour plusieurs distributions.
- Si vous avez besoin de plus de deux certificats SSL/TLS personnalisés pour votre AWS compte, rendez-vous au Support Center et créez un dossier. Indiquez le nombre de certificats que vous souhaitez être autorisé à utiliser et décrivez les circonstances de votre demande. Nous mettrons votre compte à jour dès que possible.

Utilisez le même certificat pour les CloudFront distributions créées à l'aide de AWS comptes différents

Si vous utilisez une autorité de certification tierce et que vous souhaitez utiliser le même certificat avec plusieurs CloudFront distributions créées à l'aide de AWS comptes différents, vous devez importer le certificat dans ACM ou le télécharger dans le magasin de certificats IAM une fois pour chaque AWS compte.

Si vous utilisez des certificats fournis par ACM, vous ne pouvez pas configurer CloudFront pour utiliser des certificats créés par un autre AWS compte.

Utiliser le même certificat pour CloudFront et pour les autres AWS services

Si vous avez acheté un certificat auprès d'une autorité de certification fiable telle que Comodo ou Symantec, vous pouvez utiliser le même certificat pour CloudFront et pour d'autres AWS services. DigiCert Si vous importez le certificat dans ACM, vous ne devez l’importer qu’une seule fois pour l’utiliser pour plusieurs services AWS .

Si vous utilisez les certificats fournis par ACM, ces certificats sont stockés dans ACM.

Utiliser le même certificat pour plusieurs CloudFront distributions

Vous pouvez utiliser le même certificat pour l'une ou l'ensemble des CloudFront distributions que vous utilisez pour répondre aux requêtes HTTPS. Remarques :

- Vous pouvez utiliser le même certificat pour diffuser les requêtes utilisant des adresses IP dédiées et pour celles utilisant l’extension SNI.

- Vous ne pouvez associer qu'un seul certificat à chaque distribution.
- Chaque distribution doit inclure un ou plusieurs noms de domaines alternatifs qui apparaissent aussi dans les champs Common Name ou Subject Alternative Name du certificat.
- Si vous envoyez des requêtes HTTPS à l'aide d'adresses IP dédiées et que vous avez créé toutes vos distributions en utilisant le même AWS compte, vous pouvez réduire considérablement vos coûts en utilisant le même certificat pour toutes les distributions. CloudFront des frais pour chaque certificat, et non pour chaque distribution.

  Supposons, par exemple, que vous créez trois distributions en utilisant le même AWS compte et que vous utilisiez le même certificat pour les trois distributions. Un seul montant correspondant à l'usage des adresses IP dédiées vous sera facturé.

  Toutefois, si vous envoyez des requêtes HTTPS à l'aide d'adresses IP dédiées et que vous utilisez le même certificat pour créer CloudFront des distributions sur différents AWS comptes, les frais d'utilisation des adresses IP dédiées sont facturés à chaque compte. Par exemple, si vous créez trois distributions en utilisant trois AWS comptes différents et que vous utilisez le même certificat pour les trois distributions, les frais d'utilisation des adresses IP dédiées sont facturés à chaque compte.

Configuration des noms de domaine alternatifs et du protocole HTTPS

Pour utiliser des noms de domaine alternatifs dans les URL de vos fichiers et pour utiliser le protocole HTTPS entre les utilisateurs CloudFront, suivez les procédures applicables.

Rubriques

Obtenir un certificat SSL/TLS

Commencez par obtenir un certificat SSL/TLS si vous n'en avez pas déjà un. Pour plus d'informations, consultez la documentation pertinente :

- Pour utiliser un certificat fourni par AWS Certificate Manager (ACM), consultez le guide de l'AWS Certificate Manager utilisateur. Passez ensuite à Mettez à jour votre CloudFront distribution.

> **Note**
>
> Nous vous recommandons d'utiliser ACM pour provisionner, gérer et déployer vos certificats SSL/TLS sur des ressources gérées AWS . Vous devez demander un certificat ACM dans la région USA Est (Virginie du Nord).

- Pour obtenir un certificat auprès d'une autorité de certification tierce, consultez la documentation fournie par l'autorité de certification. Lorsque vous avez obtenu le certificat, passez à la procédure suivante.

Importer un certificat SSL/TLS

Si vous avez obtenu votre certificat auprès d'une autorité de certification tierce, importez-le dans ACM ou chargez-le dans le magasin de certificats IAM :

ACM (recommandé)

ACM vous permet d'importer des certificats tiers à partir de la console ACM, ainsi que par programmation. Pour plus d'informations sur l'importation d'un certificat dans ACM, consultez Importation de certificats dans AWS Certificate Manager dans le Guide de l'utilisateur AWS Certificate Manager . Vous devez importer le certificat dans la région USA Est (Virginie du Nord).

Magasin de certificats IAM

(Non recommandé) Utilisez la AWS CLI commande suivante pour télécharger votre certificat tiers dans le magasin de certificats IAM.

```
aws iam upload-server-certificate \
        --server-certificate-name CertificateName \
        --certificate-body file://public_key_certificate_file \
        --private-key file://privatekey.pem \
        --certificate-chain file://certificate_chain_file \
        --path /cloudfront/path/
```

Notez ce qui suit :

- AWS compte : vous devez télécharger le certificat dans le magasin de certificats IAM en utilisant le même AWS compte que celui que vous avez utilisé pour créer votre CloudFront distribution.

- Paramètre --path : lorsque vous chargez le certificat dans IAM, la valeur du paramètre `--path` (chemin du certificat) doit commencer par `/cloudfront/`, comme `/cloudfront/production/` ou `/cloudfront/test/`. Le chemin doit se terminer par un caractère /.
- Certificats existants : vous devez affecter aux paramètres `--server-certificate-name` et `--path` des valeurs différentes de celles qui sont associées aux certificats existants.
- Utilisation de la CloudFront console — La valeur que vous spécifiez pour le `--server-certificate-name` paramètre dans AWS CLI, par exemple`myServerCertificate`, apparaît dans la liste des certificats SSL de la CloudFront console.
- Utilisation de l' CloudFront API — Prenez note de la chaîne alphanumérique AWS CLI renvoyée, `AS1A2M3P4L5E67SIIXR3J` par exemple. Il s'agit de la valeur que vous spécifierez dans l'élément `IAMCertificateId`. Vous n'avez pas besoin de l'ARN IAM, que renvoie également la CLI.

Pour plus d'informations sur le AWS CLI, consultez le guide de l'AWS Command Line Interface utilisateur et le manuel de référence des AWS CLI commandes.

Mettez à jour votre CloudFront distribution

Pour mettre à jour les paramètres de votre distribution, procédez comme suit :

Pour configurer votre CloudFront distribution pour les noms de domaine alternatifs

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Sous l'onglet General, choisissez Edit.
4. Mettez à jour les valeurs suivantes :

   Nom de domaine alternatif (CNAME)

   Choisissez Ajouter un élément pour ajouter les noms de domaine alternatifs applicables. Séparez les noms de domaines par des virgules ou saisissez chaque nom de domaine sur une nouvelle ligne.

   Certificat SSL personnalisé

   Sélectionnez un certificat dans la liste déroulante.

Jusqu'à 100 certificats sont répertoriés ici. Si vous avez plus de 100 certificats et que vous ne voyez pas le certificat que vous souhaitez ajouter, vous pouvez taper un nom ARN de certificat dans le champ pour le choisir.

Si vous avez chargé un certificat dans le magasin de certificats IAM mais qu'il n'apparaît pas dans la liste et que vous ne pouvez pas le choisir en tapant son nom dans le champ, revoyez la procédure Importer un certificat SSL/TLS afin de vérifier si vous avez bien chargé le certificat.

> **Important**
>
> Après avoir associé votre certificat SSL/TLS à votre CloudFront distribution, ne le supprimez pas d'ACM ou du magasin de certificats IAM tant que vous ne l'avez pas retiré de toutes les distributions et que toutes les distributions n'ont pas été déployées.

5. Sélectionnez Enregistrer les modifications.
6. Configurez CloudFront pour exiger le protocole HTTPS entre les spectateurs et CloudFront :
   a. Sous l'onglet Comportements, choisissez le comportement de cache à mettre à jour, puis sélectionnez Modifier.
   b. Spécifiez l'une des valeurs suivantes pour Politique de protocole d'utilisateur :

      Redirect HTTP to HTTPS

      Les utilisateurs peuvent utiliser les deux protocoles, mais les requêtes HTTP sont automatiquement redirigées vers les requêtes HTTPS. CloudFrontrenvoie `301 (Moved Permanently)` le code d'état HTTP ainsi que la nouvelle URL HTTPS. Le téléspectateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

      > **Important**
      >
      > CloudFront ne redirige pas `DELETEOPTIONS`,`PATCH`,`POST`, ou les `PUT` requêtes de HTTP vers HTTPS. Si vous configurez un comportement de cache pour rediriger vers HTTPS, vous CloudFront répondez au HTTP`DELETE`,`OPTIONS`,

PATCHPOST, ou aux PUT demandes relatives à ce comportement de cache avec un code d'état HTTP403 (Forbidden).

Lorsqu'un utilisateur fait une requête HTTP qui est redirigée vers une requête HTTPS, les deux requêtes sont CloudFront facturées. Pour la requête HTTP, les frais concernent uniquement la demande et les en-têtes CloudFront renvoyés au lecteur. Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et au fichier renvoyés par votre origine.

HTTPS Only

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code d'état HTTP 403 (Forbidden) et ne renvoie pas le fichier.

c. Choisissez Oui, Modifier.

d. Répétez les étapes a à c pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger le protocole HTTPS entre les utilisateurs etCloudFront.

7. Vérifiez les éléments suivants avant d'utiliser la configuration mise à jour dans un environnement de production :

- Le modèle de chemin de chaque comportement de cache s'applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
- Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d'informations, consultez Modèle de chemin d'accès.
- Les comportements de cache acheminent les requêtes vers les origines correctes.

Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA

Lorsque vous utilisez des noms de domaine CloudFront alternatifs et le protocole HTTPS, la taille maximale de la clé publique d'un certificat SSL/TLS RSA est de 4 096 bits. (Il s'agit de la taille de la clé, et non pas du nombre de caractères figurant dans la clé publique.) Si vous utilisez AWS Certificate Manager pour vos certificats, bien qu'ACM prenne en charge les clés RSA de plus grande taille, vous ne pouvez pas utiliser les clés les plus grandes avec. CloudFront

Vous pouvez déterminer la taille de la clé publique RSA en exécutant la commande OpenSSL suivante :

```
openssl x509 -in path and filename of SSL/TLS certificate -text -noout
```

Où :

- `-in` indique le chemin et nom de fichier de votre certificat RSA SSL/TLS.
- `-text` permet à OpenSSL d'afficher la longueur de la clé publique RSA en bits.
- `-noout` empêche OpenSSL d'afficher la clé publique.

Exemple de sortie :

```
Public-Key: (2048 bit)
```

Augmenter les quotas pour les certificats SSL/TLS

Il existe des quotas sur le nombre de certificats SSL/TLS que vous pouvez importer dans AWS Certificate Manager (ACM) ou télécharger vers AWS Identity and Access Management (IAM). Il existe également un quota sur le nombre de certificats SSL/TLS que vous pouvez utiliser avec et Compte AWS lorsque vous configurez CloudFront pour répondre aux requêtes HTTPS à l'aide d'adresses IP dédiées. Cependant, vous pouvez demander des quotas plus élevés.

Rubriques

- Augmenter le quota de certificats importés dans ACM
- Augmenter le quota de certificats téléchargés vers IAM
- Augmenter le quota de certificats utilisés avec des adresses IP dédiées

Augmenter le quota de certificats importés dans ACM

Pour connaître le quota du nombre de certificats que vous pouvez importer dans ACM, consultez la page Quotas dans le Guide de l'utilisateur AWS Certificate Manager .

Pour demander un quota plus élevé, créez un dossier dans la console Centre de support . Indiquez l'une des valeurs suivantes :

- Acceptez la valeur par défaut de Service Limit Increase (Augmentation de la limite de service).
- Pour Limit type (Type de limite), choisissez Certificate Manager (Gestionnaire de certificats).

- Pour Région, choisissez la AWS région dans laquelle vous souhaitez importer les certificats.
- Pour Limit (Limite), choisissez Number of ACM certificates (Nombre de certificats ACM).

Remplissez ensuite le reste du formulaire et soumettez-le.

Augmenter le quota de certificats téléchargés vers IAM

Pour connaître le quota (auparavant appelé limite) lié au nombre de certificats que vous pouvez charger dans IAM, consultez Limites IAM et STS dans le Guide de l'utilisateur IAM.

Pour demander un quota plus élevé, créez un dossier dans la console Centre de support . Indiquez l'une des valeurs suivantes :

- Acceptez la valeur par défaut de Service Limit Increase (Augmentation de la limite de service).
- Pour Limit type (Type de limite), choisissez Certificate Manager (Gestionnaire de certificats).
- Pour Région, choisissez la AWS région dans laquelle vous souhaitez importer les certificats.
- Pour Limit (Limite), choisissez Server Certificate Limit (IAM) (Limite de certificats de serveur (IAM)).

Remplissez ensuite le reste du formulaire et soumettez-le.

Augmenter le quota de certificats utilisés avec des adresses IP dédiées

Pour connaître le quota du nombre de certificats SSL que vous pouvez utiliser pour chacun Compte AWS lorsque vous répondez à des requêtes HTTPS à l'aide d'adresses IP dédiées, consultezQuotas sur les certificats SSL.

Pour demander un quota plus élevé, créez un dossier dans la console Centre de support . Indiquez l'une des valeurs suivantes :

- Acceptez la valeur par défaut de Service Limit Increase (Augmentation de la limite de service).
- Pour Type de limite, sélectionnez CloudFrontDistributions.
- Pour Limit (Limite), choisissez Dedicated IP SSL Certificate Limit per Account (Limite de certificat SSL IP dédié par compte).

Remplissez ensuite le reste du formulaire et soumettez-le.

Rotation des certificats SSL/TLS

Si vous utilisez des certificats fournis par AWS Certificate Manager (ACM), il n'est pas nécessaire de faire alterner les certificats SSL/TLS. ACM gère automatiquement le renouvellement des certificats. Pour plus d'informations, consultez Renouvellement géré dans le Guide de l'utilisateur AWS Certificate Manager .

> **Note**
>
> ACM ne gère pas le renouvellement des certificats que vous obtenez auprès d'autorités de certification tierces et importez dans ACM.

Si vous utilisez une autorité de certification tierce et que vous avez importé des certificats dans ACM (recommandé) ou que vous en avez chargé dans le magasin de certificats IAM, vous devez parfois remplacer un certificat par un autre. Par exemple, vous devez remplacer un certificat lorsque sa date d'expiration approche.

> **Important**
>
> Si vous avez configuré CloudFront pour traiter les requêtes HTTPS à l'aide d'adresses IP dédiées, l'utilisation d'un ou de plusieurs certificats supplémentaires peut vous être facturée au prorata pendant la rotation des certificats. Nous vous recommandons de mettre rapidement à jour vos distributions pour réduire les frais supplémentaires.

Rotation des certificats SSL/TLS

Pour faire tourner des certificats, exécutez la procédure suivante. Les utilisateurs peuvent continuer d'accéder à votre contenu pendant la rotation des certificats, ainsi qu'une fois le processus terminé.

Pour faire tourner des certificats SSL/TLS

1. Augmenter les quotas pour les certificats SSL/TLS pour déterminer si vous avez besoin de l'autorisation d'utiliser Plus de certificats SSL. Si c'est le cas, demandez l'autorisation et attendez que celle-ci vous soit accordée avant de passer à l'étape 2.
2. Importez le nouveau certificat dans ACM ou chargez-le dans IAM. Pour plus d'informations, consultez Importation d'un certificat SSL/TLS dans le manuel Amazon CloudFront Developer Guide.

3. Mettez vos distributions à jour une à la fois pour utiliser le nouveau certificat. Pour plus d'informations, consultez la section Liste, affichage et mise à jour CloudFront des distributions dans le manuel Amazon CloudFront Developer Guide.
4. (Facultatif) Après avoir mis à jour toutes vos CloudFront distributions, vous pouvez supprimer l'ancien certificat d'ACM ou d'IAM.

> **Important**
>
> Ne supprimez pas un certificat SSL/TLS tant que vous ne l'avez pas retiré de toutes les distributions et que le statut des distributions mises à jour n'est pas devenu `Deployed`.

Revenir d'un certificat SSL/TLS personnalisé au certificat par défaut CloudFront

Si vous avez configuré CloudFront pour utiliser le protocole HTTPS entre les utilisateurs et CloudFront, et si vous avez configuré CloudFront pour utiliser un certificat SSL/TLS personnalisé, vous pouvez modifier votre configuration pour utiliser le certificat SSL/TLS par défaut CloudFront . Le processus varie selon que vous avez utilisé ou non votre distribution pour transmettre votre contenu :

- Si vous n'avez pas utilisé votre distribution pour transmettre votre contenu, vous pouvez juste modifier la configuration. Pour plus d'informations, consultez Mettre à jour une distribution.
- Si vous avez utilisé votre distribution pour distribuer votre contenu, vous devez créer une nouvelle CloudFront distribution et modifier les URL de vos fichiers afin de réduire ou d'éliminer la durée pendant laquelle votre contenu n'est pas disponible. Pour ce faire, procédez comme suit.

Revenir au certificat par défaut CloudFront

La procédure suivante explique comment passer d'un certificat SSL/TLS personnalisé au certificat par défaut. CloudFront

Pour revenir au certificat par défaut CloudFront

1. Créez une nouvelle CloudFront distribution avec la configuration souhaitée. Pour le certificat SSL, choisissez le CloudFrontcertificat par défaut (*.cloudfront.net).

   Pour plus d'informations, consultez Créer une distribution.

2. Pour les fichiers que vous distribuez CloudFront, mettez à jour les URL de votre application pour utiliser le nom de domaine CloudFront attribué à la nouvelle distribution. Remplacez, par exemple, `https://www.example.com/images/logo.png` par `https://d111111abcdef8.cloudfront.net/images/logo.png`.
3. Supprimez la distribution associée à un certificat SSL/TLS personnalisé ou mettez-la à jour pour remplacer la valeur du certificat SSL par CloudFront certificat par défaut (*.cloudfront.net). Pour plus d'informations, consultez Mettre à jour une distribution.

   > **Important**
   >
   > Jusqu'à ce que vous ayez terminé cette étape, l'utilisation d'un certificat SSL/TLS personnalisé AWS continue de vous être facturée.

4. (Facultatif) Supprimez votre certificat SSL/TLS personnalisé.

   a. Exécutez la AWS CLI commande `list-server-certificates` pour obtenir l'ID du certificat que vous souhaitez supprimer. Pour plus d'informations, consultez list-server-certificatesle manuel de référence des AWS CLI commandes.

   b. Exécutez la AWS CLI commande `delete-server-certificate` pour supprimer le certificat. Pour plus d'informations, consultez delete-server-certificatele manuel de référence des AWS CLI commandes.

Passez d'un certificat SSL/TLS personnalisé avec adresses IP dédiées à un certificat SNI

Si vous avez configuré CloudFront pour utiliser un certificat SSL/TLS personnalisé avec des adresses IP dédiées, vous pouvez passer à l'utilisation d'un certificat SSL/TLS personnalisé avec SNI et éliminer les frais associés aux adresses IP dédiées. Il suffit de procéder comme indiqué ci-dessous.

> **Important**
>
> Cette mise à jour de votre CloudFront configuration n'a aucun effet sur les utilisateurs qui prennent en charge le SNI. Les spectateurs peuvent accéder à votre contenu avant et après la modification, ainsi que pendant que la modification se propage aux zones CloudFront périphériques. les utilisateurs qui ne prennent pas en charge l'extension SNI ne peuvent plus

accéder à votre contenu après le changement. Pour plus d'informations, consultez Choisissez le mode de CloudFront traitement des requêtes HTTPS.

Passez du certificat personnalisé au SNI

La procédure suivante explique comment passer d'un certificat SSL/TLS personnalisé avec des adresses IP dédiées à un certificat SNI.

Pour passer d'un certificat SSL/TLS personnalisé avec adresses IP dédiées à l'extension SNI

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez afficher ou mettre à jour.
3. Choisissez Paramètres de distribution.
4. Sous l'onglet General, choisissez Edit.
5. Modifiez le paramètre de Prise en charge d'un client SSL personnalisé pour obtenir Seuls les clients qui prennent en charge Server Name Indication (SNI).
6. Choisissez Oui, Modifier.

Diffusez du contenu privé avec des URL signées et des cookies signés

De nombreuses entreprises qui distribuent du contenu via Internet veulent limiter l'accès aux documents, données professionnelles, flux multimédias ou contenus destinés à des utilisateurs sélectionnés, tels que ceux qui paient un droit. Pour diffuser en toute sécurité ce contenu privé en utilisant CloudFront, vous pouvez effectuer les opérations suivantes :

- Exigez que vos utilisateurs accèdent à votre contenu privé en utilisant des URL CloudFront signées spéciales ou des cookies signés.
- Exigez que vos utilisateurs accèdent à votre contenu en utilisant CloudFront des URL, et non des URL qui accèdent au contenu directement sur le serveur d'origine (par exemple, Amazon S3 ou un serveur HTTP privé). Il n'est pas nécessaire d'exiger des CloudFront URL, mais nous le recommandons pour empêcher les utilisateurs de contourner les restrictions que vous spécifiez dans les URL signées ou les cookies signés.

Pour plus d'informations, consultez Restreindre l'accès aux fichiers.

Comment diffuser du contenu privé

Pour configurer CloudFront afin de diffuser du contenu privé, effectuez les tâches suivantes :

1. (Facultatif mais recommandé) Demandez à vos utilisateurs d'accéder à votre contenu uniquement via CloudFront. La méthode que vos utilisez varie selon que vous recourez aux origines Amazon S3 ou aux origines personnalisées :

   - Amazon S3 : voir the section called "Restreindre l'accès à une origine Amazon Simple Storage Service".
   - Origine personnalisée : voir Restreindre l'accès aux fichiers dont l'origine est personnalisée.

   Les origines personnalisées incluent Amazon EC2, les compartiments Amazon S3 configurés en tant que points de terminaison de site Web, Elastic Load Balancing et vos propres serveurs web HTTP.
2. Spécifiez les groupes de clés approuvés ou les signataires approuvés que vous souhaitez utiliser pour créer des URL ou des cookies signés. Nous vous recommandons d'utiliser des groupes de clés approuvés. Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.
3. Écrivez votre application pour répondre aux demandes des utilisateurs authentifiés avec des URL signées ou avec des en-têtes `Set-Cookie` définissant des cookies signés. Suivez les étapes décrites dans l'une des rubriques suivantes :

   - Utiliser des URL signées
   - Utiliser des cookies signés

   En cas de doute sur la méthode à utiliser, consultez Décidez d'utiliser des URL signées ou des cookies signés.

Rubriques

- Restreindre l'accès aux fichiers
- Spécifiez les signataires autorisés à créer des URL signées et des cookies signés
- Décidez d'utiliser des URL signées ou des cookies signés

- Utiliser des URL signées
- Utiliser des cookies signés
- Commandes Linux et OpenSSL pour le codage et le chiffrement base64
- Exemples de code pour la création de la signature d'une URL signée

Restreindre l'accès aux fichiers

Vous pouvez contrôler l'accès des utilisateurs à votre contenu privé de deux façons :

- Limitez l'accès aux fichiers dans les CloudFront caches.
- Restreignez l'accès aux fichiers dans votre origine en effectuant l'une des actions suivantes :
  - Configurez un contrôle d'accès à l'origine (OAC) pour votre compartiment Amazon S3.
  - Configurez des en-têtes personnalisés pour un serveur HTTP privé (origine personnalisée).

Restreindre l'accès aux fichiers dans les CloudFront caches

Vous pouvez configurer CloudFront pour obliger les utilisateurs à accéder à vos fichiers à l'aide d'URL signées ou de cookies signés. Vous pouvez alors développer votre application pour créer et distribuer des URL signées aux utilisateurs authentifiées ou pour envoyer des en-têtes `Set-Cookie` qui définissent des cookies signés pour des utilisateurs authentifiés. (Pour fournir à quelques utilisateurs un accès à long terme à un petit nombre de fichiers, vous pouvez aussi créer des URL signées manuellement.)

Lorsque vous créez des URL signées ou des cookies signés pour contrôler l'accès à vos fichiers, vous pouvez spécifier les restrictions suivantes :

- Une heure et une date de fin, au-delà desquelles l'URL n'est plus valide.
- (Facultatif) L'heure et la date auxquelles l'URL devient valide.
- (Facultatif) L'adresse IP ou la plage d'adresses IP des ordinateurs qui peuvent être utilisés pour accéder à votre contenu.

Une partie d'une URL signée ou d'un cookie signé est hachée et signée à l'aide de la clé privée d'une paire de clés publique/privée. Lorsqu'un utilisateur utilise une URL signée ou un cookie signé pour accéder à un fichier, CloudFront compare les parties signées et non signées de l'URL ou du cookie. S'ils ne correspondent pas, CloudFront ne diffuse pas le fichier.

Vous devez utiliser RSA-SHA1 pour signer des URL ou des cookies. CloudFront n'accepte pas les autres algorithmes.

Restreindre l'accès aux fichiers dans les compartiments Amazon S3

Vous pouvez éventuellement sécuriser le contenu de votre compartiment Amazon S3 afin que les utilisateurs puissent y accéder via la CloudFront distribution spécifiée, mais ne puissent pas y accéder directement en utilisant les URL Amazon S3. Cela empêche quelqu'un de contourner CloudFront et d'utiliser l'URL Amazon S3 pour accéder au contenu auquel vous souhaitez restreindre l'accès. Cette étape n’est pas obligatoire pour utiliser les URL signées, mais nous la recommandons.

Pour obliger les utilisateurs à accéder à votre contenu via CloudFront des URL, vous devez effectuer les tâches suivantes :

- Donnez à une autorisation de contrôle CloudFront d'accès à l'origine l'autorisation de lire les fichiers du compartiment S3.
- Créez le contrôle d'accès à l'origine et associez-le à votre CloudFront distribution.
- Supprimez l’autorisation pour toute autre personne d’utiliser les URL Amazon S3 pour lire les fichiers.

Pour plus d’informations, consultez the section called “Restreindre l'accès à une origine Amazon Simple Storage Service”.

Restreindre l'accès aux fichiers dont l'origine est personnalisée

Si vous utilisez une origine personnalisée, vous pouvez éventuellement configurer des en-têtes personnalisés pour limiter l’accès. CloudFront Pour obtenir vos fichiers à partir d'une origine personnalisée, ceux-ci doivent être accessibles à l'CloudFront aide d'une requête HTTP (ou HTTPS) standard. Mais en utilisant des en-têtes personnalisés, vous pouvez restreindre davantage l'accès à votre contenu afin que les utilisateurs puissent y accéder uniquement par le biaisCloudFront, et non directement. Cette étape n’est pas obligatoire pour utiliser les URL signées, mais nous la recommandons.

Pour obliger les utilisateurs à accéder au contenu via CloudFront, modifiez les paramètres suivants dans vos CloudFront distributions :

Origin Custom Headers

Configurez CloudFront pour transférer les en-têtes personnalisés vers votre origine. veuillez consulter Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine.

Viewer Protocol Policy

Configurez votre distribution pour obliger les spectateurs à utiliser le protocole HTTPS pour y accéder CloudFront. veuillez consulter Viewer Protocol Policy.

Origin Protocol Policy

Configurez votre distribution CloudFront pour exiger l'utilisation du même protocole que les spectateurs pour transférer les demandes à l'origine. veuillez consulter Protocole (origines personnalisées uniquement).

Après avoir apporté ces modifications, mettez à jour votre application sur votre origine personnalisée pour n'accepter que les demandes qui incluent les en-têtes personnalisés que vous avez configurés CloudFront pour envoyer.

La combinaison de la Politique de protocole d'utilisateur et de la Politique de protocole d'origine garantit que les en-têtes personnalisés sont chiffrés en transit. Cependant, nous vous recommandons de procéder régulièrement comme suit pour faire pivoter les en-têtes personnalisés qui sont CloudFront renvoyés vers votre origine :

1. Mettez à jour votre CloudFront distribution pour commencer à transférer un nouvel en-tête vers votre origine personnalisée.
2. Mettez à jour votre application pour accepter le nouvel en-tête comme confirmation de l'origine de la demande CloudFront.
3. Lorsque les demandes n'incluent plus l'en-tête que vous remplacez, mettez à jour votre application pour qu'elle n'accepte plus l'ancien en-tête comme confirmation de l'origine de la demande CloudFront.

Spécifiez les signataires autorisés à créer des URL signées et des cookies signés

Rubriques

- Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS

- Créez des paires de clés pour vos signataires
- Reformater la clé privée (.NET et Java uniquement)
- Ajouter un signataire à une distribution
- Rotation de paires de clés

Pour créer des URL ou des cookies signés, vous avez besoin d'un signataire. Un signataire est soit un groupe de clés fiables dans lequel vous créez CloudFront, soit un AWS compte contenant une paire de CloudFront clés. Nous vous recommandons d'utiliser des groupes de clés approuvés avec des URL et des cookies signés. Pour plus d'informations, consultez Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS.

Le signataire a deux finalités :

- Dès que vous ajoutez le signataire à votre distribution, CloudFront les utilisateurs doivent désormais utiliser des URL signées ou des cookies signés pour accéder à vos fichiers.
- Lorsque vous créez des URL ou des cookies signés, vous utilisez la clé privée de la paire de clés du signataire pour signer une partie de l'URL ou du cookie. Lorsqu'un utilisateur demande un fichier restreint, CloudFront compare la signature contenue dans l'URL ou le cookie avec l'URL ou le cookie non signé, afin de vérifier qu'il n'a pas été falsifié. CloudFront vérifie également que l'URL ou le cookie est valide, ce qui signifie, par exemple, que la date et l'heure d'expiration ne sont pas dépassées.

Lorsque vous spécifiez un signataire, vous spécifiez également indirectement les fichiers qui requièrent des URL ou des cookies signés en ajoutant le signataire à un comportement de cache. Si votre distribution ne comporte qu'un seul comportement de cache, les utilisateurs doivent employer des URL ou des cookies signés pour accéder à un fichier de la distribution. Si vous créez plusieurs comportements de cache et que vous ajoutez des utilisateurs à certains comportements de cache et pas à d'autres, vous pouvez exiger que les utilisateurs emploient des URL ou des cookies signés pour accéder à certains fichiers, et non à d'autres.

Pour spécifier les signataires (les clés privées) autorisés à créer des URL signées ou des cookies signés, et pour ajouter les signataires à votre CloudFront distribution, effectuez les tâches suivantes :

1. Décidez si vous souhaitez utiliser un groupe de clés approuvé ou un Compte AWS en tant que signataire. Nous vous recommandons d'utiliser un groupe de clés approuvé. Pour plus d'informations, consultez Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS.

2. Pour le signataire que vous avez choisi à l'étape 1, créez une paire de clés privées/publiques. Pour plus d'informations, consultez Créez des paires de clés pour vos signataires.
3. Si vous utilisez .NET ou Java pour créer des URL signées ou des cookies signés, reformatez la clé privée. Pour plus d'informations, consultez Reformater la clé privée (.NET et Java uniquement).
4. Dans la distribution pour laquelle vous créez des URL ou des cookies signés, spécifiez le signataire. Pour plus d'informations, consultez Ajouter un signataire à une distribution.

Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS

Pour utiliser des URL ou des cookies signés, vous avez besoin d'un signataire. Un signataire est soit un groupe de clés fiables dans lequel vous créez CloudFront, soit un groupe Compte AWS contenant une paire de CloudFront clés. Nous vous recommandons d'utiliser des groupes de clés approuvés, pour les raisons suivantes :

- Avec les groupes de CloudFront clés, il n'est pas nécessaire d'utiliser l'utilisateur root du AWS compte pour gérer les clés publiques des URL CloudFront signées et des cookies signés. AWS les meilleures pratiques recommandent de ne pas utiliser l'utilisateur root lorsque ce n'est pas nécessaire.
- Avec les groupes de CloudFront clés, vous pouvez gérer les clés publiques, les groupes de clés et les signataires de confiance à l'aide de l' CloudFront API. Vous pouvez utiliser l'API pour automatiser la création et la rotation des clés. Lorsque vous utilisez l'utilisateur AWS root, vous devez utiliser le AWS Management Console pour gérer les paires de CloudFront clés. Vous ne pouvez donc pas automatiser le processus.
- Comme vous pouvez gérer des groupes de clés avec l' CloudFront API, vous pouvez également utiliser des politiques d'autorisation AWS Identity and Access Management (IAM) pour limiter ce que les différents utilisateurs sont autorisés à faire. Par exemple, vous pouvez autoriser les utilisateurs à télécharger des clés publiques, mais pas à les supprimer. Vous pouvez également autoriser les utilisateurs à supprimer des clés publiques, mais uniquement lorsque certaines conditions sont remplies, telles que l'utilisation d'une authentification à plusieurs facteurs, l'envoi de la demande à partir d'un réseau particulier ou dans une plage de dates et d'heures spécifiques.
- Avec les groupes de CloudFront clés, vous pouvez associer un plus grand nombre de clés publiques à votre CloudFront distribution, ce qui vous donne plus de flexibilité dans la manière dont vous utilisez et gérez les clés publiques. Par défaut, vous pouvez associer jusqu'à quatre groupes de clés avec une seule distribution, et vous pouvez avoir jusqu'à cinq clés publiques dans un groupe de clés.

Lorsque vous utilisez l'utilisateur root du AWS compte pour gérer les paires de CloudFront clés, vous ne pouvez avoir que deux paires de CloudFront clés actives par AWS compte.

Créez des paires de clés pour vos signataires

Chaque signataire que vous utilisez pour créer des URL CloudFront signées ou des cookies signés doit disposer d'une paire de clés publique-privée. Le signataire utilise sa clé privée pour signer l'URL ou les cookies, et CloudFront utilise la clé publique pour vérifier la signature.

La façon dont vous créez une paire de clés varie selon que vous utilisez un groupe de clés approuvé comme signataire (recommandé) ou une paire de CloudFront clés. Pour plus d'informations, consultez les sections suivantes. La paire de clés que vous créez doit satisfaire aux exigences suivantes :

- Il doit s'agir d'une paire de clés SSH-2 RSA.
- Elle doit être au format PEM codé en base64.
- Il doit s'agir d'une paire de clés 2048 bits.

Pour aider à sécuriser vos applications, nous vous recommandons d'effectuer une rotation périodique des paires de clés. Pour plus d'informations, consultez Rotation de paires de clés.

Création d'une paire de clés pour un groupe de clés approuvé (recommandé)

Pour créer une paire de clés pour un groupe de clés approuvé, effectuez les opérations suivantes :

1. Créez la paire de clés privées/publiques.
2. Téléchargez la clé publique sur CloudFront.
3. Ajoutez la clé publique à un groupe de CloudFront clés.

Pour plus d'informations, consultez les procédures suivantes.

Pour créer une paire de clés

> **Note**
>
> Les étapes suivantes utilisent OpenSSL comme exemple de création d'une paire de clés. Il existe de nombreuses autres façons de créer une paire de clés RSA.

1. L'exemple de commande suivant utilise OpenSSL pour générer une paire de clés RSA d'une longueur de 2048 bits et l'enregistrer dans le fichier nommé `private_key.pem`.

```
openssl genrsa -out private_key.pem 2048
```

2. Le fichier obtenu contient à la fois la clé publique et la clé privée. L'exemple de commande suivant extrait la clé publique du fichier nommé `private_key.pem`.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

   Vous chargez la clé publique (dans le fichier `public_key.pem`) ultérieurement, dans le cadre de la procédure suivante.

Pour télécharger la clé publique sur CloudFront

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le menu de navigation, choisissez Clés publiques.
3. Choisissez Créer une clé publique.
4. Dans la fenêtre Créer une clé publique, procédez comme suit :
   a. Dans Nom de la clé, saisissez un nom pour identifier la clé publique.
   b. Dans Valeur de clé, collez la clé publique. Si vous avez suivi les étapes de la procédure précédente, la clé publique se trouve dans le fichier nommé `public_key.pem`. Pour copier et coller le contenu de la clé publique, vous pouvez :
      - Utilisez la commande cat sur la ligne de commande macOS ou Linux, comme ceci :

```
cat public_key.pem
```

        Copiez la sortie de cette commande, puis collez-la dans le champ Valeur de clé.
      - Ouvrez le `public_key.pem` fichier à l'aide d'un éditeur de texte brut tel que le Bloc-notes (sous Windows) ou TextEdit (sous macOS). Copiez le contenu du fichier, puis collez-le dans le champ Valeur de clé.

c. (Facultatif) Dans Commentaire, ajoutez un commentaire pour décrire la clé publique.

Lorsque vous avez terminé, choisissez Ajouter.

5. Enregistrez l'ID de clé publique. Vous l'utiliserez ultérieurement lors de la création des URL ou des cookies signés, comme valeur du champ `Key-Pair-Id`.

Pour ajouter la clé publique à un groupe de clés

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le menu de navigation, choisissez Groupes de clés.
3. Choisissez Ajouter un groupe de clés.
4. Sur la page Créer un groupe de clés procédez comme suit :

   a. Dans Nom du groupe de clés, saisissez un nom pour identifier le groupe de clés.

   b. (Facultatif) Dans Commentaire, saisissez un commentaire pour décrire le groupe de clés.

   c. Dans Clés publiques, sélectionnez la clé publique à ajouter au groupe de clés, puis choisissez Ajouter. Répétez cette étape pour chaque clé publique que vous souhaitez ajouter au groupe de clés.

5. Choisissez Créer une paire de clés.
6. Enregistrez le nom du groupe de clés. Vous l'utiliserez ultérieurement pour associer le groupe de clés à un comportement de cache dans une CloudFront distribution. (Dans l' CloudFront API, vous utilisez l'ID du groupe de clés pour associer le groupe de clés à un comportement de cache.)

Création d'une paire de CloudFront clés (non recommandé, nécessite l'utilisateur Compte AWS root)

> **Important**
>
> Nous vous recommandons de créer une clé publique pour un groupe de clés approuvé au lieu de suivre ces étapes. Pour connaître la manière recommandée de créer des clés publiques pour les URL signées et les cookies signés, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).

Vous pouvez créer une paire de CloudFront clés de différentes manières :

- Créez une paire de clés dans le AWS Management Console et téléchargez la clé privée. Consultez la procédure suivante.
- Créez une paire de clés RSA à l'aide d'une application tel qu'OpenSSL, puis chargez la clé publique sur AWS Management Console. Pour plus d'informations sur la création d'une paire de clés, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).

Pour créer des paires de CloudFront clés dans le AWS Management Console

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de l'utilisateur root du AWS compte.

   > **Important**
   >
   > Les utilisateurs d'IAM ne peuvent pas créer de paires de CloudFront clés. Pour créer des paires de clés, vous devez vous connecter à l'aide des informations d'identification de l'utilisateur racine.

2. Choisissez le nom de votre compte, puis Mes informations d'identification de sécurité.
3. Choisissez CloudFront des paires de clés.
4. Confirmez que vous n'avez pas plus d'une paire de clés active. Vous ne pouvez pas créer une paire de clés si vous en avez déjà deux actives.
5. Choisissez Créer une nouvelle paire de clés.

   > **Note**
   >
   > Vous pouvez également choisir de créer votre propre paire de clés et de télécharger la clé publique. CloudFront les paires de clés prennent en charge les clés de 1024, 2048 ou 4096 bits.

6. Dans la boîte de dialogue Créer une paire de clés, choisissez Télécharger fichier de clés privées, puis enregistrez le fichier sur votre ordinateur.

   > **Important**
   >
   > Enregistrez la clé privée de votre paire de CloudFront clés dans un emplacement sécurisé et définissez des autorisations sur le fichier afin que seuls les administrateurs souhaités puissent le lire. Si quelqu'un obtient votre clé privée, il peut générer des

cookies signés et des URL signées valides, et télécharger votre contenu. Vous ne pouvez pas récupérer la clé privée. Par conséquent, si vous la perdez ou la supprimez, vous devez créer une nouvelle paire de CloudFront clés.

7. Enregistrez l'ID de paire de clés de votre paire de clés. (Dans le AWS Management Console, cela s'appelle l'ID de clé d'accès.) Vous l'utiliserez quand vous créerez des cookies ou des URL signés.

Reformater la clé privée (.NET et Java uniquement)

Si vous utilisez .NET ou Java pour créer des URL signées ou des cookies signés, vous ne pouvez pas utiliser la clé privée de votre paire de clés au format PEM par défaut pour créer la signature. Dans ce cas, procédez comme suit :

- .NET framework : convertit la clé privée au format XML utilisé par .NET framework. Plusieurs outils sont disponibles.
- Java : convertit la clé privée au format DER. On peut utiliser la commande OpenSSL suivante pour le faire. Dans la commande suivante, `private_key.pem` est le nom du fichier qui contient la clé privée au format PEM et `private_key.der` le nom du fichier qui contient la clé privée au format DER après l'exécution de la commande.

  ```
  openssl pkcs8 -topk8 -nocrypt -in private_key.pem -inform PEM -out private_key.der -
  outform DER
  ```

  Pour garantir que l'encodeur fonctionne correctement, ajoutez le fichier JAR des API de chiffrement Bouncy Castle Java à votre projet, puis ajoutez le fournisseur Bouncy Castle.

Ajouter un signataire à une distribution

Un signataire est le groupe de clés approuvé (recommandé) ou la paire de CloudFront clés qui peut créer des URL signées et des cookies signés pour une distribution. Pour utiliser des URL signées ou des cookies signés avec une CloudFront distribution, vous devez spécifier un signataire.

Les signataires sont associés aux comportements de cache. Cela vous permet de requérir des URL signées ou des cookies signés pour certains fichiers et pas pour d'autres dans la même distribution.

Une distribution nécessite des URL ou des cookies signés uniquement pour les fichiers associés aux comportements de cache correspondants.

De même, un signataire peut uniquement signer des URL ou des cookies pour les fichiers associés aux comportements de cache correspondants. Par exemple, si vous avez un signataire pour un comportement de cache et un autre pour un autre comportement de cache, ni l'un ni l'autre ne peuvent créer des URL ou des cookies signés pour les fichiers associés à l'autre comportement de cache.

Important

Avant d'ajouter un signataire à votre distribution, procédez comme suit :

- Définissez soigneusement les modèles de chemin d'accès dans les comportements de cache et la séquence des comportements de cache de façon à ne pas donner aux utilisateurs un accès non prévu à votre contenu ou à les empêcher d'accéder à un contenu que vous voulez disponible pour tout le monde.

  Par exemple, imaginons qu'une demande corresponde au modèle de chemin de deux comportements de cache. Le premier comportement de cache n'exige pas d'URL signées ou de cookies signés, à l'inverse du second comportement de cache. Les utilisateurs pourront accéder aux fichiers sans utiliser d'URL signées ni de cookies signés, car il CloudFront traite le comportement du cache associé à la première correspondance.

  Pour plus d'informations sur les modèles de chemin d'accès, consultez Modèle de chemin d'accès.
- Pour une distribution que vous utilisez déjà pour distribuer du contenu, assurez-vous d'être prêt à démarrer la génération d'URL et de cookies signés avant d'ajouter un signataire. Lorsque vous ajoutez un signataire, CloudFront rejette les demandes qui n'incluent pas d'URL signée ou de cookie signé valide.

Vous pouvez ajouter des signataires à votre distribution à l'aide de la CloudFront console ou de l' CloudFrontAPI.

Console

Les étapes suivantes montrent comment ajouter un groupe de clés approuvé en tant que signataire. Vous pouvez également ajouter un Compte AWS en tant que signataire de confiance, mais cela n'est pas recommandé.

Pour ajouter un signataire à une distribution à l'aide de la console

1. Enregistrez l'ID de groupe de clés du groupe de clés que vous souhaitez utiliser en tant que signataire approuvé. Pour plus d'informations, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).
2. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
3. Choisissez la distribution dont vous souhaitez protéger les fichiers avec des URL ou des cookies signés.

   > **Note**
   >
   > Pour ajouter un signataire à une nouvelle distribution, vous spécifiez les mêmes paramètres que ceux décrits à l'étape 6 lors de la création de la distribution.

4. Choisissez l'onglet Comportements.
5. Sélectionnez le comportement du cache dont le modèle de chemin d'accès correspond aux fichiers que vous souhaitez protéger avec des URL ou des cookies signés, puis choisissez Modifier.
6. Sur la page Modifier le comportement procédez comme suit :
   a. Pour Restrict Viewer Access (Use Signed URLs or Signed Cookies), cliquez sur Yes.
   b. Dans Groupes de clés approuvés ou Signataire approuvé, choisissez Groupes de clés approuvés.
   c. Dans Groupes de clés approuvés, choisissez le groupe de clés à ajouter, puis Ajouter. Recommencez si vous souhaitez ajouter plusieurs groupes de clés.
7. Choisissez Oui, Modifier pour mettre à jour le comportement du cache.

API

Vous pouvez utiliser l' CloudFront API pour ajouter un groupe de clés fiables en tant que signataire. Vous pouvez ajouter un signataire à une distribution existante ou à une nouvelle distribution. Dans les deux cas, spécifiez les valeurs dans l'élément `TrustedKeyGroups`.

Vous pouvez également ajouter un Compte AWS en tant que signataire de confiance, mais cela n'est pas recommandé.

Consultez les rubriques suivantes dans le manuel Amazon CloudFront API Reference :

- Mettre à jour une distribution existante — UpdateDistribution
- Créez une nouvelle distribution — CreateDistribution

Rotation de paires de clés

Nous vous recommandons d'effectuer une rotation (modifier) périodique de vos paires de clés pour les URL et les cookies signés. Pour effectuer une rotation des paires de clés que vous utilisez pour créer des URL ou des cookies signés sans invalider les URL ou cookies qui n'ont pas encore expiré, exécutez les tâches suivantes :

1. Créez une nouvelle paire de clés et ajoutez la clé publique à un groupe de clés. Pour plus d'informations, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).
2. Si vous avez créé un nouveau groupe de clés à l'étape précédente, ajoutez le groupe de clés à la distribution en tant que signataire.

   > **Important**
   >
   > Ne supprimez pas encore des clés publiques existantes du groupe de clés, ni les groupes de clés de la distribution. Ajoutez seulement les nouveaux.

3. Mettez à jour votre application pour créer des signatures à l'aide des clés privées à partir de la nouvelle paire de clés. Vérifiez que les URL ou les cookies signés avec les nouvelles clés privées fonctionnent.
4. Attendez jusqu'à ce que la date d'expiration soit passée dans les URL ou cookies signés à l'aide de la paire de clés précédente. Ensuite, supprimez l'ancienne clé publique du groupe de clés. Si

vous avez créé un nouveau groupe de clés à l'étape 2, supprimez l'ancien groupe de clés de votre distribution.

Décidez d'utiliser des URL signées ou des cookies signés

CloudFront Les URL signées et les cookies signés fournissent les mêmes fonctionnalités de base : ils vous permettent de contrôler qui peut accéder à votre contenu. Si vous souhaitez diffuser du contenu privé CloudFront et que vous essayez de décider d'utiliser des URL signées ou des cookies signés, considérez ce qui suit.

Utilisez les URL signées dans les cas suivants :

- Vous voulez restreindre l'accès aux fichiers individuels : par exemple, un téléchargement d'installation de votre application.
- Vos utilisateurs utilisent un client (par exemple, un client HTTP personnalisé) qui ne prend pas en charge les cookies.

Utilisez les cookies signés dans les cas suivants :

- Vous voulez fournir l'accès à plusieurs fichiers restreints : par exemple, tous les fichiers d'une vidéo au format HLS ou tous les fichiers de la section des abonnés d'un site web.
- Vous ne voulez pas modifier vos URL actuelles.

Si vous n'utilisez pas actuellement d'URL signées et si vos URL (non signées) contiennent l'un des paramètres de chaîne de requête suivants, vous ne pouvez pas utiliser d'URL signées ni de cookies signés :

- `Expires`
- `Policy`
- `Signature`
- `Key-Pair-Id`

CloudFront suppose que les URL contenant l'un de ces paramètres de chaîne de requête sont des URL signées et n'examineront donc pas les cookies signés.

Utilisez à la fois des URL signées et des cookies signés

Les URL signées ont priorité sur les cookies signés. Si vous utilisez à la fois des URL signées et des cookies signés pour contrôler l'accès aux mêmes fichiers et qu'un utilisateur utilise une URL signée pour demander un fichier, CloudFront détermine s'il convient de renvoyer le fichier au lecteur en se basant uniquement sur l'URL signée.

Utiliser des URL signées

Une URL signée inclut des informations supplémentaires, par exemple une heure et date d'expiration, qui vous donnent un meilleur contrôle de l'accès à votre contenu. Ces informations supplémentaires apparaissent dans une déclaration de politique, basée sur une politique prédéfinie ou une politique personnalisée. Les différences entre les politiques prédéfinies et les politiques personnalisées sont expliquées dans les deux prochaines sections.

> **Note**
>
> Vous pouvez créer certaines URL signées à l'aide de politiques prédéfinies et d'autres à l'aide de politiques personnalisées pour la même distribution.

Rubriques

Décidez d'utiliser des politiques prédéfinies ou personnalisées pour les URL signées

Lorsque vous créez une URL signée, vous écrivez une instruction de politique au format JSON qui spécifie les restrictions sur l'URL signée : par exemple, la durée de validité de l'URL. Vous pouvez utiliser une politique prédéfinie ou une politique personnalisée. Comparaison des politiques prédéfinies et des politiques personnalisées :

Description	Politique prédéfinie	Politique personnalisée
Vous pouvez réutiliser la déclaration de politique pour plusieurs fichiers. Pour ce faire, vous devez utiliser les caractères génériques de l'objet `Resource`. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée.)	Non	Oui
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs peuvent commencer à accéder à votre contenu.	Non	Oui (facultatif)
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs ne peuvent plus accéder à votre contenu.	Oui	Oui
Vous pouvez spécifier l'adresse IP ou la plage d'adresses IP des utilisateurs qui peuvent accéder à votre contenu.	Non	Oui (facultatif)
L'URL signée inclut une version encodée base 64 de la politique, ce qui se traduit par une URL plus longue.	Non	Oui

Pour plus d'informations sur la création d'URL signées à l'aide d'une politique prédéfinie, consultez Création d'une URL signée à l'aide d'une politique prédéfinie.

Pour plus d'informations sur la création d'URL signées à l'aide d'une politique personnalisée, consultez Création d'une URL signée à l'aide d'une politique personnalisée.

Fonctionnement des URL signées

Voici un aperçu de la façon dont vous configurez CloudFront et Amazon S3 pour les URL signées et de la façon dont un utilisateur CloudFront répond lorsqu'un utilisateur utilise une URL signée pour demander un fichier.

1. Dans votre CloudFront distribution, spécifiez un ou plusieurs groupes de clés fiables, qui contiennent les clés publiques CloudFront pouvant être utilisées pour vérifier la signature de l'URL. Vous utilisez les clés privées correspondantes pour signer les URL.

   Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.
2. Développez votre application pour déterminer si un utilisateur doit avoir accès à votre contenu et pour créer des URL signées pour les fichiers ou parties de votre application auxquels vous voulez limiter l'accès. Pour plus d'informations, consultez les rubriques suivantes :

   - Création d'une URL signée à l'aide d'une politique prédéfinie
   - Création d'une URL signée à l'aide d'une politique personnalisée
3. Un utilisateur demande un fichier pour lequel vous voulez requérir des URL signées.
4. Votre application vérifie que l'utilisateur est autorisé à accéder au fichier : il est abonné, il a payé pour accéder au contenu ou il a satisfait à quelque autre condition pour accéder.
5. Votre application crée et renvoie une URL signée à l'utilisateur.
6. L'URL signée autorise l'utilisateur à télécharger ou diffuser le contenu.

   Cette étape est automatique ; l'utilisateur n'a généralement rien à faire de plus pour accéder au contenu. Pa exemple, si un utilisateur accède à votre contenu dans un navigateur web, votre application renvoie l'URL signée au navigateur. Le navigateur utilise immédiatement l'URL signée pour accéder au fichier dans le cache CloudFront périphérique sans aucune intervention de l'utilisateur.
7. CloudFront utilise la clé publique pour valider la signature et confirmer que l'URL n'a pas été falsifiée. Si la signature n'est pas valide, la demande est rejetée.

   Si la signature est valide, CloudFront examine la déclaration de politique contenue dans l'URL (ou en crée une si vous utilisez une politique prédéfinie) pour confirmer que la demande est toujours valide. Par exemple, si vous avez spécifié une date et une heure de début et de fin pour l'URL, cela CloudFront confirme que l'utilisateur essaie d'accéder à votre contenu pendant la période pendant laquelle vous souhaitez autoriser l'accès.

   Si la demande répond aux exigences de la déclaration de politique, CloudFront effectue les opérations standard : détermine si le fichier se trouve déjà dans le cache périphérique, transmet la demande à l'origine si nécessaire et renvoie le fichier à l'utilisateur.

> **Note**
>
> Si une URL non signée contient des paramètres de chaîne de requête, assurez-vous de les inclure dans la partie de l'URL que vous signez. Si vous ajoutez une chaîne de requête à une URL signée après l'avoir signée, l'URL renvoie un code d'état HTTP 403.

Décidez de la durée de validité des URL signées

Vous pouvez distribuer le contenu privé à l'aide d'une URL signée qui est valide pendant une brève durée, de quelques minutes au plus. Les URL signées qui sont valides pour une période aussi courte sont utiles pour distribuer du contenu on-the-fly à un utilisateur dans un but précis, comme la location de films ou le téléchargement de musique aux clients à la demande. Si vos URL signées sont valides pour une brève période, vous voudrez probablement les générer automatiquement à l'aide d'une application que vous développez. Lorsque l'utilisateur commence à télécharger un fichier ou à lire un fichier multimédia, CloudFront compare le délai d'expiration indiqué dans l'URL avec l'heure actuelle pour déterminer si l'URL est toujours valide.

Vous pouvez aussi distribuer le contenu privé à l'aide d'une URL signée qui est valide pour une durée plus longue, quelques années peut-être. Les URL signées qui sont valides pendant une période plus longue sont utiles pour distribuer un contenu privé aux utilisateurs connus, comme la distribution d'un business plan aux investisseurs ou de documents de formation aux employés. Vous pouvez développer une application pour générer ces URL signées à plus long terme pour vous.

Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée

CloudFront vérifie la date et l'heure d'expiration d'une URL signée au moment de la requête HTTP. Si un client commence à télécharger un fichier volumineux immédiatement avant la date d'expiration, le téléchargement se termine même si la date d'expiration intervient pendant le téléchargement. Si la connexion TCP cesse et que le client essaie de redémarrer le téléchargement une fois la date d'expiration passée, le téléchargement échoue.

Si un client utilise des intervalles GET pour obtenir un fichier en parties plus petites, toute requête GET qui intervient après la date d'expiration échoue. Pour plus d'informations sur Range GET, consultez Comment CloudFront traite les demandes partielles pour un objet (plage GETS).

Exemple de code et outils tiers

Pour obtenir un exemple de code qui crée la partie hachée et signée des URL signées, consultez les rubriques suivantes :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Création d'une URL signée à l'aide d'une politique prédéfinie

Pour créer une URL signée à l'aide d'une politique prédéfinie, procédez comme suit.

Pour créer une URL signée à l'aide d'une politique prédéfinie

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformater la clé privée (.NET et Java uniquement).
2. Concaténez les valeurs suivantes dans l'ordre indiqué, en reproduisant le format indiqué dans cet exemple d'URL signée :

   ```
   https://d111111abcdef8.cloudfront.net/
   image.jpg?color=red&size=medium&Expires=1357034400&Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5Ew
   j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
   TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
   Pair-Id=K2JCJMDEHXQW5F
   ```

   Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne). Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application. Toutes les valeurs ont un type de`String`.

   1. ***URL de base du fichier***

      L'URL de base est l' CloudFront URL que vous utiliseriez pour accéder au fichier si vous n'utilisiez pas d'URL signées, y compris vos propres paramètres de chaîne de requête, le cas échéant. Dans l'exemple précédent, l'URL de base est`https://`

`d111111abcdef8.cloudfront.net/image.jpg`. Pour plus d'informations sur le format des URL pour les distributions, consultez Personnalisez le format d'URL pour les fichiers dans CloudFront.

- L' CloudFront URL suivante concerne un fichier image dans une distribution (en utilisant le nom de CloudFront domaine). Notez que `image.jpg` se trouve dans un répertoire `images`. Le chemin d'accès au fichier de l'URL doit correspondre à celui du fichier de votre serveur HTTP ou de votre compartiment Amazon S3.

  ```
  https://d111111abcdef8.cloudfront.net/images/image.jpg
  ```

- L' CloudFront URL suivante inclut une chaîne de requête :

  ```
  https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
  ```

- Les CloudFront URL suivantes concernent les fichiers image d'une distribution. Les deux utilisent un autre nom de domaine. La seconde inclut une chaîne de requête :

  ```
  https://www.example.com/images/image.jpg
  ```

  ```
  https://www.example.com/images/image.jpg?color=red
  ```

- L' CloudFront URL suivante concerne un fichier image d'une distribution qui utilise un autre nom de domaine et le protocole HTTPS :

  ```
  https://www.example.com/images/image.jpg
  ```

2. **?**

   ?Cela indique que les paramètres de la chaîne de requête suivent l'URL de base. Incluez le ? même si vous n'avez pas vos propres paramètres de chaîne de requête.

3. ***Les paramètres de votre chaîne de requête, le cas échéant*** **&**

   Ce champ est facultatif. Si vous voulez ajouter vos propres paramètres de chaîne de requête, par exemple :

   ```
   color=red&size=medium
   ```

   puis ajoutez les paramètres après ? et avant le `Expires` paramètre. Dans certaines circonstances exceptionnelles, il se peut que vous ayez besoin de placer vos paramètres de chaîne de requête après `Key-Pair-Id`.

> **Important**
>
> Vos paramètres ne peuvent pas se nommer `Expires`, `Signature` ou `Key-Pair-Id`.

Si vous ajoutez vos propres paramètres, ajoutez-en un & après chacun d'eux, y compris le dernier.

4. **`Expires=`*`date et heure au format Unix (en secondes) et temps universel coordonné (UTC)`***

   Date et heure auxquelles vous souhaitez que l'URL cesse d'autoriser l'accès au fichier.

   Spécifiez la date et l'heure d'expiration au format horaire Unix (en secondes) et en heure UTC. Par exemple, le 1er janvier 2013 à 10 h UTC est converti `1357034400` au format horaire Unix, comme indiqué dans l'exemple au début de cette rubrique. Pour utiliser l'heure de l'époque, utilisez un entier de 32 bits pour une date qui n'est pas postérieure à 2147483647 (19 janvier 2038 à 03:14:07 UTC). Pour plus d'informations sur l'UTC, consultez la RFC 3339, Date et heure sur Internet : horodatages.

5. **`&Signature=`*`version hachée et signée de la déclaration de politique`***

   Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour une URL signée qui utilise une politique prédéfinie.

6. **`&Key-Pair-Id=`*`ID de clé publique pour la clé CloudFront publique dont vous utilisez la clé privée correspondante pour générer la signature`***

   L'ID d'une clé CloudFront publique, par exemple,`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront la clé publique à utiliser pour valider l'URL signée. CloudFront compare les informations de la signature avec celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

   Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.

Création d'une signature pour une URL signée qui utilise une politique prédéfinie

Pour créer la signature d'une URL signée qui utilise une politique prédéfinie, procédez comme suit.

Rubriques

Création d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie

Lorsque vous créez une URL signée avec une politique prédéfinie, le paramètre `Signature` est une version hachée et signée d'une déclaration de politique. Pour les URL signées qui utilisent une politique prédéfinie, vous n'incluez pas la déclaration de politique dans l'URL, comme vous le faites pour les URL signées qui utilisent une politique personnalisée. Pour créer la déclaration de politique, effectuez la procédure suivante.

Pour créer la déclaration de politique d'une URL signée qui utilise une politique prédéfinie

1. Construisez la déclaration de politique à l'aide du format JSON suivant et de l'encodage de caractères UTF-8. Incluez la ponctuation et les autres valeurs littérales exactement comme spécifié. Pour plus d'informations sur les paramètres `Resource` et `DateLessThan`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique prédéfinie.

```
{
    "Statement": [
        {
            "Resource": "base URL or stream name",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": ending date and time in Unix time format and
 UTC
                }
            }
        }
    ]
}
```

2. Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.

Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique prédéfinie

Lorsque vous créez une déclaration de politique pour une politique prédéfinie, vous spécifiez les valeurs suivantes.

Ressource

> **Note**
>
> Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

L'URL de base, y compris vos chaînes de requête, le cas échéant, mais à l' CloudFront `Expires`exclusion des `Key-Pair-Id` paramètres`Signature`, et, par exemple :

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

Notez ce qui suit :

- Protocole : la valeur doit commencer par `http://` ou `https://`.
- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour l'objet.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. Par exemple, la date 1er janvier 2013 10 h 00 UTC est convertie en 1357034400 au format horaire Unix.

Cette valeur doit correspondre à la valeur du paramètre de la chaîne de requête `Expires` de l'URL signée. N'entourez pas la valeur de points d'interrogation.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée.

Exemple d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie

Lorsque vous utilisez l'exemple de déclaration de politique suivant dans une URL signée, un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/horizon.jpg` jusqu'au 1er janvier 2013 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1357034400
                }
            }
        }
    ]
}
```

Création d'une signature pour une URL signée qui utilise une politique prédéfinie

Pour créer la valeur du paramètre `Signature` d'une URL signée, vous hachez et signez la déclaration de politique que vous avez créée dans Création d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Commandes Linux et OpenSSL pour le codage et le chiffrement base64
- Exemples de code pour la création de la signature d'une URL signée

Option 1 : Créer une signature à l'aide d'une politique prédéfinie

1. Utilisez la fonction de hachage SHA-1 et RSA pour hacher et signer la déclaration de politique que vous avez créée dans la procédure Pour créer la déclaration de politique d'une URL signée

qui utilise une politique prédéfinie. Utilisez la version de la déclaration de politique qui ne contient plus d'espaces vides.

Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

> **Note**
>
> La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la chaîne hachée et signée.
3. Encodez en base64 la chaîne à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `&Signature=`, et retournez à Pour créer une URL signée à l'aide d'une politique prédéfinie pour terminer la concaténation des parties de votre URL signée.

Création d'une URL signée à l'aide d'une politique personnalisée

Pour créer une URL signée à l'aide d'une politique personnalisée, procédez comme suit.

Pour créer une URL signée utilisant une politique personnalisée

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformater la clé privée (.NET et Java uniquement).
2. Concaténez les valeurs suivantes dans l'ordre indiqué, en reproduisant le format indiqué dans cet exemple d'URL signée :

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Policy=eyANCiAgICEXAMPLEW1lbnQiOiBbeyANCiAgICAgICJSZXNvdXJj
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

   Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne). Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application. Toutes les valeurs ont un type de`String`.

   1. ***URL de base du fichier***

      L'URL de base est l' CloudFront URL que vous utiliseriez pour accéder au fichier si vous n'utilisiez pas d'URL signées, y compris vos propres paramètres de chaîne de requête, le cas échéant. Dans l'exemple précédent, l'URL de base est`https://d111111abcdef8.cloudfront.net/image.jpg`. Pour plus d'informations sur le format des URL pour les distributions, consultez Personnalisez le format d'URL pour les fichiers dans CloudFront.

      Les exemples suivants affichent les valeurs que vous spécifiez pour les distributions.

      - L' CloudFront URL suivante concerne un fichier image dans une distribution (en utilisant le nom de CloudFront domaine). Notez que `image.jpg` se trouve dans un répertoire `images`. Le chemin d'accès au fichier de l'URL doit correspondre à celui du fichier de votre serveur HTTP ou de votre compartiment Amazon S3.

        ```
        https://d111111abcdef8.cloudfront.net/images/image.jpg
        ```

      - L' CloudFront URL suivante inclut une chaîne de requête :

        ```
        https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
        ```

- Les CloudFront URL suivantes concernent les fichiers image d'une distribution. Les deux utilisent un nom de domaine alternatif ; le second inclut une chaîne de requête :

  ```
  https://www.example.com/images/image.jpg
  ```

  ```
  https://www.example.com/images/image.jpg?color=red
  ```

- L' CloudFront URL suivante concerne un fichier image d'une distribution qui utilise un autre nom de domaine et le protocole HTTPS :

  ```
  https://www.example.com/images/image.jpg
  ```

2. **?**

   ?Cela indique que les paramètres de la chaîne de requête suivent l'URL de base. Incluez le ? même si vous n'avez pas vos propres paramètres de chaîne de requête.

3. ***Les paramètres de votre chaîne de requête, le cas échéant*** **&**

   Ce champ est facultatif. Si vous voulez ajouter vos propres paramètres de chaîne de requête, par exemple :

   ```
   color=red&size=medium
   ```

   puis ajoutez-les après `?` et avant le `Policy` paramètre. Dans certaines circonstances exceptionnelles, il se peut que vous ayez besoin de placer vos paramètres de chaîne de requête après `Key-Pair-Id`.

   > **Important**
   >
   > Vos paramètres ne peuvent pas se nommer `Policy`, `Signature` ou `Key-Pair-Id`.

   Si vous ajoutez vos propres paramètres, ajoutez-en un & après chacun d'eux, y compris le dernier.

4. **Policy=*version codée en base64 de la déclaration de politique***

   Votre déclaration de politique au format JSON, avec les espaces vides supprimés, puis encodée en base64. Pour plus d'informations, consultez Création d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée.

La déclaration de politique contrôle l'accès accordé par une URL signée à un utilisateur. Elle inclut l'URL du fichier, une date et une heure d'expiration, une date et une heure (facultatif) auxquelles l'URL devient valide et une adresse IP (facultatif) ou une plage d'adresses IP autorisées à accéder au fichier.

5. **&Signature=*version hachée et signée de la déclaration de politique***

   Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour une URL signée qui utilise une politique personnalisée.

6. **&Key-Pair-Id=*ID de clé publique pour la clé CloudFront publique dont vous utilisez la clé privée correspondante pour générer la signature***

   L'ID d'une clé CloudFront publique, par exemple,`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront la clé publique à utiliser pour valider l'URL signée. CloudFront compare les informations de la signature avec celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

   Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.

Création d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée

Effectuez la procédure suivante pour créer une déclaration de politique pour une URL signée qui utilise une politique personnalisée.

Pour obtenir des exemples de déclaration de politique qui contrôlent l'accès aux fichiers de différentes façons, consultez the section called "Exemple d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée".

Pour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée

1. Construisez la déclaration de politique à l'aide du format JSON suivant. Remplacez les symboles inférieur à (<) et supérieur à (>), ainsi que les descriptions qu'ils contiennent, par vos propres valeurs. Pour plus d'informations, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

   ```
   {
   ```

```
   "Statement": [
       {
           "Resource": "<Optional but recommended: URL of the file>",
           "Condition": {
               "DateLessThan": {
                "AWS:EpochTime": <Required: ending date and time in Unix time
 format and UTC>
               },
               "DateGreaterThan": {
                "AWS:EpochTime": <Optional: beginning date and time in Unix time
 format and UTC>
               },
               "IpAddress": {
                "AWS:SourceIp": "<Optional: IP address>"
               }
           }
       }
   ]
}
```

Notez ce qui suit :

- Vous pouvez inclure une seule déclaration dans cette politique.
- Utilisez l'encodage de caractères UTF-8.
- Incluez la ponctuation et les noms de paramètre exactement comme spécifié. Les abréviations ne sont pas acceptées pour les noms de paramètre.
- L'ordre des paramètres de la section `Condition` n'importe pas.
- Pour plus d'informations sur les valeurs de `Resource`, `DateLessThan`, `DateGreaterThan` et `IpAddress`, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

2. Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.
3. Encodez en base64 la déclaration de politique à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `Policy=`.
6. Créez une signature pour l'URL signée en hachant, signant et encodant en base64 la déclaration de politique. Pour plus d'informations, consultez the section called "Création d'une signature pour une URL signée qui utilise une politique personnalisée".

Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée

Lorsque vous créez une déclaration de politique pour une politique personnalisée, vous spécifiez les valeurs suivantes.

Ressource

L'URL, y compris les chaînes de requête, à l'exception des `Key-Pair-Id` paramètres CloudFront `PolicySignature`, et. Par exemple :

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg\?
size=large&license=yes
```

Vous ne pouvez spécifier qu'une seule valeur d'URL pour `Resource`.

> **Important**
>
> Vous pouvez omettre le paramètre `Resource` dans une politique, mais cela signifie que toute personne disposant de l'URL signée peut accéder à tous les fichiers de toute distribution associée à cette paire de clés que vous utilisez pour créer l'URL signée.

Notez ce qui suit :

- Protocole : la valeur doit commencer par `http://`, `https://` ou `*://`.

- Paramètres de chaîne de requête : si l'URL comporte des paramètres de chaîne de requête, utilisez une barre oblique inverse (\) pour échapper le point d'interrogation (?) qui commence la chaîne de requête. Par exemple :

  ```
  https://d111111abcdef8.cloudfront.net/images/horizon.jpg\?
  size=large&license=yes
  ```

- Caractères génériques : vous pouvez utiliser des caractères génériques dans l'URL de la politique. Les caractères génériques suivants sont pris en charge :
  - astérisque (*), qui correspond à zéro, un ou plusieurs caractères
  - point d'interrogation (?), qui correspond à un et un seul caractère

  Lorsque l'URL de la politique CloudFront correspond à celle de la requête HTTP, l'URL de la politique est divisée en quatre sections (protocole, domaine, chemin et chaîne de requête) comme suit :

  ```
  [protocol]://[domain]/[path]\?[query string]
  ```

  Lorsque vous utilisez un caractère générique dans l'URL de la politique, la correspondance avec le caractère générique s'applique uniquement dans les limites de la section qui contient ce caractère générique. Par exemple, envisagez l'URL suivante dans une politique :

  ```
  https://www.example.com/hello*world
  ```

  Dans cet exemple, le caractère générique astérisque (*) s'applique uniquement dans la section du chemin. Il correspond donc aux URL `https://www.example.com/helloworld` et `https://www.example.com/hello-world`, mais il ne correspond pas à l'URL `https://www.example.net/hello?world`.

  Les exceptions suivantes s'appliquent aux limites des sections pour la mise en correspondance des caractères génériques :

  - La présence d'un astérisque à la fin de la section de chemin implique un astérisque dans la section de la chaîne de requête. Par exemple, `http://example.com/hello*` équivaut à `http://example.com/hello*\?*`.
  - La présence d'un astérisque à la fin de la section de domaine implique un astérisque dans les sections de chemin et de chaîne de requête. Par exemple, `http://example.com*` équivaut à `http://example.com*/*\?*`.

- Une URL figurant dans la politique peut omettre la section de protocole et commencer par un astérisque dans la section de domaine. Dans ce cas, la section de protocole est implicitement définie sur un astérisque. Par exemple, l'URL `*example.com` d'une politique est équivalente à `*://*example.com/`.
- Un astérisque à lui seul (`"Resource": "*"`) correspond à n'importe quelle URL.

Par exemple, la valeur `https://d111111abcdef8.cloudfront.net/*game_download.zip*` dans une politique correspond à toutes les URL suivantes :

- `https://d111111abcdef8.cloudfront.net/game_download.zip`
- `https://d111111abcdef8.cloudfront.net/example_game_download.zip?license=yes`
- `https://d111111abcdef8.cloudfront.net/test_game_download.zip?license=temp`

- Autres noms de domaine : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL de la politique, la requête HTTP doit utiliser ce nom de domaine alternatif dans votre page ou application Web. Ne spécifiez pas l'URL Amazon S3 pour le fichier dans une politique.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. Dans la politique, n'entourez pas la valeur avec des points d'interrogation. Pour obtenir des informations sur UTC, consultez Date et heure sur Internet : Horodatages.

Par exemple, l'horodatage 31 janvier 2023 10 h 00 UTC est converti en 1675159200 au format horaire Unix.

Il s'agit du seul paramètre obligatoire dans `Condition` cette section. CloudFront nécessite cette valeur pour empêcher les utilisateurs d'avoir un accès permanent à votre contenu privé.

Pour plus d'informations, consultez the section called "Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée".

DateGreaterThan (Facultatif)

(Facultatif) Date et heure de début de l'URL au format horaire Unix (en secondes) et en heure UTC. Les utilisateurs ne sont pas autorisés à accéder au fichier à la date et à l'heure spécifiées ou avant. N'entourez pas la valeur de points d'interrogation.

IpAddress (Facultatif)

Adresse IP du client formulant la requête HTTP. Notez ce qui suit :

- Pour autoriser une adresse IP à accéder au fichier, omettez le paramètre `IpAddress`.
- Vous pouvez spécifier une adresse IP ou une plage d'adresses IP. Vous ne pouvez pas utiliser cette politique pour autoriser l'accès si l'adresse IP du client figure dans l'une des deux plages distinctes.
- Pour autoriser l'accès depuis une seule adresse IP, vous spécifiez :

  `"`*`Adresse IP IPv4`*`/32"`
- Vous devez spécifier les plages d'adresses IP selon le format IPv4 CIDR standard (par exemple, `192.0.2.0/24`). Pour plus d'informations, consultez Routage inter-domaines sans classe (CIDR) : plan d'agrégation et d'affectation d'adresses Internet.

  > **Important**
  >
  > Les adresses IP au format IPv6, telles que 2001:0db8:85a3::8a2e:0370:7334, ne sont pas prises en charge.

  Si vous utilisez une politique personnalisée qui inclut `IpAddress`, n'activez pas IPv6 pour la distribution. Si vous souhaitez limiter l'accès à un contenu spécifique par adresse IP et prendre en charge les requêtes IPv6 pour les autres contenus, vous pouvez créer deux distributions. Pour plus d'informations, consultez the section called "Activation d'IPv6" dans la rubrique the section called "Paramètres de distribution".

Exemple d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée

Les exemples suivants de déclaration de politique montrent comment accéder à un fichier spécifique, à tous les objets d'un répertoire ou à tous les fichiers associés à un ID de paire de clés. Les exemples montrent aussi comment contrôler l'accès depuis une adresse IP individuelle ou une plage d'adresses IP, et comment empêcher les utilisateurs d'employer l'URL signée au-delà d'une date et heure spécifiées.

Si vous copiez et collez l'un de ces exemples, supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne), remplacez les valeurs par vos propres valeurs et insérez un caractère de nouvelle ligne après l'accolade fermante (). }

Pour plus d'informations, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

Rubriques

Exemple de déclaration de politique : accéder à un fichier à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée dans une URL signée spécifie qu'un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/game_download.zip` à partir des adresses IP de la plage `192.0.2.0/24` jusqu'au 31 janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée vous permet de créer des URL signées pour n'importe quel fichier du répertoire `training`, comme l'indique le caractère générique astérisque (`*`) du paramètre `Resource`. Les utilisateurs peuvent accéder au fichier depuis une adresse IP de la plage `192.0.2.0/24` jusqu'au 31 janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
```

```
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Chaque URL signée avec laquelle vous utilisez cette politique inclut une URL qui identifie un fichier spécifique ; par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Exemple de déclaration de politique : accédez à tous les fichiers associés à un identifiant de paire de clés à partir d'une adresse IP

L'exemple suivant de politique personnalisée vous permet de créer des URL signées pour tout fichier associé à une distribution quelconque, comme l'indique le caractère générique astérisque (*) du paramètre `Resource`. L'URL signée doit utiliser le protocole `https://`, et non `http://`. L'utilisateur doit employer l'adresse IP `192.0.2.10/32`. (La valeur `192.0.2.10/32` en notation CIDR fait référence à une seule adresse IP, `192.0.2.10`.) Les fichiers ne sont disponibles qu'entre le 31 janvier 2023 10 h 00 UTC et le 2 février 2023 10 h 00 UTC :

```
{
    "Statement": [
       {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1675159200
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675332000
                }
```

```
            }
        }
    ]
}
```

Chaque URL signée avec laquelle vous utilisez cette politique possède une URL qui identifie un fichier spécifique dans une CloudFront distribution spécifique, par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

L'URL signée inclut aussi un ID de paire de clés, qui doit être associé à un groupe de clés autorisé dans la distribution (d111111abcdef8.cloudfront.net) que vous spécifiez dans l'URL.

Création d'une signature pour une URL signée qui utilise une politique personnalisée

La signature d'une URL signée utilisant une politique personnalisée est une version hachée, signée et encodée en base64 de la déclaration de politique. Pour créer une signature pour une politique personnalisée, procédez comme suit.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Commandes Linux et OpenSSL pour le codage et le chiffrement base64
- Exemples de code pour la création de la signature d'une URL signée

Option 1 : Créer une signature à l'aide d'une politique personnalisée

1. Utilisez la fonction de hachage SHA-1 et RSA pour hacher et signer la déclaration de politique JSON que vous avez créée dans la procédure Pour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée. Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides mais qui n'a pas encore été codée en base64.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

   > **Note**
   >
   > La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la chaîne hachée et signée.
3. Encodez en base64 la chaîne à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `&Signature=`, et retournez à Pour créer une URL signée utilisant une politique personnalisée pour terminer la concaténation des parties de votre URL signée.

Utiliser des cookies signés

CloudFront les cookies signés vous permettent de contrôler qui peut accéder à votre contenu lorsque vous ne souhaitez pas modifier vos URL actuelles ou lorsque vous souhaitez donner accès à plusieurs fichiers restreints, par exemple tous les fichiers de la zone réservée aux abonnés d'un site Web. Cette rubrique explique l'utilisation des cookies signés et décrit comment les définir à l'aide de politiques prédéfinies et personnalisées.

Rubriques

- Décidez d'utiliser des politiques prédéfinies ou personnalisées pour les cookies signés
- Fonctionnement des cookies signés
- Empêcher l'utilisation abusive des cookies signés
- Quand CloudFront vérifie la date et l'heure d'expiration dans un cookie signé
- Exemple de code et outils tiers
- Définissez des cookies signés à l'aide d'une politique prédéfinie

- Définissez des cookies signés à l'aide d'une politique personnalisée

Décidez d'utiliser des politiques prédéfinies ou personnalisées pour les cookies signés

Lorsque vous créez un cookie signé, vous écrivez une instruction de politique au format JSON qui spécifie les restrictions sur le cookie signé : par exemple, la durée de validité du cookie. Vous pouvez utiliser une politique prédéfinie ou une politique personnalisé e. Le tableau suivant compare les politiques prédéfinies et les politiques personnalisées :

Description	Politique prédéfinie	Politique personnalisée
Vous pouvez réutiliser la déclaration de politique pour plusieurs fichiers. Pour ce faire, vous devez utiliser les caractères génériques de l'objet `Resource`. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.)	Non	Oui
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs peuvent commencer à accéder à votre contenu	Non	Oui (facultatif)
Vous pouvez indiquer la date et l'heure auxquelle s les utilisateurs ne peuvent plus accéder à votre contenu	Oui	Oui
Vous pouvez spécifier l'adresse IP ou la plage d'adresses IP des utilisateurs qui peuvent accéder à votre contenu	Non	Oui (facultatif)

Pour plus d'informations sur la création de cookies signés à l'aide d'une politique prédéfinie, consultez Définissez des cookies signés à l'aide d'une politique prédéfinie.

Pour plus d'informations sur la création de cookies signés à l'aide d'une politique personnalisée, consultez Définissez des cookies signés à l'aide d'une politique personnalisée.

Fonctionnement des cookies signés

Voici un aperçu de la façon dont vous configurez CloudFront les cookies signés et de la manière dont vous CloudFront répondez lorsqu'un utilisateur soumet une demande contenant un cookie signé.

1. Dans votre CloudFront distribution, spécifiez un ou plusieurs groupes de clés fiables, qui contiennent les clés publiques CloudFront pouvant être utilisées pour vérifier la signature de l'URL. Vous utilisez les clés privées correspondantes pour signer les URL.

   Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.
2. Vous développez votre application pour déterminer si un utilisateur doit avoir accès à votre contenu et, si tel est le cas, pour envoyer trois en-têtes `Set-Cookie` à l'utilisateur. (Chaque `Set-Cookie` en-tête ne peut contenir qu'une seule paire nom-valeur, et un cookie CloudFront signé nécessite trois paires nom-valeur.) Vous devez envoyer les en-têtes `Set-Cookie` à l'utilisateur avant qu'il ne demande votre contenu privé. Si vous définissez une durée d'expiration brève sur le cookie, il se peut aussi que vous vouliez envoyer trois en-têtes `Set-Cookie` supplémentaires en réponse aux demandes suivantes, de telle sorte que l'utilisateur puisse continuer à y accéder.

   En règle générale, votre CloudFront distribution aura au moins deux comportements de cache, l'un qui ne nécessite pas d'authentification et l'autre qui en nécessite une. La page d'erreur de la partie sécurisé du site inclut une redirection ou un lien vers une page de connexion.

   Si vous configurez votre distribution pour mettre en cache des fichiers basés sur des cookies, CloudFront elle ne met pas en cache des fichiers séparés en fonction des attributs des cookies signés.
3. Un utilisateur se connecte à votre site web et paie le contenu ou satisfait à quelques autres exigences pour l'accès.
4. Votre application renvoie les en-têtes `Set-Cookie` dans la réponse, et l'utilisateur stocke les paires nom-valeur.
5. L'utilisateur demande un fichier.

   Le navigateur de cet utilisateur ou d'un autre obtient les paires nom-valeur de l'étape 4 et les ajoute à la demande dans un en-tête `Cookie`. Il s'agit du cookie signé.
6. CloudFront utilise la clé publique pour valider la signature du cookie signé et pour confirmer que le cookie n'a pas été falsifié. Si la signature n'est pas valide, la demande est rejetée.

Si la signature contenue dans le cookie est valide, CloudFront consultez la déclaration de politique contenue dans le cookie (ou créez-en une si vous utilisez une politique prédéfinie) pour confirmer que la demande est toujours valide. Par exemple, si vous avez spécifié une date et une heure de début et de fin pour le cookie, cela CloudFront confirme que l'utilisateur essaie d'accéder à votre contenu pendant la période pendant laquelle vous souhaitez autoriser l'accès.

Si la demande répond aux exigences de la déclaration de politique, CloudFront diffuse votre contenu comme elle le fait pour le contenu non restreint : elle détermine si le fichier se trouve déjà dans le cache périphérique, transmet la demande à l'origine si nécessaire et renvoie le fichier à l'utilisateur.

Empêcher l'utilisation abusive des cookies signés

Si vous spécifiez le paramètre `Domain` dans un en-tête `Set-Cookie`, spécifiez la valeur la plus précise possible pour réduire les possibilités d’accès par une personne ayant le même nom de domaine racine. Par exemple, app.example.com est préférable à example.com, particulièrement quand vous ne contrôlez pas example.com. Vous empêchez ainsi qu’une personne accède à votre contenu depuis www.example.com.

Pour contribuer à empêcher ce type d’attaque, procédez comme suit :

- Excluez les attributs de cookie `Expires` et `Max-Age`, de telle sorte que l’en-tête `Set-Cookie` crée un cookie de session. Les cookies de session sont automatiquement supprimés quand l’utilisateur clôt le navigateur, ce qui réduit la possibilité que quelqu’un n’obtienne un accès non autorisé à votre contenu.
- Incluez l’attribut `Secure`, de telle sorte que le cookie soit chiffré quand un utilisateur l’inclut dans une demande.
- Chaque fois que possible, utilisez une politique personnalisée et incluez l’adresse IP de l’utilisateur.
- Dans l’attribut `CloudFront-Expires`, spécifiez la durée d’expiration raisonnable la plus courte selon la période pendant laquelle vous autorisez les utilisateurs à accéder à votre contenu.

Quand CloudFront vérifie la date et l'heure d'expiration dans un cookie signé

Pour déterminer si un cookie signé est toujours valide, CloudFront vérifie la date et l'heure d'expiration du cookie au moment de la requête HTTP. Si un client commence à télécharger un fichier volumineux immédiatement avant la date d’expiration, le téléchargement se termine même si la date

d'expiration intervient pendant le téléchargement. Si la connexion TCP cesse et que le client essaie de redémarrer le téléchargement une fois la date d'expiration passée, le téléchargement échoue.

Si un client utilise des intervalles GET pour obtenir un fichier en parties plus petites, toute requête GET qui intervient après la date d'expiration échoue. Pour plus d'informations sur Range GET, consultez Comment CloudFront traite les demandes partielles pour un objet (plage GETS).

Exemple de code et outils tiers

L'exemple de code de contenu privé montre uniquement comment créer la signature pour les URL signées. Cependant, le processus de création d'une signature d'un cookie signé étant très similaire, une grande partie de l'exemple de code continue à être pertinente. Pour plus d'informations, consultez les rubriques suivantes :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Définissez des cookies signés à l'aide d'une politique prédéfinie

Pour définir un cookie signé à l'aide d'une politique prédéfinie, procédez comme suit. Pour créer la signature, consultez Création d'une signature pour un cookie signé qui utilise une politique prédéfinie.

Pour définir un cookie signé à l'aide d'une politique prédéfinie

1. Si vous utilisez .NET ou Java pour créer des cookies signés et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformater la clé privée (.NET et Java uniquement).
2. Programmez votre application pour qu'elle envoie trois en-têtes `Set-Cookie` aux utilisateurs approuvées. Vous avez besoin de trois `Set-Cookie` en-têtes car chaque `Set-Cookie` en-tête ne peut contenir qu'une seule paire nom-valeur, et un cookie CloudFront signé nécessite trois paires nom-valeur. Les paires nom-valeur sont : `CloudFront-Expires`, `CloudFront-Signature` et `CloudFront-Key-Pair-Id`. Les valeurs doivent être présentes sur la visionneuse avant qu'un utilisateur ne puisse faire la requête d'un fichier dont vous voulez contrôler l'accès.

> **Note**
>
> En règle générale, nous recommandons d'exclure les attributs `Expires` et `Max-Age`. L'exclusion des attributs conduit le navigateur à supprimer le cookie quand l'utilisateur ferme le navigateur, ce qui réduit la possibilité qu'une personne obtienne un accès non autorisé à votre contenu. Pour plus d'informations, consultez Empêcher l'utilisation abusive des cookies signés.

Les noms des attributs de cookie sont sensibles à la casse.

Les sauts de ligne ne sont inclus que pour rendre les attributs plus lisibles.

```
Set-Cookie:
CloudFront-Expires=date and time in Unix time format (in seconds) and Coordinated
 Universal Time (UTC);
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Signature=hashed and signed version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Key-Pair-Id=public key ID for the CloudFront public key whose
 corresponding private key you're using to generate the signature;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly
```

(Facultatif) **`Domain`**

Nom de domaine du fichier demandé. Si vous ne spécifiez pas un attribut `Domain`, la valeur par défaut est le nom de domaine de l'URL et ne s'applique qu'au nom de domaine spécifié,

non aux sous-domaines. Si vous spécifiez un attribut `Domain`, il s'applique aussi aux sous-domaines. Un point devant le nom de domaine (par exemple, `Domain=.example.com`) est facultatif. De plus, si vous spécifiez un attribut `Domain`, le nom de domaine de l'URL et la valeur de l'attribut `Domain` doivent correspondre.

Vous pouvez spécifier le nom de domaine CloudFront attribué à votre distribution, par exemple d111111abcdef8.cloudfront.net, mais vous ne pouvez pas spécifier*.cloudfront.net pour le nom de domaine.

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence des paramètres de distribution.

(Facultatif) **`Path`**

Chemin d'accès du fichier demandé. Si vous ne spécifiez pas d'attribut `Path`, la valeur par défaut est le chemin d'accès de l'URL.

`Secure`

Nécessite que l'utilisateur chiffre les cookies avant d'envoyer une demande. Nous vous recommandons d'envoyer l'`Set-Cookie`en-tête via une connexion HTTPS pour vous assurer que les attributs du cookie sont protégés contre man-in-the-middle les attaques.

`HttpOnly`

Définit la manière dont le navigateur (lorsqu'il est pris en charge) interagit avec la valeur du cookie. Avec`HttpOnly`, les valeurs des cookies ne sont pas accessibles à JavaScript. Cette précaution peut contribuer à atténuer les attaques par script intersite (XSS). Pour plus d'informations, consultez la section Utilisation de cookies HTTP.

`CloudFront-Expires`

Spécifiez la date et l'heure d'expiration au format horaire Unix (en secondes) et en heure UTC. Par exemple, la date 1er janvier 2013 10 h 00 UTC est convertie en 1357034400 au format horaire Unix. Pour utiliser l'heure epoch, utilisez un entier de 32 bits pour une date qui ne peut pas être postérieure à 2147483647 (19 janvier 2038 à 03:14:07 UTC). Pour plus d'informations sur UTC, consultez RFC 3339, Date et heure sur Internet : Horodatages, https://tools.ietf.org/html/rfc3339.

`CloudFront-Signature`

Version hachée, signée et encodée en base 64 d'une déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique prédéfinie.

`CloudFront-Key-Pair-Id`

L'ID d'une clé CloudFront publique, par exemple,`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront la clé publique à utiliser pour valider l'URL signée. CloudFront compare les informations de la signature avec celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.

L'exemple suivant illustre les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers :

```
Set-Cookie: CloudFront-Expires=1426500000; Domain=d111111abcdef8.cloudfront.net; Path=/
images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=yXrSIgyQoeE4FBI4eMKF6ho~CA8_;
 Domain=d111111abcdef8.cloudfront.net; Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=d111111abcdef8.cloudfront.net; Path=/images/*; Secure; HttpOnly
```

L'exemple suivant illustre les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez le nom de domaine alternatif example.org dans les URL de vos fichiers :

```
Set-Cookie: CloudFront-Expires=1426500000; Domain=example.org; Path=/images/*; Secure;
 HttpOnly
Set-Cookie: CloudFront-Signature=yXrSIgyQoeE4FBI4eMKF6ho~CA8_; Domain=example.org;
 Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/images/*;
 Secure; HttpOnly
```

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou

non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence des paramètres de distribution.

Création d'une signature pour un cookie signé qui utilise une politique prédéfinie

Pour créer la signature d'un cookie signé qui utilise une politique prédéfinie, procédez comme suit.

Rubriques

- Création d'une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie
- Signez la déclaration de politique pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

Création d'une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie

Lorsque vous définissez un cookie signé qui utilise une politique prédéfinie, l'attribut `CloudFront-Signature` est une version hachée et signée d'une déclaration de politique. Pour les cookies signés qui utilisent une politique prédéfinie, vous n'incluez pas la déclaration de politique dans l'en-tête `Set-Cookie`, comme vous le faites pour les cookies signés qui utilisent une politique personnalisée. Pour créer l'a déclaration de politique, procédez comme suit.

Pour créer une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie

1. Construisez la déclaration de politique à l'aide du format JSON suivant et de l'encodage de caractères UTF-8. Incluez la ponctuation et les autres valeurs littérales exactement comme spécifié. Pour plus d'informations sur les paramètres `Resource` et `DateLessThan`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique prédéfinie pour les cookies signés.

```
{
    "Statement": [
        {
            "Resource": "base URL or stream name",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": ending date and time in Unix time format and
 UTC
                }
            }
        }
    ]
```

```
}
```

2. Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.

Valeurs que vous spécifiez dans la déclaration de politique d'une politique prédéfinie pour les cookies signés

Lorsque vous créez une déclaration de politique pour une politique prédéfinie, vous spécifiez les valeurs suivantes :

Ressource

L'URL de base incluant vos chaînes de requête, le cas échéant ; par exemple :

`https://d111111abcdef8.cloudfront.net/images/horizon.jpg?size=large&license=yes`

Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

Remarques :

- Protocole : la valeur doit commencer par `http://` ou `https://`.
- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour le fichier.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. N'entourez pas la valeur de points d'interrogation.

Par exemple, la date 16 mars 2015 10 h 00 UTC est convertie en 1426500000 au format horaire Unix.

Cette valeur doit correspondre à la valeur de l'attribut `CloudFront-Expires` de l'en-tête `Set-Cookie`. N'entourez pas la valeur de points d'interrogation.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration dans un cookie signé.

Exemple de déclaration de politique pour une politique prédéfinie

Lorsque vous utilisez l'exemple de déclaration de politique suivant dans un cookie signé, un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/horizon.jpg` jusqu'au 16 mars 2015 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1426500000
                }
            }
        }
    ]
}
```

Signez la déclaration de politique pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

Pour créer la valeur de l'attribut `CloudFront-Signature` d'un en-tête `Set-Cookie`, vous hachez et signez la déclaration de politique que vous avez créée dans Pour créer une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez les rubriques suivantes :

- Commandes Linux et OpenSSL pour le codage et le chiffrement base64
- Exemples de code pour la création de la signature d'une URL signée

Pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

1. Utilisez la fonction de hachage SHA-1 et RSA pour hacher et signer la déclaration de politique que vous avez créée dans la procédure Pour créer une déclaration de politique pour un cookie

signé qui utilise une politique prédéfinie. Utilisez la version de la déclaration de politique qui ne contient plus d'espaces vides.

Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

> **Note**
>
> La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la chaîne hachée et signée.
3. Encodez en base64 la chaîne à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans l'en-tête `Set-Cookie` de la paire nom-valeur `CloudFront-Signature`. Puis retournez à Pour définir un cookie signé à l'aide d'une politique prédéfinie pour ajouter l'en-tête `Set-Cookie` de `CloudFront-Key-Pair-Id`.

Définissez des cookies signés à l'aide d'une politique personnalisée

Pour définir un cookie signé qui utilise une politique personnalisée, effectuez la procédure suivante.

Pour définir un cookie signé utilisant une politique personnalisée

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformater la clé privée (.NET et Java uniquement).
2. Programmez votre application pour qu'elle envoie trois en-têtes `Set-Cookie` aux utilisateurs approuvées. Vous avez besoin de trois `Set-Cookie` en-têtes car chaque `Set-Cookie` en-tête ne peut contenir qu'une seule paire nom-valeur, et un cookie CloudFront signé nécessite trois paires nom-valeur. Les paires nom-valeur sont : `CloudFront-Policy`, `CloudFront-Signature` et `CloudFront-Key-Pair-Id`. Les valeurs doivent être présentes sur la visionneuse avant qu'un utilisateur ne puisse faire la requête d'un fichier dont vous voulez contrôler l'accès.

   > **Note**
   >
   > En règle générale, nous recommandons d'exclure les attributs `Expires` et `Max-Age`. Cette exclusion conduit le navigateur à supprimer le cookie quand l'utilisateur ferme le navigateur, ce qui réduit la possibilité qu'une personne obtienne un accès non autorisé à votre contenu. Pour plus d'informations, consultez Empêcher l'utilisation abusive des cookies signés.

   Les noms des attributs de cookie sont sensibles à la casse.

   Les sauts de ligne ne sont inclus que pour rendre les attributs plus lisibles.

```
Set-Cookie:
CloudFront-Policy=base64 encoded version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly


Set-Cookie:
CloudFront-Signature=hashed and signed version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
```

```
Secure;
HttpOnly

Set-Cookie:
CloudFront-Key-Pair-Id=public key ID for the CloudFront public key whose
 corresponding private key you're using to generate the signature;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly
```

(Facultatif) **`Domain`**

Nom de domaine du fichier demandé. Si vous ne spécifiez pas un attribut `Domain`, la valeur par défaut est le nom de domaine de l'URL et ne s'applique qu'au nom de domaine spécifié, non aux sous-domaines. Si vous spécifiez un attribut `Domain`, il s'applique aussi aux sous-domaines. Un point devant le nom de domaine (par exemple, `Domain=.example.com`) est facultatif. De plus, si vous spécifiez un attribut `Domain`, le nom de domaine de l'URL et la valeur de l'attribut `Domain` doivent correspondre.

Vous pouvez spécifier le nom de domaine CloudFront attribué à votre distribution, par exemple d111111abcdef8.cloudfront.net, mais vous ne pouvez pas spécifier*.cloudfront.net pour le nom de domaine.

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence des paramètres de distribution.

(Facultatif) **`Path`**

Chemin d'accès du fichier demandé. Si vous ne spécifiez pas d'attribut `Path`, la valeur par défaut est le chemin d'accès de l'URL.

`Secure`

Nécessite que l'utilisateur chiffre les cookies avant d'envoyer une demande. Nous vous recommandons d'envoyer l'`Set-Cookie`en-tête via une connexion HTTPS pour vous assurer que les attributs du cookie sont protégés contre man-in-the-middle les attaques.

`HttpOnly`

Requiert que l'utilisateur n'envoie le cookie que dans les requêtes HTTP ou HTTPS.

`CloudFront-Policy`

Votre déclaration de politique au format JSON, avec les espaces vides supprimés, puis encodée en base64. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

La déclaration de politique contrôle l'accès accordé par un cookie signé à un utilisateur. Elle inclut les fichiers auxquels l'utilisateur peut accéder, une date et une heure d'expiration, une date et une heure (facultatif) auxquelles l'URL devient valide et une adresse IP (facultatif) ou une plage d'adresses IP autorisées à accéder au fichier.

`CloudFront-Signature`

Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

`CloudFront-Key-Pair-Id`

L'ID d'une clé CloudFront publique, par exemple,`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront la clé publique à utiliser pour valider l'URL signée. CloudFrontcompare les informations de la signature avec celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécifiez les signataires autorisés à créer des URL signées et des cookies signés.

Exemples d'**`Set-Cookie`**en-têtes pour les politiques personnalisées

Consultez les exemples de paires d'`Set-Cookie`en-têtes suivants.

Si vous souhaitez utiliser un autre nom de domaine tel que exemple.org dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez ou non l'`Domain`attribut. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence des paramètres de distribution.

Example Exemple 1

Vous pouvez utiliser `Set-Cookie` les en-têtes d'un cookie signé lorsque vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
```

Example Exemple 2

Vous pouvez utiliser `Set-Cookie` les en-têtes d'un cookie signé lorsque vous utilisez un autre nom de domaine (exemple.org) dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=example.org; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_; Domain=example.org;
 Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/; Secure;
 HttpOnly
```

Example Exemple 3

Vous pouvez utiliser les paires d'`Set-Cookie`en-têtes pour une demande signée lorsque vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=dd111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
```

Example Exemple 4

Vous pouvez utiliser les paires `Set-Cookie` d'en-têtes pour une demande signée lorsque vous utilisez un autre nom de domaine (exemple.org) associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=example.org; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_; Domain=example.org;
 Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/; Secure;
 HttpOnly
```

Création d'une déclaration de politique pour un cookie signé qui utilise une politique personnalisée

Pour créer une déclaration de politique pour une politique personnalisée, effectuez la procédure suivante. Pour obtenir des exemples de déclaration de politique qui contrôlent l’accès aux fichiers de différentes façons, consultez Exemple d’une déclaration de politique pour un cookie signé qui utilise une politique personnalisée.

Pour créer la déclaration de politique d’un cookie signé qui utilise une politique personnalisée

1. Construisez la déclaration de politique à l’aide du format JSON suivant.

```
{
    "Statement": [
        {
            "Resource": "URL of the file",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime":required ending date and time in Unix time
 format and UTC
                },
                "DateGreaterThan": {
                    "AWS:EpochTime":optional beginning date and time in Unix time
 format and UTC
                },
                "IpAddress": {
                    "AWS:SourceIp": "optional IP address"
                }
            }
```

```
        }
    ]
}
```

Remarques :

- Vous pouvez inclure une seule instruction.
- Utilisez l'encodage de caractères UTF-8.
- Incluez la ponctuation et les noms de paramètre exactement comme spécifié. Les abréviations ne sont pas acceptées pour les noms de paramètre.
- L'ordre des paramètres de la section `Condition` n'importe pas.
- Pour plus d'informations sur les valeurs de `Resource`, `DateLessThan`, `DateGreaterThan` et `IpAddress`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.

2. Supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.
3. Encodez en base64 la déclaration de politique à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans votre en-tête `Set-Cookie` après `CloudFront-Policy=`.

6. Créez une signature pour l'en-tête `Set-Cookie` de `CloudFront-Signature` en hachant, signant et encodant en base64 la déclaration de politique. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés

Lorsque vous créez une déclaration de politique pour une politique personnalisée, vous spécifiez les valeurs suivantes.

Ressource

L'URL de base incluant vos chaînes de requête, le cas échéant :

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

> **Important**
>
> Si vous omettez le paramètre `Resource`, les utilisateurs peuvent accéder à tous les fichiers associés à une distribution elle-même associée à la paire de clés que vous utilisez pour créer l'URL signée.

Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

Remarques :

- Protocole : la valeur doit commencer par `http://` ou `https://`.
- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Caractères génériques : vous pouvez utiliser à tout moment dans la chaîne, le caractère générique qui correspond à zéro caractère ou plus (*) ou celui qui correspond exactement à un seul caractère (?). Par exemple, la valeur :

  ```
  https://d111111abcdef8.cloudfront.net/*game_download.zip*
  ```

  inclut (par exemple) les fichiers suivants :

  - `https://d111111abcdef8.cloudfront.net/game_download.zip`

  - `https://d111111abcdef8.cloudfront.net/example_game_download.zip?license=yes`
  - `https://d111111abcdef8.cloudfront.net/test_game_download.zip?license=temp`
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour le fichier.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. N'entourez pas la valeur de points d'interrogation.

Par exemple, la date 16 mars 2015 10 h 00 UTC est convertie en 1426500000 au format horaire Unix.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration dans un cookie signé.

DateGreaterThan (Facultatif)

(Facultatif) Date et heure de début de l'URL au format horaire Unix (en secondes) et en heure UTC. Les utilisateurs ne sont pas autorisés à accéder au fichier à la date et à l'heure spécifiées ou avant. N'entourez pas la valeur de points d'interrogation.

IpAddress (Facultatif)

Adresse IP du client formulant la demande GET. Remarques :

- Pour autoriser une adresse IP à accéder au fichier, omettez le paramètre `IpAddress`.
- Vous pouvez spécifier une adresse IP ou une plage d'adresses IP. Par exemple, vous pouvez définir la politique pour autoriser l'accès si l'adresse IP du client figure dans l'une des deux plages distinctes.
- Pour autoriser l'accès depuis une seule adresse IP, vous spécifiez :

  `"`*`Adresse IP IPv4`*`/32"`
- Vous devez spécifier les plages d'adresses IP selon le format IPv4 CIDR standard (par exemple, `192.0.2.0/24`). Pour plus d'informations, consultez RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, https://tools.ietf.org/html/rfc4632.

> **Important**
>
> Les adresses IP au format IPv6, telles que 2001:0db8:85a3::8a2e:0370:7334, ne sont pas prises en charge.

Si vous utilisez une politique personnalisée qui inclut `IpAddress`, n'activez pas IPv6 pour la distribution. Si vous souhaitez limiter l'accès à un contenu spécifique par adresse IP et prendre en charge les requêtes IPv6 pour les autres contenus, vous pouvez créer deux distributions. Pour plus d'informations, consultez Activation d'IPv6 dans la rubrique Référence des paramètres de distribution.

Exemple d'une déclaration de politique pour un cookie signé qui utilise une politique personnalisée

Les exemples suivants de déclaration de politique montrent comment accéder à un fichier spécifique, à tous les objets d'un répertoire ou à tous les fichiers associés à un ID de paire de clés. Les exemples montrent aussi comment contrôler l'accès depuis une adresse IP individuelle ou une plage d'adresses IP, et comment empêcher les utilisateurs d'employer le cookie signé au-delà d'une date et heure spécifiées.

Si vous copiez et collez l'un de ces exemples, supprimez tous les espaces vides (y compris les tabulations et les caractères de nouvelle ligne), remplacez les valeurs par vos propres valeurs et insérez un caractère de nouvelle ligne après l'accolade fermante (}).

Pour plus d'informations, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.

Rubriques

- Exemple de déclaration de politique : accéder à un fichier à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accédez à tous les fichiers associés à un identifiant de paire de clés à partir d'une adresse IP

Exemple de déclaration de politique : accéder à un fichier à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée dans un cookie signé spécifie qu'un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/game_download.zip` à partir des adresses IP de la plage `192.0.2.0/24` jusqu'au 1er janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1357034400
                }
            }
        }
    ]
}
```

Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée vous permet de créer des cookies signés pour n'importe quel fichier du répertoire `training`, comme indiqué par le caractère générique * du paramètre `Resource`. Les utilisateurs peuvent accéder au fichier depuis une adresse IP de la plage `192.0.2.0/24` jusqu'au 1er janvier 2013 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1357034400
                }
            }
```

```
        }
    ]
}
```

Chaque cookie signé dans lequel vous utilisez cette politique inclut une URL de base qui identifie un fichier spécifique ; par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Exemple de déclaration de politique : accédez à tous les fichiers associés à un identifiant de paire de clés à partir d'une adresse IP

L'exemple suivant de politique personnalisée vous permet de définir des cookies signés pour tout fichier associé à une distribution, comme indiqué par le caractère générique * du paramètre `Resource`. L'utilisateur doit employer l'adresse IP `192.0.2.10/32`. (La valeur `192.0.2.10/32` en notation CIDR fait référence à une seule adresse IP, `192.0.2.10`.) Les fichiers ne sont disponibles qu'entre le 1er janvier 2013 10 h 00 UTC et le 2 janvier 2013 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1357034400
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1357120800
                }
            }
        }
    ]
}
```

Chaque cookie signé dans lequel vous utilisez cette politique inclut une URL de base qui identifie un fichier spécifique dans une CloudFront distribution spécifique, par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Le cookie signé inclut aussi un ID de paire de clés, qui doit être associé à un groupe de clés approuvé de la distribution (d111111abcdef8.cloudfront.net) que vous spécifiez dans l'URL de base.

Création d'une signature pour un cookie signé qui utilise une politique personnalisée

La signature d'un cookie signé utilisant une politique personnalisée est une version hachée, signée et encodée en base64 de la déclaration de politique.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Commandes Linux et OpenSSL pour le codage et le chiffrement base64
- Exemples de code pour la création de la signature d'une URL signée

Pour créer une signature pour un cookie signé en utilisant une politique personnalisée

1. Utilisez la fonction de hachage SHA-1 et RSA pour hacher et signer la déclaration de politique JSON que vous avez créée dans la procédure Pour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée. Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides mais qui n'a pas encore été codée en base64.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

   > **Note**
   >
   > La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (y compris les tabulations et les caractères de nouvelle ligne) de la chaîne hachée et signée.
3. Encodez en base64 la chaîne à l'aide de l'encodage MIME base64. Pour plus d'informations, consultez Section 6.8, Base64 Content-Transfer-Encoding dans RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans l'en-tête `Set-Cookie` de la paire nom-valeur `CloudFront-Signature=`, et retournez à Pour définir un cookie signé utilisant une politique personnalisée pour ajouter l'en-tête `Set-Cookie` de `CloudFront-Key-Pair-Id`.

Commandes Linux et OpenSSL pour le codage et le chiffrement base64

Vous pouvez utiliser la commande de ligne de commande Linux suivante et OpenSSL pour hacher et signer la déclaration de politique, encoder la signature en base64 et remplacer les caractères non valides des paramètres de la chaîne de requête de l'URL par des caractères valides.

Pour plus d'informations sur OpenSSL, rendez-vous sur https://www.openssl.org.

```
cat policy | tr -d "\n" | tr -d " \t\n\r" | openssl sha1 -sign private_key.pem |
 openssl base64 -A | tr -- '+=/' '-_~'
```

Dans la commande précédente :

- `cat`lit le `policy` fichier
- `tr -d "\n" | tr -d " \t\n\r"`supprime les espaces vides et le caractère de nouvelle ligne ajoutés par `cat`
- OpenSSL hache le fichier à l'aide de SHA-1 et le signe à l'aide de RSA et du fichier de clé privée `private_key.pem`
- OpenSSL base64 encode la déclaration de politique hachée et signée
- `tr`remplace les caractères non valides dans les paramètres de chaîne de requête d'URL par des caractères valides

Pour d'autres exemples de code illustrant la création d'une signature, consultezExemples de code pour la création de la signature d'une URL signée.

Exemples de code pour la création de la signature d'une URL signée

Cette section inclut des exemples d'application téléchargeables qui montrent comment créer des signatures pour les URL signées. Les exemples sont disponibles en Perl, PHP, C# et Java. Vous pouvez utiliser l'un des exemples pour créer des URL signées. Le script Perl s'exécute sur les plateformes Linux et MacOS. L'exemple PHP fonctionne sur n'importe quel serveur qui exécute PHP. L'exemple C# utilise le .NET Framework.

Pour un exemple de code dans JavaScript (Node.js), consultez la section Création d'URL CloudFront signées Amazon dans Node.js sur le blog des AWS développeurs.

Pour un exemple de code en Python, consultez Generate a signed URL for Amazon CloudFront dans le AWS SDK for Python (Boto3) API Reference et cet exemple de code dans le référentiel Boto3. GitHub

Rubriques

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Créer une signature d'URL avec Perl

Cette section inclut un script Perl pour les plates-formes Linux/Mac que vous pouvez utiliser pour créer la signature du contenu privé. Pour créer la signature, exécutez le script avec des arguments de ligne de commande qui spécifient l' CloudFront URL, le chemin d'accès à la clé privée du signataire, l'ID de la clé et la date d'expiration de l'URL. L'outil peut aussi décoder les URL signées.

> **Note**
>
> La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec une URL signée. Pour plus d'informations sur le end-to-end processus, consultezUtiliser des URL signées.

Rubriques

Source du script Perl pour la création d'une URL signée

Le code source Perl suivant peut être utilisé pour créer une URL signée pour CloudFront. Les commentaires du code incluent les informations sur les fonctions et les commutateurs de ligne de commande de l'outil.

```
#!/usr/bin/perl -w

# Copyright 2008 Amazon Technologies, Inc.  Licensed under the Apache License, Version
 2.0 (the "License");
# you may not use this file except in compliance with the License. You may obtain a
 copy of the License at:
#
# https://aws.amazon.com/apache2.0
#
# This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
 KIND, either express or implied.
# See the License for the specific language governing permissions and limitations under
 the License.

=head1 cfsign.pl

cfsign.pl - A tool to generate and verify Amazon CloudFront signed URLs

=head1 SYNOPSIS

This script uses an existing RSA key pair to sign and verify Amazon CloudFront signed
 URLs

View the script source for details as to which CPAN packages are required beforehand.

For help, try:

cfsign.pl --help

URL signing examples:

cfsign.pl --action encode --url https://images.my-website.com/gallery1.zip --policy
 sample_policy.json --private-key privkey.pem --key-pair-id mykey
```

```
cfsign.pl --action encode --url https://images.my-website.com/gallery1.zip --expires
 1257439868 --private-key privkey.pem --key-pair-id mykey

URL decode example:

cfsign.pl --action decode --url "http//mydist.cloudfront.net/?Signature=AGO-
PgxkYo99MkJFHvjfGXjG1QDEXeaDb4Qtzmy85wqyJjK7eKojQWa4BCRcow__&Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc29
Pair-Id=mykey"


To generate an RSA key pair, you can use openssl and the following commands:

# Generate a 2048 bit key pair
openssl genrsa -out private-key.pem 2048
openssl rsa -in private-key.pem -pubout -out public-key.pem


=head1 OPTIONS

=over 8

=item B<--help>

Print a help message and exits.

=item B<--action> [action]

The action to execute.  action can be one of:

  encode - Generate a signed URL (using a canned policy or a user policy)
  decode - Decode a signed URL

=item B<--url>

The URL to en/decode

=item B<--stream>

The stream to en/decode

=item B<--private-key>

The path to your private key.
```

```
=item B<--key-pair-id>

The key pair identifier.

=item B<--policy>

The CloudFront policy document.

=item B<--expires>

The Unix epoch time when the URL is to expire. If both this option and
the --policy option are specified, --policy will be used. Otherwise, this
option alone will use a canned policy.

=back

=cut

use strict;
use warnings;

# you might need to use CPAN to get these modules.
# run perl -MCPAN -e "install <module>" to get them.
# The openssl command line will also need to be in your $PATH.
use File::Temp qw/tempfile/;
use File::Slurp;
use Getopt::Long;
use IPC::Open2;
use MIME::Base64 qw(encode_base64 decode_base64);
use Pod::Usage;
use URI;

my $CANNED_POLICY
    = '{"Statement":[{"Resource":"<RESOURCE>","Condition":{"DateLessThan":
{"AWS:EpochTime":<EXPIRES>}}}]}';

my $POLICY_PARAM      = "Policy";
my $EXPIRES_PARAM     = "Expires";
my $SIGNATURE_PARAM   = "Signature";
my $KEY_PAIR_ID_PARAM = "Key-Pair-Id";

my $verbose = 0;
my $policy_filename = "";
```

```
my $expires_epoch = 0;
my $action = "";
my $help = 0;
my $key_pair_id = "";
my $url = "";
my $stream = "";
my $private_key_filename = "";

my $result = GetOptions("action=s"      => \$action,
                        "policy=s"      => \$policy_filename,
                        "expires=i"     => \$expires_epoch,
                        "private-key=s" => \$private_key_filename,
                        "key-pair-id=s" => \$key_pair_id,
                        "verbose"       => \$verbose,
                        "help"          => \$help,
                        "url=s"         => \$url,
                        "stream=s"      => \$stream,
                    );

if ($help or !$result) {
    pod2usage(1);
    exit;
}

if ($url eq "" and $stream eq "") {
    print STDERR "Must include a stream or a URL to encode or decode with the --stream
 or --url option\n";
    exit;
}

if ($url ne "" and $stream ne "") {
    print STDERR "Only one of --url and --stream may be specified\n";
    exit;
}

if ($url ne "" and !is_url_valid($url)) {
    exit;
}

if ($stream ne "") {
    exit unless is_stream_valid($stream);

    # The signing mechanism is identical, so from here on just pretend we're
    # dealing with a URL
```

```
    $url = $stream;
}

if ($action eq "encode") {
    # The encode action will generate a private content URL given a base URL,
    # a policy file (or an expires timestamp) and a key pair id parameter
    my $private_key;
    my $public_key;
    my $public_key_file;

    my $policy;
    if ($policy_filename eq "") {
        if ($expires_epoch == 0) {
            print STDERR "Must include policy filename with --policy argument or an
 expires" .
                         "time using --expires\n";
        }

        $policy = $CANNED_POLICY;
        $policy =~ s/<EXPIRES>/$expires_epoch/g;
        $policy =~ s/<RESOURCE>/$url/g;
    } else {
        if (! -e $policy_filename) {
            print STDERR "Policy file $policy_filename does not exist\n";
            exit;
        }
        $expires_epoch = 0; # ignore if set
        $policy = read_file($policy_filename);
    }

    if ($private_key_filename eq "") {
        print STDERR "You must specific the path to your private key file with --
private-key\n";
        exit;
    }

    if (! -e $private_key_filename) {
        print STDERR "Private key file $private_key_filename does not exist\n";
        exit;
    }

    if ($key_pair_id eq "") {
        print STDERR "You must specify a key pair id with --key-pair-id\n";
        exit;
```

```
    }

    my $encoded_policy = url_safe_base64_encode($policy);
    my $signature = rsa_sha1_sign($policy, $private_key_filename);
    my $encoded_signature = url_safe_base64_encode($signature);

    my $generated_url = create_url($url, $encoded_policy, $encoded_signature,
 $key_pair_id, $expires_epoch);


    if ($stream ne "") {
        print "Encoded stream (for use within a swf):\n" . $generated_url . "\n";
        print "Encoded and escaped stream (for use on a webpage):\n" .
 escape_url_for_webpage($generated_url) . "\n";
    } else {
        print "Encoded URL:\n" . $generated_url . "\n";
    }
} elsif ($action eq "decode") {
    my $decoded = decode_url($url);
    if (!$decoded) {
        print STDERR "Improperly formed URL\n";
        exit;
    }

    print_decoded_url($decoded);
} else {
    # No action specified, print help.  But only if this is run as a program (caller
 will be empty)
    pod2usage(1) unless caller();
}

# Decode a private content URL into its component parts
sub decode_url {
    my $url = shift;

    if ($url =~ /(.*)\?(.*)/) {
        my $base_url = $1;
        my $params = $2;

        my @unparsed_params = split(/&/, $params);
        my %params = ();
        foreach my $param (@unparsed_params) {
            my ($key, $val) = split(/=/, $param);
            $params{$key} = $val;
```

```
        }

        my $encoded_signature = "";
        if (exists $params{$SIGNATURE_PARAM}) {
            $encoded_signature = $params{"Signature"};
        } else {
            print STDERR "Missing Signature URL parameter\n";
            return 0;
        }

        my $encoded_policy = "";
        if (exists $params{$POLICY_PARAM}) {
            $encoded_policy = $params{$POLICY_PARAM};
        } else {
            if (!exists $params{$EXPIRES_PARAM}) {
                print STDERR "Either the Policy or Expires URL parameter needs to be
specified\n";
                return 0;
            }

            my $expires = $params{$EXPIRES_PARAM};

            my $policy = $CANNED_POLICY;
            $policy =~ s/<EXPIRES>/$expires/g;

            my $url_without_cf_params = $url;
            $url_without_cf_params =~ s/$SIGNATURE_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$POLICY_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$EXPIRES_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$KEY_PAIR_ID_PARAM=[^&]*&?//g;

            if ($url_without_cf_params =~ /(.*)\?$/) {
                $url_without_cf_params = $1;
            }

            $policy =~ s/<RESOURCE>/$url_without_cf_params/g;

            $encoded_policy = url_safe_base64_encode($policy);
        }

        my $key = "";
        if (exists $params{$KEY_PAIR_ID_PARAM}) {
            $key = $params{$KEY_PAIR_ID_PARAM};
        } else {
```

```
            print STDERR "Missing $KEY_PAIR_ID_PARAM parameter\n";
            return 0;
        }

        my $policy = url_safe_base64_decode($encoded_policy);

        my %ret = ();
        $ret{"base_url"} = $base_url;
        $ret{"policy"} = $policy;
        $ret{"key"} = $key;

        return \%ret;
    } else {
        return 0;
    }
}

# Print a decoded URL out
sub print_decoded_url {
    my $decoded = shift;

    print "Base URL: \n" . $decoded->{"base_url"} . "\n";
    print "Policy: \n" . $decoded->{"policy"} . "\n";
    print "Key: \n" . $decoded->{"key"} . "\n";
}

# Encode a string with base 64 encoding and replace some invalid URL characters
sub url_safe_base64_encode {
    my ($value) = @_;

    my $result = encode_base64($value);
    $result =~ tr|+=/|-_~|;

    return $result;
}

# Decode a string with base 64 encoding.  URL-decode the string first
# followed by reversing any special character ("+=/") translation.
sub url_safe_base64_decode {
    my ($value) = @_;

    $value =~ s/%([0-9A-Fa-f]{2})/chr(hex($1))/eg;
    $value =~ tr|-_~|+=/|;
```

```
    my $result = decode_base64($value);

    return $result;
}

# Create a private content URL
sub create_url {
    my ($path, $policy, $signature, $key_pair_id, $expires) = @_;

    my $result;
    my $separator = $path =~ /\?/ ? '&' : '?';
    if ($expires) {
        $result = "$path$separator$EXPIRES_PARAM=$expires&$SIGNATURE_PARAM=$signature&
$KEY_PAIR_ID_PARAM=$key_pair_id";
    } else {
        $result = "$path$separator$POLICY_PARAM=$policy&$SIGNATURE_PARAM=$signature&
$KEY_PAIR_ID_PARAM=$key_pair_id";
    }
    $result =~ s/\n//g;

    return $result;
}

# Sign a document with given private key file.
# The first argument is the document to sign
# The second argument is the name of the private key file
sub rsa_sha1_sign {
    my ($to_sign, $pvkFile) = @_;
    print "openssl sha1 -sign $pvkFile $to_sign\n";

    return write_to_program($pvkFile, $to_sign);
}

# Helper function to write data to a program
sub write_to_program {
my ($keyfile, $data) = @_;
unlink "temp_policy.dat" if (-e "temp_policy.dat");
unlink "temp_sign.dat" if (-e "temp_sign.dat");

write_file("temp_policy.dat", $data);

system("openssl dgst -sha1 -sign \"$keyfile\" -out temp_sign.dat temp_policy.dat");

my $output = read_file("temp_sign.dat");
```

```
    return $output;
}

# Read a file into a string and return the string
sub read_file {
    my ($file) = @_;

    open(INFILE, "<$file") or die("Failed to open $file: $!");
    my $str = join('', <INFILE>);
    close INFILE;

    return $str;
}

sub is_url_valid {
    my ($url) = @_;

    # HTTP distributions start with http[s]:// and are the correct thing to sign
    if ($url =~ /^https?:\/\//) {
        return 1;
    } else {
        print STDERR "CloudFront requires absolute URLs for HTTP distributions\n";
        return 0;
    }
}

sub is_stream_valid {
    my ($stream) = @_;

    if ($stream =~ /^rtmp:\/\// or $stream =~ /^\/?cfx\/st/) {
        print STDERR "Streaming distributions require that only the stream name is
 signed.\n";
        print STDERR "The stream name is everything after, but not including, cfx/st/
\n";
        return 0;
    } else {
        return 1;
    }
}

# flash requires that the query parameters in the stream name are url
# encoded when passed in through javascript, etc.  This sub handles the minimal
# required url encoding.
```

```
sub escape_url_for_webpage {
    my ($url) = @_;

    $url =~ s/\?/%3F/g;
    $url =~ s/=/%3D/g;
    $url =~ s/&/%26/g;

    return $url;
}

1;
```

Créer une signature d'URL avec PHP

Tout serveur Web qui exécute PHP peut utiliser cet exemple de code PHP pour créer des déclarations de politique et des signatures pour CloudFront des distributions privées. L'exemple complet crée une page Web fonctionnelle avec des liens URL signés qui diffusent un flux vidéo CloudFront en streaming. Vous pouvez télécharger l'exemple complet à l'adresse https:// docs.aws.amazon.com/ AmazonCloudFront DeveloperGuide /latest/ /samples/demo-php.zip.

Vous pouvez aussi créer des URL signées à l'aide de la classe `UrlSigner` du AWS SDK for PHP. Pour plus d'informations, consultez la section Classe UrlSigner dans la référence de AWS SDK for PHP l'API.

> **Note**
>
> La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec une URL signée. Pour plus d'informations sur la totalité du processus, consultez Utiliser des URL signées.

Rubriques

Exemple : signature RSA SHA-1

Dans l'exemple de code suivant, la fonction `rsa_sha1_sign` hache et signe la déclaration de politique. Les arguments requis sont une déclaration de politique et la clé privée qui correspond à une clé publique qui se trouve dans un groupe de clés approuvé pour votre distribution. Ensuite, la fonction `url_safe_base64_encode` crée une version à URL sécurisée de la signature.

```
function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";

    // load the private key
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);

    // compute signature
    openssl_sign($policy, $signature, $pkeyid);

    // free the key from memory
    openssl_free_key($pkeyid);

    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    // replace unsafe characters +, = and / with
    // the safe characters -, _ and ~
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

Exemple : créer une politique prédéfinie

L'exemple de code suivant construit une déclaration de politique prédéfinie pour la signature. Pour plus d'informations sur les politiques prédéfinies, consultez Création d'une URL signée à l'aide d'une politique prédéfinie.

> **Note**
>
> La variable `$expires` est un horodatage qui doit être un entier et non une chaîne.

```
function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it,
    // since it contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';

    // sign the canned policy
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a url
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // url-encode the query string characters to work around a flash player bug
    return encode_query_params($stream_name);
}
```

Exemple : créer une politique personnalisée

L'exemple de code suivant construit une déclaration de politique personnalisée pour la signature. Pour plus d'informations sur les politiques personnalisées, consultez Création d'une URL signée à l'aide d'une politique personnalisée.

```
function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // sign the policy
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a url
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // url-encode the query string characters to work around a flash player bug
    return encode_query_params($stream_name);
```

```
}
```

Exemple de code complet

L'exemple de code suivant fournit une démonstration complète de la création d'URL CloudFront signées avec PHP. Vous pouvez télécharger cet exemple complet à l'adresse https:// docs.aws.amazon.com/ AmazonCloudFront DeveloperGuide /latest/ /samples/demo-php.zip.

Dans l'exemple suivant, vous pouvez modifier l'`$policyCondition`élément pour autoriser les plages d'adresses IPv4 et IPv6. Par exemple, consultez la section Utilisation des adresses IPv6 dans les politiques IAM du guide de l'utilisateur d'Amazon Simple Storage Service.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";

    // load the private key
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);

    // compute signature
    openssl_sign($policy, $signature, $pkeyid);

    // free the key from memory
    openssl_free_key($pkeyid);

    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    // replace unsafe characters +, = and / with the safe characters -, _ and ~
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}

function create_stream_name($stream, $policy, $signature, $key_pair_id, $expires) {
    $result = $stream;
```

```
    // if the stream already contains query parameters, attach the new query parameters
 to the end
    // otherwise, add the query parameters
    $separator = strpos($stream, '?') == FALSE ? '?' : '&';
    // the presence of an expires time means we're using a canned policy
    if($expires) {
        $result .= $path . $separator . "Expires=" . $expires . "&Signature=" .
 $signature . "&Key-Pair-Id=" . $key_pair_id;
    }
    // not using a canned policy, include the policy itself in the stream name
    else {
        $result .= $path . $separator . "Policy=" . $policy . "&Signature=" .
 $signature . "&Key-Pair-Id=" . $key_pair_id;
    }

    // new lines would break us, so remove them
    return str_replace('\n', '', $result);
}

function encode_query_params($stream_name) {
    // Adobe Flash Player has trouble with query parameters being passed into it,
    // so replace the bad characters with their URL-encoded forms
    return str_replace(
        array('?', '=', '&'),
        array('%3F', '%3D', '%26'),
        $stream_name);
}

function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
```

```
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters to support Flash Player
    return encode_query_params($stream_name);
}

function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters to support Flash Player
    return encode_query_params($stream_name);
}


// Path to your private key.  Be very careful that this file is not accessible
// from the web!

$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';

$video_path = 'example.mp4';

$expires = time() + 300; // 5 min from now
$canned_policy_stream_name = get_canned_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $expires);

$client_ip = $_SERVER['REMOTE_ADDR'];
$policy =
'{'.
    '"Statement":['.
        '{'.
            '"Resource":"'. $video_path . '",'.
            '"Condition":{'.
                '"IpAddress":{"AWS:SourceIp":"' . $client_ip . '/32"},'.
```

```
                '"DateLessThan":{"AWS:EpochTime":' . $expires . '}'.
            '}'.
        '}'.
    ']' .
    '}';
$custom_policy_stream_name = get_custom_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $policy);

?>

<html>

<head>
    <title>CloudFront</title>
<script type='text/javascript' src='https://example.cloudfront.net/player/
swfobject.js'></script>
</head>

<body>
    <h1>Amazon CloudFront</h1>
    <h2>Canned Policy</h2>
    <h3>Expires at <?= gmdate('Y-m-d H:i:s T', $expires) ?></h3>
    <br />

    <div id='canned'>The canned policy video will be here</div>

    <h2>Custom Policy</h2>
    <h3>Expires at <?= gmdate('Y-m-d H:i:s T', $expires) ?> only viewable by IP <?=
 $client_ip ?></h3>
    <div id='custom'>The custom policy video will be here</div>

    <!-- ************** Have to update the player.swf path to a real JWPlayer instance.
    The fake one means that external people cannot watch the video right now -->
    <script type='text/javascript'>
  var so_canned = new SWFObject('https://files.example.com/
player.swf','mpl','640','360','9');
  so_canned.addParam('allowfullscreen','true');
  so_canned.addParam('allowscriptaccess','always');
  so_canned.addParam('wmode','opaque');
  so_canned.addVariable('file','<?= $canned_policy_stream_name ?>');
  so_canned.addVariable('streamer','rtmp://example.cloudfront.net/cfx/st');
        so_canned.write('canned');
```

```
  var so_custom = new SWFObject('https://files.example.com/
player.swf','mpl','640','360','9');
  so_custom.addParam('allowfullscreen','true');
  so_custom.addParam('allowscriptaccess','always');
  so_custom.addParam('wmode','opaque');
  so_custom.addVariable('file','<?= $custom_policy_stream_name ?>');
  so_custom.addVariable('streamer','rtmp://example.cloudfront.net/cfx/st');
  so_custom.write('custom');
    </script>
</body>

</html>
```

Voir aussi:

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Créer une signature d'URL avec C# et .NET Framework

Les exemples C# présentés dans cette section mettent en œuvre un exemple d'application qui montre comment créer des signatures pour des distributions CloudFront privées à l'aide de déclarations de politique prédéfinies et personnalisées. Les exemples incluent des fonctions utilitaires basées sur le AWS SDK for .NET pour .NET et qui peuvent être utiles dans les applications .NET.

Vous pouvez aussi créer des URL et des cookies signés à l'aide du AWS SDK for .NET. Dans la Référence d'API du AWS SDK for .NET , consultez les rubriques suivantes :

- URL signées — AmazonCloudFrontUrlSigner
- Cookies signés — AmazonCloudFrontCookieSigner

Pour télécharger le code, consultez Code de signature en C#.

> **Note**
>
> La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec une URL signée. Pour plus d'informations sur la totalité du processus, consultez Utiliser

des URL signées. Pour plus d'informations sur l'utilisation de cookies signés, consultezUtiliser des cookies signés.

Utiliser une clé RSA dans le .NET Framework

Pour utiliser une clé RSA dans le .NET Framework, vous devez convertir le fichier .pem AWS fourni au format XML utilisé par le .NET Framework.

Après la conversion, le fichier de clé privée RSA est au format suivant :

Example : clé privée RSA au format XML .NET Framework

```
<RSAKeyValue>
  <Modulus>
    wO5IvYCP5UcoCKDo1dcspoMehWBZcyfs9QEzGi6Oe5y+ewGr1oW+vB2GPB
    ANBiVPcUHTFWhwaIBd3oglmF0lGQljP/jOfmXHUK2kUUnLnJp+oOBL2NiuFtqcW6h/L5lIpD8Yq+NRHg
    Ty4zDsyr2880MvXv88yEFURCkqEXAMPLE=
  </Modulus>
  <Exponent>AQAB</Exponent>
  <P>
    5bmKDaTz
    npENGVqz4Cea8XPH+sxt+2VaAwYnsarVUoSBeVt8WLloVuZGG9IZYmH5KteXEu7fZveYd9UEXAMPLE==
  </P>
  <Q>
    1v9l/WN1a1N3rOK4VGoCokx7kR2SyTMSbZgF9IWJNOugR/WZw7HTnjipO3c9dy1Ms9pUKwUF4
    6d7049EXAMPLE==
  </Q>
  <DP>
    RgrSKuLWXMyBH+/l1Dx/I4tXuAJIrlPyo+VmiOc7b5NzHptkSHEPfR9s1
    OK0VqjknclqCJ3Ig86OMEtEXAMPLE==
  </DP>
  <DQ>
    pjPjvSFw+RoaTu0pgCA/jwW/FGyfN6iim1RFbkT4
    z49DZb2IM885f3vf35eLTaEYRYUHQgZtChNEV0TEXAMPLE==
  </DQ>
  <InverseQ>
    nkvOJTg5QtGNgWb9i
    cVtzrL/1pFEOHbJXwEJdU99N+7sMK+1066DL/HSBUCD63qD4USpnf0myc24in0EXAMPLE==</InverseQ>
  <D>
      Bc7mp7XYHynuPZxChjWNJZIq+A73gm0ASDv6At7F8Vi9r0xUlQe/v0AQS3ycN8QlyR4XMbzMLYk
      3yjxFDXo4ZKQtOGzLGteCU2srANiLv26/imXA8FVidZftTAtLviWQZBVPTeYIA69ATUYPEq0a5u5wjGy
      UOij9OWyuEXAMPLE=
```

```
   </D>
</RSAKeyValue>
```

Méthode de signature de politique prédéfinie en C#

Le code C# suivant crée une URL signée qui utilise une politique prédéfinie en effectuant les opérations suivantes :

- Crée une déclaration de politique.
- Hache la déclaration de politique avec SHA1 et signe le résultat à l'aide de RSA et de la clé privée dont la clé publique correspondante se trouve dans un groupe de clés approuvé.
- Encode en base64 la déclaration de politique hachée et signée, et remplace les caractères spéciaux pour assurer la sécurité de la chaîne utilisée comme paramètre de demande d'URL.
- Concatène les valeurs.

Pour l'implémentation complète, consultez l'exemple de la rubrique Code de signature en C#.

> **Note**
>
> Le `keyId` est renvoyé lorsque vous téléchargez une clé publique sur CloudFront. Pour plus d'informations, consultez
>
> 6
>
> &Key-Pair-Id.

Example : méthode de signature de politique prédéfinie en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}

public static string CreateCannedPrivateURL(string urlString,
    string durationUnits, string durationNumber, string pathToPolicyStmnt,
    string pathToPrivateKey, string keyId)
{
```

```
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-pathToPolicyStmnt,
    // 5-pathToPrivateKey, 6-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);

    // Create the policy statement.
    string strPolicy = CreatePolicyStatement(pathToPolicyStmnt,
        urlString,
        DateTime.Now,
        DateTime.Now.Add(timeSpanInterval),
        "0.0.0.0/0");
    if ("Error!" == strPolicy) return "Invalid time frame." +
        "Start time cannot be greater than end time.";

    // Copy the expiration time defined by policy statement.
    string strExpiration = CopyExpirationTimeFromPolicy(strPolicy);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    using (SHA1CryptoServiceProvider
        cryptoSHA1 = new SHA1CryptoServiceProvider())
    {
        bufferPolicy = cryptoSHA1.ComputeHash(bufferPolicy);

        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA and
        // create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter rsaFormatter =
            new RSAPKCS1SignatureFormatter(providerRSA);
        rsaFormatter.SetHashAlgorithm("SHA1");
        byte[] signedPolicyHash = rsaFormatter.CreateSignature(bufferPolicy);
```

```
        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedPolicyHash);

        // Concatenate the URL, the timestamp, the signature,
        // and the key pair ID to form the signed URL.
        return urlString +
            "?Expires=" +
            strExpiration +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Méthode de signature de politique personnalisée en C#

Le code C# suivant crée une URL signée qui utilise une politique personnalisée en effectuant les opérations suivantes :

1. Crée une déclaration de politique.
2. Encode en base64 la déclaration de politique et remplace les caractères spéciaux pour assurer la sécurité de la chaîne utilisée comme paramètre de demande d'URL.
3. Hache la déclaration de politique avec SHA1 et chiffre le résultat à l'aide de RSA et de la clé privée dont la clé publique correspondante se trouve dans un groupe de clés approuvé.
4. Encode en base64 la déclaration de politique hachée et remplace les caractères spéciaux pour assurer la sécurité de la chaîne utilisée comme paramètre de demande d'URL.
5. Concatène les valeurs.

Pour l'implémentation complète, consultez l'exemple de la rubrique Code de signature en C#.

> **Note**
>
> Le `keyId` est renvoyé lorsque vous téléchargez une clé publique sur CloudFront. Pour plus d'informations, consultez
>
> 6
>
> &Key-Pair-Id.

Example : méthode de signature de politique personnalisée en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}

public static string CreateCustomPrivateURL(string urlString,
    string durationUnits, string durationNumber, string startIntervalFromNow,
    string ipaddress, string pathToPolicyStmnt, string pathToPrivateKey,
    string keyId)
{
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-starttimeFromNow,
    // 5-ip_address, 6-pathToPolicyStmt, 7-pathToPrivateKey, 8-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);
    TimeSpan timeSpanToStart = GetDurationByUnits(durationUnits,
        startIntervalFromNow);
    if (null == timeSpanToStart)
        return "Invalid duration units." +
            "Valid options: seconds, minutes, hours, or days";

    string strPolicy = CreatePolicyStatement(
        pathToPolicyStmnt, urlString, DateTime.Now.Add(timeSpanToStart),
        DateTime.Now.Add(timeSpanInterval), ipaddress);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Convert the policy statement to URL-safe base64 encoding and
    // replace unsafe characters + = / with the safe characters - _ ~

    string urlSafePolicy = ToUrlSafeBase64String(bufferPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    byte[] bufferPolicyHash;
    using (SHA1CryptoServiceProvider cryptoSHA1 =
        new SHA1CryptoServiceProvider())
    {
        bufferPolicyHash = cryptoSHA1.ComputeHash(bufferPolicy);
```

```
        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA
        // and create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter RSAFormatter =
            new RSAPKCS1SignatureFormatter(providerRSA);
        RSAFormatter.SetHashAlgorithm("SHA1");
        byte[] signedHash = RSAFormatter.CreateSignature(bufferPolicyHash);

        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedHash);

        return urlString +
            "?Policy=" +
            urlSafePolicy +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Méthodes d’utilité pour la génération de signatures

Les méthodes suivantes obtiennent la déclaration de politique d’un fichier et analyse les intervalles de temps pour la génération des signatures.

Example : Méthodes utilitaires pour la génération de signatures

```
public static string CreatePolicyStatement(string policyStmnt,
   string resourceUrl,
   DateTime startTime,
   DateTime endTime,
   string ipAddress)
```

```
{
   // Create the policy statement.
   FileStream streamPolicy = new FileStream(policyStmnt, FileMode.Open,
 FileAccess.Read);
   using (StreamReader reader = new StreamReader(streamPolicy))
   {
      string strPolicy = reader.ReadToEnd();

      TimeSpan startTimeSpanFromNow = (startTime - DateTime.Now);
      TimeSpan endTimeSpanFromNow = (endTime - DateTime.Now);
      TimeSpan intervalStart =
         (DateTime.UtcNow.Add(startTimeSpanFromNow)) -
         new DateTime(1970, 1, 1, 0, 0, 0, DateTimeKind.Utc);
      TimeSpan intervalEnd =
         (DateTime.UtcNow.Add(endTimeSpanFromNow)) -
         new DateTime(1970, 1, 1, 0, 0, 0, DateTimeKind.Utc);

      int startTimestamp = (int)intervalStart.TotalSeconds; // START_TIME
      int endTimestamp = (int)intervalEnd.TotalSeconds;  // END_TIME

      if (startTimestamp > endTimestamp)
         return "Error!";

      // Replace variables in the policy statement.
      strPolicy = strPolicy.Replace("RESOURCE", resourceUrl);
      strPolicy = strPolicy.Replace("START_TIME", startTimestamp.ToString());
      strPolicy = strPolicy.Replace("END_TIME", endTimestamp.ToString());
      strPolicy = strPolicy.Replace("IP_ADDRESS", ipAddress);
      strPolicy = strPolicy.Replace("EXPIRES", endTimestamp.ToString());
      return strPolicy;
   }
}

public static TimeSpan GetDuration(string units, string numUnits)
{
   TimeSpan timeSpanInterval = new TimeSpan();
   switch (units)
   {
      case "seconds":
         timeSpanInterval = new TimeSpan(0, 0, 0, int.Parse(numUnits));
         break;
      case "minutes":
         timeSpanInterval = new TimeSpan(0, 0, int.Parse(numUnits), 0);
```

```
         break;
      case "hours":
         timeSpanInterval = new TimeSpan(0, int.Parse(numUnits), 0 ,0);
         break;
      case "days":
         timeSpanInterval = new TimeSpan(int.Parse(numUnits),0 ,0 ,0);
         break;
      default:
         Console.WriteLine("Invalid time units;" +
            "use seconds, minutes, hours, or days");
         break;
   }
   return timeSpanInterval;
}

private static TimeSpan GetDurationByUnits(string durationUnits,
   string startIntervalFromNow)
{
   switch (durationUnits)
   {
      case "seconds":
         return new TimeSpan(0, 0, int.Parse(startIntervalFromNow));
      case "minutes":
         return new TimeSpan(0, int.Parse(startIntervalFromNow), 0);
      case "hours":
         return new TimeSpan(int.Parse(startIntervalFromNow), 0, 0);
      case "days":
         return new TimeSpan(int.Parse(startIntervalFromNow), 0, 0, 0);
      default:
         return new TimeSpan(0, 0, 0, 0);
   }
}

public static string CopyExpirationTimeFromPolicy(string policyStatement)
{
   int startExpiration = policyStatement.IndexOf("EpochTime");
   string strExpirationRough = policyStatement.Substring(startExpiration +
      "EpochTime".Length);
   char[] digits = { '0', '1', '2', '3', '4', '5', '6', '7', '8', '9' };

   List<char> listDigits = new List<char>(digits);
   StringBuilder buildExpiration = new StringBuilder(20);

   foreach (char c in strExpirationRough)
```

```
    {
        if (listDigits.Contains(c))
            buildExpiration.Append(c);
    }
    return buildExpiration.ToString();
}
```

Voir aussi

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec Java

Créer une signature d'URL avec Java

Outre l'exemple de code suivant, vous pouvez utiliser la classe `CloudFrontUrlSigner` utilitaire de la AWS SDK for Java (version 1) pour créer des URL CloudFront signées.

Pour plus d'exemples, consultez la section Création d'URL signées et de cookies à l'aide d'un AWS SDK dans la bibliothèque de codes d'exemples de code AWS SDK.

> **Note**
>
> La création d'une URL signée n'est qu'une partie du processus de diffusion de contenu privé avec CloudFront. Pour plus d'informations sur la totalité du processus, consultez Utiliser des URL signées.

L'exemple suivant montre comment créer une URL CloudFront signée.

Example Méthodes de chiffrement de politiques et de signatures Java

```
package org.example;

import java.time.Instant;
import java.time.temporal.ChronoUnit;
import software.amazon.awssdk.services.cloudfront.CloudFrontUtilities;
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;
import software.amazon.awssdk.services.cloudfront.url.SignedUrl;
```

```
public class Main {

    public static void main(String[] args) throws Exception {
        CloudFrontUtilities cloudFrontUtilities = CloudFrontUtilities.create();
        Instant expirationDate = Instant.now().plus(7, ChronoUnit.DAYS);
        String resourceUrl = "https://a1b2c3d4e5f6g7.cloudfront.net";
        String keyPairId = "K1UA3WV15I7JSD";
        CannedSignerRequest cannedRequest = CannedSignerRequest.builder()
                .resourceUrl(resourceUrl)
                .privateKey(new java.io.File("/path/to/private_key.pem").toPath())
                .keyPairId(keyPairId)
                .expirationDate(expirationDate)
                .build();
        SignedUrl signedUrl =
 cloudFrontUtilities.getSignedUrlWithCannedPolicy(cannedRequest);
        String url = signedUrl.url();
        System.out.println(url);

    }
}
```

Voir aussi :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework

Restreindre l'accès à une AWS origine

Vous pouvez configurer CloudFront certaines AWS origines d'une manière qui offre les avantages suivants :

- Restreint l'accès à l' AWS origine afin qu'elle ne soit pas accessible au public
- Veille à ce que les spectateurs (utilisateurs) puissent accéder au contenu de l' AWS origine uniquement par le biais de la CloudFront distribution spécifiée, en les empêchant d'accéder au contenu directement depuis le bucket ou par le biais d'une distribution involontaire CloudFront

Pour ce faire, configurez CloudFront pour envoyer des demandes authentifiées à votre AWS origine, et configurez l' AWS origine pour autoriser uniquement l'accès aux demandes authentifiées provenant

de. CloudFront Pour plus d'informations, consultez les rubriques suivantes pour connaître les types d' AWS origines compatibles.

Rubriques

Restreindre l'accès à une origine AWS Elemental MediaPackage v2

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à une origine MediaPackage v2.

> **Note**
>
> CloudFront OAC ne prend en charge que la MediaPackage v2. MediaPackage la v1 n'est pas prise en charge.

Rubriques

Création d'un nouvel OAC

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouvel OAC dans CloudFront.

Rubriques

Prérequis

Avant de créer et de configurer OAC, vous devez disposer d'une CloudFront distribution d'origine MediaPackage v2. Pour plus d'informations, consultez Utiliser un MediaStore conteneur ou un MediaPackage canal.

Donner à l'OAC l'autorisation d'accéder à l'origine de la MediaPackage version v2

Avant de créer un OAC ou de le configurer dans une CloudFront distribution, assurez-vous que l'OAC est autorisé à accéder à l'origine MediaPackage v2. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l'origine MediaPackage v2 dans la configuration de distribution.

Pour autoriser l'OAC à accéder à l'origine MediaPackage v2, utilisez une politique IAM pour autoriser le principal de CloudFront service (`cloudfront.amazonaws.com`) à accéder à l'origine. L'`Condition`élément de la politique permet d'accéder CloudFront à l'origine MediaPackage v2 uniquement lorsque la demande est au nom de la CloudFront distribution qui contient l'origine MediaPackage v2.

Example : politique IAM qui autorise l'accès en lecture seule à une distribution CloudFront

La politique suivante autorise la CloudFront distribution (*E1PDK09ESKHJWT*) à accéder à l'origine MediaPackage v2. L'origine est l'ARN spécifié pour l'`Resource`élément.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "mediapackagev2:GetObject",
            "Resource": "arn:aws:mediapackagev2:us-
east-1:123456789012:channelGroup/channel-group-name/channel/channel-name/
originEndpoint/origin_endpoint_name",
            "Condition": {
                "StringEquals": {"AWS:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT"}
            }
        }
    ]
```

```
}
```

> **Note**
>
> Si vous créez une distribution qui n'est pas autorisée à accéder à votre origine MediaPackage v2, vous pouvez choisir Copier la politique depuis la CloudFront console, puis choisir Mettre à jour les autorisations du point de terminaison. Vous pouvez ensuite associer l'autorisation copiée au point de terminaison. Pour plus d'informations, consultez les champs de politique des terminaux dans le guide de AWS Elemental MediaPackage l'utilisateur.

Création de l'OAC

Pour créer un OAC, vous pouvez utiliser le AWS Management Console AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un OAC

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Dans le formulaire Créer un nouveau OAC, procédez comme suit :
   a. Entrez un nom et (éventuellement) une description pour l'OAC.
   b. Pour le comportement de signature, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d'informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.
5. Pour le type d'origine, choisissez MediaPackage V2.
6. Choisissez Créer.

> **Tip**
>
> Après avoir créé l'OAC, notez le nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un OAC à une origine MediaPackage v2 dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution d'origine MediaPackage V2 à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origins.
3. Sélectionnez l'origine MediaPackage v2 à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant du contrôle d'accès Origin, choisissez le nom OAC que vous souhaitez utiliser.
6. Sélectionnez Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine MediaPackage v2.

CloudFormation

Pour créer un OAC avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, pour créer un OAC.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: mediapackagev2
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, consultez la section AWS::CloudFront::OriginAccessContrôle dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à une origine MediaPackage v2 dans une CloudFront distribution.

Pour attacher un OAC à une origine MediaPackage v2 dans une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une origine MediaPackage v2.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine MediaPackage v2.

API

Pour créer un OAC avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou un autre client d'API.

Après avoir créé un OAC, vous pouvez l'associer à une origine MediaPackage v2 dans une distribution, à l'aide de l'un des appels d'API suivants :

- Pour le rattacher à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, fournissez l'ID OAC dans le `OriginAccessControlId` champ, dans une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité CloudFront OAC inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

L'OAC contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et AWS CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d'utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l'API, la CLI et AWS CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l'origine de la MediaPackage v2.

Ne jamais signer les demandes d'origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre pour désactiver l'OAC pour toutes les origines dans toutes les distributions qui utilisent cet OAC. Cela permet d'économiser du temps et des efforts par rapport à la suppression d'un OAC de toutes les origines et distributions qui l'utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l'origine de la MediaPackage v2.

> **Warning**
>
> Pour utiliser ce paramètre, l'origine MediaPackage v2 doit être accessible au public. Si vous utilisez ce paramètre avec une origine MediaPackage v2 qui n'est pas accessible au public, CloudFront vous ne pouvez pas accéder à l'origine. L'origine MediaPackage v2 renvoie les erreurs CloudFront et les CloudFront transmet aux spectateurs. Pour plus d'informations, consultez l'exemple de politique MediaPackage v2 pour les politiques et les autorisations MediaPackage dans le guide de AWS Elemental MediaPackage l'utilisateur.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour transmettre l'`Authorization`en-tête de la demande du lecteur, vous devez l'`Authorization`ajouter à une politique de cache pour tous les comportements de cache qui utilisent des origines MediaPackage v2 associées à ce contrôle d'accès à l'origine.

Restreindre l'accès à une AWS Elemental MediaStore origine

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à une AWS Elemental MediaStore origine.

Rubriques

- Création d'un nouveau contrôle d'accès à l'origine
- Paramètres avancés pour le contrôle d'accès à l'origine

Création d'un nouveau contrôle d'accès à l'origine

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouveau contrôle d'accès à l'origine dans CloudFront.

Rubriques

- Prérequis
- Donner à l'origine l'autorisation de contrôle d'accès d'accéder à l' MediaStore origine
- Création du contrôle d'accès à l'origine

Prérequis

Avant de créer et de configurer le contrôle d'accès à l'origine, vous devez disposer d'une CloudFront distribution avec une MediaStore origine.

Donner à l'origine l'autorisation de contrôle d'accès d'accéder à l' MediaStore origine

Avant de créer un contrôle d'accès à l'origine ou de le configurer dans une CloudFront distribution, assurez-vous que l'OAC est autorisé à accéder à l' MediaStore origine. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l' MediaStoreorigine dans la configuration de distribution.

Pour autoriser l'OAC à accéder à l' MediaStore origine, utilisez une politique de MediaStore conteneur pour autoriser le principal de CloudFront service (`cloudfront.amazonaws.com`) à accéder à l'origine. Utilisez un `Condition` élément de la politique pour autoriser l'accès CloudFront au MediaStore conteneur uniquement lorsque la demande est présentée au nom de la CloudFront distribution qui contient l' MediaStore origine.

Voici des exemples de politiques relatives aux MediaStore conteneurs qui permettent à un CloudFront OAC d'accéder à une MediaStore origine.

Example MediaStore politique de conteneur qui autorise l'accès en lecture seule à un OAC CloudFront

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadOnly",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject"
                ],
                "Resource":
 "arn:aws:mediastore:<region>:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
```

```
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

Example MediaStore politique de conteneur qui autorise l'accès en lecture et en écriture à un CloudFront OAC

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadWrite",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject",
                  "mediastore:PutObject"
                ],
                "Resource":
 "arn:aws:mediastore:<region>:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

> **Note**
>
> Pour autoriser l'accès en écriture, vous devez configurer les méthodes HTTP autorisées à inclure PUT dans les paramètres de comportement de votre CloudFront distribution.

Création du contrôle d'accès à l'origine

Pour créer un OAC, vous pouvez utiliser le AWS Management Console AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un contrôle d'accès à l'origine

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :
   a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.
   b. Dans le volet Paramètres, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d'informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.
5. MediaStore Choisissez dans le menu déroulant Type d'origine.
6. Choisissez Créer.

   Après avoir créé l'OAC, prenez note de Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès à l'origine à une MediaStore origine dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Choisissez une distribution avec une MediaStore origine à laquelle vous souhaitez ajouter l'OAC, puis cliquez sur l'onglet Origines.
3. Sélectionnez l' MediaStore origine à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Sélectionnez Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du MediaStore compartiment.

CloudFormation

Pour créer un contrôle d'accès à l'origine (OAC) avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, pour créer un contrôle d'accès à l'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: mediastore
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, consultez la section AWS::CloudFront::OriginAccessContrôle dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à une MediaStore origine dans une CloudFront distribution.

Pour attacher un OAC à une MediaStore origine dans une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une MediaStore origine.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
- Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l' MediaStoreorigine.

API

Pour créer un contrôle d'accès à l'origine avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé un contrôle d'accès à l'origine, vous pouvez l'associer à une MediaStore origine dans une distribution à l'aide de l'un des appels d'API suivants :

- Pour l'associer à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de contrôle d'accès à l'origine dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité de contrôle CloudFront d'accès à l'origine inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

Le contrôle d'accès à Origin contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et AWS CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d'utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l'API, la CLI et AWS CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l' MediaStore origine.

Ne jamais signer les demandes d'origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre pour désactiver le contrôle d'accès à l'origine pour toutes les origines dans toutes les distributions qui utilisent ce contrôle d'accès à l'origine. Cela permet d'économiser du temps et des efforts par rapport à la suppression d'un contrôle d'accès à l'origine de toutes les origines et distributions qui l'utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l' MediaStore origine.

> **Warning**
>
> Pour utiliser ce paramètre, l' MediaStore origine doit être accessible au public. Si vous utilisez ce paramètre avec une MediaStore origine qui n'est pas accessible au public, vous CloudFront ne pouvez pas accéder à l'origine. L' MediaStore origine renvoie les erreurs CloudFront et les CloudFront transmet aux spectateurs. Pour plus d'informations, consultez l'exemple de politique de MediaStore conteneur pour l'accès public en lecture via HTTPS.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage

correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour transmettre l'`Authorization`en-tête de la demande du lecteur, vous devez l'`Authorization`ajouter à une politique de cache pour tous les comportements de cache qui utilisent des MediaStore origines associées à ce contrôle d'accès aux origines.

Restreindre l'accès à l'origine de l'URL d'une AWS Lambda fonction

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à l'origine de l'URL d'une fonction Lambda.

Rubriques

- Création d'un nouvel OAC
- Paramètres avancés pour le contrôle d'accès à l'origine

Création d'un nouvel OAC

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouvel OAC dans CloudFront.

> **Note**
>
> Si vous utilisez `POST` des méthodes `PUT` or avec l'URL de votre fonction Lambda, vos utilisateurs doivent inclure la valeur de hachage de la charge utile dans l'`x-amz-content-sha256`en-tête lorsqu'ils envoient la demande à. CloudFront Lambda ne prend pas en charge les charges utiles non signées.

Rubriques

- Prérequis
- Donnez à l'OAC l'autorisation d'accéder à l'URL de la fonction Lambda

- Création de l'OAC

Prérequis

Avant de créer et de configurer OAC, vous devez disposer d'une CloudFront distribution avec une URL de fonction Lambda comme origine. Pour plus d'informations, consultez Utiliser l'URL d'une fonction Lambda.

Donnez à l'OAC l'autorisation d'accéder à l'URL de la fonction Lambda

Avant de créer un OAC ou de le configurer dans une CloudFront distribution, assurez-vous que l'OAC est autorisé à accéder à l'URL de la fonction Lambda. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l'URL de la fonction Lambda dans la configuration de distribution.

> **Note**
>
> Pour mettre à jour la politique IAM pour l'URL de la fonction Lambda, vous devez utiliser AWS Command Line Interface le AWS CLI(). La modification de la politique IAM dans la console Lambda n'est pas prise en charge pour le moment.

La AWS CLI commande suivante accorde au CloudFront service principal (`cloudfront.amazonaws.com`) l'accès à l'URL de votre fonction Lambda. L'`Condition`élément de la politique permet d'accéder CloudFront à Lambda uniquement lorsque la demande provient de la CloudFront distribution qui contient l'URL de la fonction Lambda.

Example : AWS CLI commande pour mettre à jour une politique afin d'autoriser l'accès en lecture seule à un OAC CloudFront

La AWS CLI commande suivante permet à la CloudFront distribution (*`E1PDK09ESKHJWT`*) d'accéder à votre Lambda *`FUNCTION_URL_NAME`*.

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipal" \
--action "lambda:InvokeFunctionUrl" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
```

```
--function-name FUNCTION_URL_NAME
```

> **Note**
>
> Si vous créez une distribution et qu'elle n'est pas autorisée à accéder à l'URL de votre fonction Lambda, vous pouvez choisir la commande Copy CLI depuis la CloudFront console, puis entrer cette commande depuis votre terminal de ligne de commande. Pour plus d'informations, consultez la section Accorder l'accès à une fonction Services AWS dans le Guide du AWS Lambda développeur.

Création de l'OAC

Pour créer un OAC, vous pouvez utiliser le AWS Management Console AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un OAC

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Dans le formulaire Créer un nouveau OAC, procédez comme suit :
   a. Entrez un nom et (éventuellement) une description pour l'OAC.
   b. Pour le comportement de signature, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d'informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.
5. Pour le type d'origine, choisissez Lambda.
6. Choisissez Créer.

> **Tip**
>
> Après avoir créé l'OAC, notez le nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès à l'origine à l'URL d'une fonction Lambda dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une URL de fonction Lambda à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origins.
3. Sélectionnez l'URL de la fonction Lambda à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant du contrôle d'accès Origin, choisissez le nom OAC que vous souhaitez utiliser.
6. Sélectionnez Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'URL de la fonction Lambda.

CloudFormation

Pour créer un OAC avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, pour créer un OAC.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: lambda
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, consultez la section AWS::CloudFront::OriginAccessContrôle dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à l'URL d'une fonction Lambda dans CloudFront une distribution.

Pour associer un OAC à l'URL d'une fonction Lambda dans une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une URL de fonction Lambda comme origine.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'URL de la fonction Lambda.

API

Pour créer un OAC avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou un autre client d'API.

Après avoir créé un OAC, vous pouvez l'associer à l'URL d'une fonction Lambda dans une distribution, à l'aide de l'un des appels d'API suivants :

- Pour le rattacher à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, fournissez l'ID OAC dans le `OriginAccessControlId` champ, dans une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité CloudFront OAC inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

L'OAC contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et AWS CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d'utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l'API, la CLI et AWS CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes envoyées à l'URL de la fonction Lambda.

Ne jamais signer les demandes d'origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre pour désactiver l'OAC pour toutes les origines dans toutes les distributions qui utilisent cet OAC. Cela permet d'économiser du temps et des efforts par rapport à la suppression d'un OAC de toutes les origines et distributions qui l'utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l'URL de la fonction Lambda.

> **Warning**
>
> Pour utiliser ce paramètre, l'URL de la fonction Lambda doit être accessible au public. Si vous utilisez ce paramètre avec une URL de fonction Lambda qui n'est pas accessible au public, CloudFront vous ne pouvez pas accéder à l'origine. L'URL de la fonction Lambda renvoie des erreurs CloudFront et les CloudFront transmet aux utilisateurs. Pour plus d'informations, consultez la section Modèle de sécurité et d'authentification pour les URL des fonctions Lambda dans AWS Lambda le guide de l'utilisateur.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour transmettre l'`Authorization`en-tête de la demande du lecteur, vous devez l'`Authorization`ajouter à une politique de cache pour tous les comportements de cache qui utilisent des URL de fonction Lambda associées à ce contrôle d'accès à l'origine.

Restreindre l'accès à une origine Amazon Simple Storage Service

CloudFront propose deux méthodes pour envoyer des demandes authentifiées à une origine Amazon S3 : le contrôle d'accès à l'origine (OAC) et l'identité d'accès à l'origine (OAI). OAC vous aide à sécuriser vos origines, par exemple pour Amazon S3. Nous vous recommandons d'utiliser OAC car il prend en charge :

- Tous les compartiments Amazon S3 en tout Régions AWS, y compris les régions optionnelles lancées après décembre 2022
- Chiffrement côté serveur avec AWS KMS (SSE-KMS) Amazon S3
- Demandes dynamiques (`PUT` et `DELETE`) vers Amazon S3

L'identité d'accès d'origine ne fonctionne pas pour les scénarios de la liste précédente ou nécessite des solutions de contournement supplémentaires dans ces scénarios. Les rubriques suivantes décrivent comment utiliser le contrôle d'origine d'accès (OAC) avec une origine Amazon S3. Pour plus d'informations sur la migration de l'identité d'accès d'origine (OAI) vers le contrôle d'accès d'origine (OAC), consultez the section called “Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)”.

Remarques

- Lorsque vous utilisez l' CloudFront OAC avec les origines des compartiments Amazon S3, vous devez définir Amazon S3 Object Ownership pour que le propriétaire du compartiment soit appliqué, ce qui est le cas par défaut pour les nouveaux compartiments Amazon S3. Si vous avez besoin d'ACL, utilisez le paramètre préféré du propriétaire du compartiment pour garder le contrôle sur les objets chargés via CloudFront.
- Si votre origine est un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous devez le configurer en CloudFront tant qu'origine personnalisée. Cela signifie que vous ne pouvez pas utiliser OAC (ou OAI). OAC ne prend pas en charge la redirection d'origine à l'aide de Lambda @Edge.

Rubriques

Création d'un nouveau contrôle d'accès à l'origine

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouveau contrôle d'accès à l'origine dans CloudFront.

Rubriques

Prérequis

Avant de créer et de configurer le contrôle d'accès à l'origine (OAC), vous devez disposer d'une CloudFront distribution avec une origine de compartiment Amazon S3. Cette origine doit être un

compartiment S3 normal, et non un compartiment configuré en tant que point de terminaison. Pour plus d'informations sur la configuration d'une CloudFront distribution avec une origine de compartiment S3, consultezthe section called “Commencez avec une distribution de base”.

> **Note**
>
> Lorsque vous utilisez OAC pour sécuriser l'origine de votre compartiment S3, la communication entre Amazon S3 CloudFront et Amazon S3 s'effectue toujours via HTTPS, quels que soient vos paramètres spécifiques.

Donnez à l'origine l'autorisation de contrôle d'accès d'accéder au compartiment S3

Avant de créer un contrôle d'accès à l'origine (OAC) ou de le configurer dans une CloudFront distribution, assurez-vous que l'OAC est autorisé à accéder à l'origine du compartiment S3. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l'origine S3 dans la configuration de distribution.

Pour autoriser l'OAC à accéder au compartiment S3, utilisez une politique de compartiment S3 pour autoriser le principal de CloudFront service (`cloudfront.amazonaws.com`) à accéder au compartiment. Utilisez un `Condition` élément de la politique CloudFront pour autoriser l'accès au compartiment uniquement lorsque la demande provient de la CloudFront distribution contenant l'origine S3.

Pour plus d'informations sur l'ajout ou la modification d'une stratégie de compartiment, consultez Ajout d'une stratégie de compartiment à l'aide de la console Amazon S3 dans le Guide de l’utilisateur Amazon S3.

Voici des exemples de politiques de compartiment S3 qui permettent à un CloudFront OAC d'accéder à une origine S3.

Example Politique de compartiment S3 qui autorise l'accès en lecture seule à un OAC CloudFront

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowCloudFrontServicePrincipalReadOnly",
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudfront.amazonaws.com"
        },
```

```
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::<S3 bucket name>/*",
        "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
    }
}
```

Example Politique de compartiment S3 qui autorise l'accès en lecture et en écriture à un CloudFront OAC

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowCloudFrontServicePrincipalReadWrite",
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudfront.amazonaws.com"
        },
        "Action": [
            "s3:GetObject",
            "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::<S3 bucket name>/*",
        "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
    }
}
```

SSE-KMS

Si les objets de l'origine du compartiment S3 sont chiffrés à l'aide du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS), vous devez vous assurer que l'OAC est autorisé à utiliser la clé. AWS KMS Pour accorder à l'identité d'accès l'autorisation d'utiliser la clé KMS, ajoutez une instruction à la Stratégie de clé KMS. Pour plus d'informations sur la modification d'une stratégie

de clé, consultez Modification d'une stratégie de clé dans le Manuel du développeur AWS Key Management Service .

L'exemple suivant montre une déclaration de stratégie de clé KMS qui permet à l'OAC d'utiliser la clé KMS.

Example Déclaration de politique relative aux clés KMS qui permet à un CloudFront OAC d'accéder à une clé KMS pour SSE-KMS

```
{
    "Sid": "AllowCloudFrontServicePrincipalSSE-KMS",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "cloudfront.amazonaws.com"
        ]
     },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
}
```

Création du contrôle d'accès à l'origine

Pour créer un contrôle d'accès à l'origine (OAC), vous pouvez utiliser le AWS Management Console AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un contrôle d'accès à l'origine

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :

   a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.

   b. Dans le volet Paramètres, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d'informations, consultez the section called "Paramètres avancés pour le contrôle d'accès à l'origine".
5. Choisissez S3 dans la liste déroulante Origin type (Type de l'origine).
6. Choisissez Créer.

   Après avoir créé l'OAC, prenez note de Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès à une origine S3 dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une origine S3 à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origines.
3. Sélectionnez l'origine S3 que vous souhaitez ajouter à l'origine, puis choisissez Modifier.
4. Pour l'accès à Origin, choisissez les paramètres de contrôle d'accès Origin (recommandé).
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Sélectionnez Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du compartiment S3.

CloudFormation

Pour créer un contrôle d'accès à l'origine (OAC) avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, pour créer un contrôle d'accès à l'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: s3
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, consultez la section AWS::CloudFront::OriginAccessContrôle dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à l'origine d'un compartiment S3 dans une CloudFront distribution.

Pour attacher un OAC à l'origine d'un compartiment S3 dans une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une origine de compartiment S3.

   ```
   aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
   output yaml > dist-config.yaml
   ```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

   ```
   aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
   input-yaml file://dist-config.yaml
   ```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du compartiment S3.

API

Pour créer un contrôle d'accès à l'origine avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé un contrôle d'accès à l'origine, vous pouvez l'attacher à l'origine d'un compartiment S3 dans une distribution, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de contrôle d'accès à l'origine dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Supprimer une distribution avec un OAC attaché à un compartiment S3

Si vous devez supprimer une distribution avec un OAC attaché à un compartiment S3, vous devez supprimer la distribution avant de supprimer l'origine du compartiment S3. Vous pouvez également inclure la région dans le nom de domaine d'origine. Si cela n'est pas possible, vous pouvez supprimer l'OAC de la distribution en passant au mode public avant de le supprimer. Pour plus d’informations, consultez Supprimer une distribution .

Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)

Pour migrer d'une ancienne identité d'accès à l'origine (OAI) vers un contrôle d'accès à l'origine (OAC), commencez par mettre à jour l'origine du compartiment S3 afin de permettre à l'OAI et à l'OAC d'accéder au contenu du compartiment. Cela garantit qu'il CloudFront ne perdra jamais l'accès au bucket pendant la transition. Pour permettre à l'OAI et à l'OAC d'accéder à un compartiment S3, mettez à jour la Stratégie de compartiment de façon à inclure deux déclarations, une pour chaque type de principal.

L'exemple de stratégie de compartiment S3 suivant permet à la fois à une OAI et à un OAC d'accéder à une origine S3.

Example Stratégie de compartiment S3 autorisant l'accès en lecture seule à une OAI et à un OAC

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipalReadOnly",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                }
            }
        },
        {
            "Sid": "AllowLegacyOAIReadOnly",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Après avoir mis à jour la stratégie de compartiment de l'origine S3 pour autoriser l'accès à la fois à l'OAI et à l'OAC, vous pouvez mettre à jour la configuration de distribution pour utiliser l'OAC au lieu de l'OAI. Pour plus d'informations, consultez the section called “Création d'un nouveau contrôle d'accès à l'origine”.

Une fois la distribution entièrement déployée, vous pouvez supprimer l'instruction de la politique de compartiment qui autorise l'accès à l'OAI. Pour plus d'informations, consultez the section called “Donnez à l'origine l'autorisation de contrôle d'accès d'accéder au compartiment S3”.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité de contrôle CloudFront d'accès à l'origine inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

Le contrôle d'accès à Origin contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et AWS CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d'utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l'API, la CLI et AWS CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l'origine du compartiment S3.

Ne jamais signer les demandes d'origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre pour désactiver le contrôle d'accès à l'origine pour toutes les origines dans toutes les distributions qui utilisent ce contrôle d'accès à l'origine. Cela permet d'économiser du temps et des efforts par rapport à la suppression d'un contrôle d'accès à l'origine de toutes les origines et distributions qui l'utilisent, une par une. Avec ce paramètre, il CloudFront ne signe aucune demande envoyée à l'origine du compartiment S3.

> **Warning**
>
> Pour utiliser ce paramètre, l'origine du compartiment S3 doit être accessible au public. Si vous utilisez ce paramètre avec une origine de compartiment S3 qui n'est pas accessible au public, vous CloudFront ne pouvez pas accéder à l'origine. L'origine du compartiment S3 renvoie les erreurs aux utilisateurs CloudFront et les CloudFront transmet aux utilisateurs.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et AWS CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront

transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour parcourir l'en-tête `Authorization` de la demande de l'utilisateur, vous devez ajouter l'en-tête `Authorization` à une stratégie de mise en cache pour tous les comportements de cache qui utilisent les origines du compartiment S3 associées à ce contrôle d'accès à l'origine.

Utiliser une identité d'accès d'origine (ancienne, non recommandée)

Présentation de l'identité d'accès à l'origine

CloudFront L'identité d'accès à l'origine (OAI) fournit des fonctionnalités similaires à celles du contrôle d'accès à l'origine (OAC), mais elle ne fonctionne pas dans tous les scénarios. C'est pourquoi nous vous recommandons d'utiliser OAC à la place. Plus précisément, l'OAI ne prend pas en charge :

- Tous les compartiments Amazon S3 Régions AWS, y compris les régions optionnelles
- Chiffrement côté serveur avec AWS KMS (SSE-KMS) Amazon S3
- Demandes dynamiques (`PUT`, `POST` ou `DELETE`) vers Amazon S3
- Nouveau Régions AWS lancé après décembre 2022

Pour plus d'informations sur la migration d'OAI vers OAC, consultez the section called “Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)”.

Autoriser une identité d'accès d'origine à lire des fichiers dans le compartiment Amazon S3

Lorsque vous créez un OAI ou que vous en ajoutez un à une distribution à l'aide de la CloudFront console, vous pouvez automatiquement mettre à jour la politique de compartiment Amazon S3 pour autoriser l'OAI à accéder à votre compartiment. Vous pouvez également choisir de créer ou de mettre à jour manuellement la politique de compartiment. Quelle que soit la méthode que vous utilisez, vous devez toujours vérifier les autorisations pour vous assurer que :

- Votre CloudFront OAI peut accéder aux fichiers du bucket pour le compte des utilisateurs qui les demandent. CloudFront

- Les utilisateurs ne peuvent pas utiliser les URL Amazon S3 pour accéder à vos fichiers en dehors de CloudFront.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transférer toutes les méthodes HTTP compatibles, CloudFront assurez-vous d'accorder à votre CloudFront OAI les autorisations souhaitées. Par exemple, si vous configurez CloudFront pour accepter et transférer les demandes qui utilisent cette `DELETE` méthode, configurez votre politique de compartiment de manière à gérer les `DELETE` demandes de manière appropriée afin que les utilisateurs puissent supprimer uniquement les fichiers que vous souhaitez qu'ils souhaitent.

Utiliser les politiques relatives aux compartiments Amazon S3

Vous pouvez accorder à un CloudFront OAI l'accès aux fichiers d'un compartiment Amazon S3 en créant ou en mettant à jour la politique de compartiment de la manière suivante :

- Utilisation de l'onglet Autorisations du compartiment Amazon S3 dans la console Amazon S3.
- Utilisation PutBucketPolicydans l'API Amazon S3.
- En utilisant la console CloudFront. Lorsque vous ajoutez un OAI à vos paramètres d'origine dans la CloudFront console, vous pouvez choisir Oui, mettre à jour la politique de compartiment pour indiquer de mettre CloudFront à jour la politique de compartiment en votre nom.

Si vous mettez à jour manuellement la politique de compartiment, assurez-vous que vous :

- Spécifiez l'identité d'accès à l'origine correcte comme `Principal` dans la politique.
- Accordez à l'identité d'accès à l'origine les autorisations dont elle a besoin pour accéder aux objets pour le compte des utilisateurs.

Pour plus d'informations, consultez les sections suivantes.

Spécification d'une OAI comme **`Principal`** dans une politique de compartiment

Pour spécifier une OAI comme `Principal` dans une politique de compartiment Amazon S3, utilisez l'Amazon Resource Name (ARN) qui inclut son ID. Par exemple :

```
"Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <origin
 access identity ID>"
}
```

Trouvez l'ID OAI dans la CloudFront console sous Security, Origin access, Identities (legacy). Vous pouvez également l'utiliser ListCloudFrontOriginAccessIdentitiesdans l' CloudFrontAPI.

Octroi d’autorisations à une OAI

Pour donner à l’identité d’accès à l’origine les autorisations pour accéder aux objets de votre compartiment Amazon S3, utilisez des actions dans la politique qui se rapportent à des opérations d’API Amazon S3 spécifiques. Par exemple, l'action `s3:GetObject` permet à l'identité d'accès à l'origine de lire des objets dans le compartiment. Pour plus d’informations, consultez les exemples de la section suivante ou la section Actions Amazon S3 du Guide de l’utilisateur Amazon Simple Storage Service.

Exemples de politique de compartiment Amazon S3

Les exemples suivants présentent les politiques de compartiment Amazon S3 qui permettent à CloudFront OAI d'accéder à un compartiment S3.

Trouvez l'ID OAI dans la CloudFront console sous Security, Origin access, Identities (legacy). Vous pouvez également l'utiliser ListCloudFrontOriginAccessIdentitiesdans l' CloudFrontAPI.

Example Politique de compartiment Amazon S3 qui donne à l’identité d’accès à l’origine un accès en lecture

L’exemple suivant permet à l’identité d’accès à l’origine de lire des objets dans le compartiment spécifié (`s3:GetObject`).

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
```

```
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Example Politique de compartiment Amazon S3 qui donne à l'identité d'accès à l'origine un accès en lecture et en écriture

L'exemple suivant permet à l'identité d'accès à l'origine de lire et d'écrire des objets dans le compartiment spécifié (`s3:GetObject` et `s3:PutObject`). Cela permet aux utilisateurs de télécharger des fichiers dans votre compartiment Amazon S3 via CloudFront.

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Utiliser les ACL d'objets Amazon S3 (non recommandé)

> **Important**
>
> Il est recommandé d'utiliser les politiques du compartiment Amazon S3 pour attribuer à une OAI l'accès à un compartiment S3. Vous pouvez utiliser des listes de contrôle d'accès (ACL) comme décrit dans cette section, mais nous le déconseillons.
> Amazon S3 recommande de définir S3 Object Ownership (Propriété de l'objet S3) sur bucket owner enforced (appliqué par le propriétaire du compartiment), ce qui signifie que les listes

ACL sont désactivées pour le compartiment et les objets à l'intérieur. Lorsque vous appliquez ce paramètre à Object Ownership (Propriété de l'objet), vous devez utiliser des politiques du compartiment pour donner l'accès à l'OAI (consultez la section précédente).
La section suivante concerne uniquement les cas d'utilisation hérités nécessitant des listes ACL.

Vous pouvez accorder à un CloudFront OAI l'accès aux fichiers d'un compartiment Amazon S3 en créant ou en mettant à jour l'ACL du fichier de la manière suivante :

- Utilisation de l'onglet Autorisations de l'objet Amazon S3 dans la console Amazon S3.
- Utilisation PutObjectAcldans l'API Amazon S3.

Lorsque vous accordez l'accès à une identité d'accès à l'origine à l'aide d'une liste ACL, vous devez spécifier l'identité d'accès à l'origine à l'aide de son ID d'utilisateur canonique Amazon S3. Dans la CloudFront console, vous pouvez trouver cet identifiant sous Sécurité, Accès à l'origine, Identités (ancienne). Si vous utilisez l' CloudFront API, utilisez la valeur de l'`S3CanonicalUserId`élément renvoyé lorsque vous avez créé l'OAI, ou appelez ListCloudFrontOriginAccessIdentitiesl' CloudFrontAPI.

Utiliser une identité d'accès d'origine dans les régions Amazon S3 qui prennent uniquement en charge l'authentification par signature version 4

Les régions Amazon S3 plus récentes requièrent que vous utilisiez Signature version 4 pour les demandes authentifiées. (Pour connaître les versions de signatures prises en charge dans chaque région Amazon S3, consultez la section Points de terminaison et quotas Amazon Simple Storage Service de la Références générales AWS.) Si vous utilisez une identité d'accès à l'origine et que votre compartiment se trouve dans l'une des régions qui nécessitent Signature version 4, notez les points suivants :

- Les demandes `DELETE`, `GET`, `HEAD`, `OPTIONS` et`PATCH` sont prises en charge sans qualifications.
- Les demandes `POST` ne sont pas prises en charge.

Restreindre l'accès aux équilibreurs de charge des applications

Dans le cas d'une application Web ou d'un autre contenu diffusé par un Application Load Balancer connecté à Internet CloudFront , Elastic Load Balancing peut mettre en cache des objets et les

diffuser directement aux utilisateurs (spectateurs), réduisant ainsi la charge sur votre Application Load Balancer. Un équilibreur de charge connecté à Internet possède un nom DNS pouvant être résolu publiquement et achemine les demandes des clients vers des cibles via Internet.

CloudFrontpeut également contribuer à réduire la latence et même à absorber certaines attaques par déni de service distribué (DDoS).

Toutefois, si les utilisateurs peuvent contourner CloudFront et accéder directement à votre Application Load Balancer, vous ne bénéficierez pas de ces avantages. Mais vous pouvez configurer Amazon CloudFront et votre Application Load Balancer pour empêcher les utilisateurs d'accéder directement à l'Application Load Balancer. Cela permet aux utilisateurs d'accéder à l'Application Load Balancer uniquement par le biais de celui-ci CloudFront, ce qui vous permet de bénéficier des avantages de son utilisation. CloudFront

Pour empêcher les utilisateurs d'accéder directement à un Application Load Balancer et n'autoriser l'accès que par ce biais CloudFront, procédez comme suit :

1. Configurez CloudFront pour ajouter un en-tête HTTP personnalisé aux demandes qu'il envoie à l'Application Load Balancer.
2. Configurez l'Application Load Balancer pour transférer uniquement les demandes contenant l'en-tête HTTP personnalisé.
3. (Facultatif) HTTPS est requis pour améliorer la sécurité de cette solution.

Pour plus d’informations, consultez les rubriques suivantes. Une fois ces étapes effectuées, les utilisateurs ne peuvent accéder à votre Application Load Balancer que via. CloudFront

Rubriques

Configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux demandes

Vous pouvez configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes qu'il envoie à votre origine (dans ce cas, un Application Load Balancer).

> **Important**
>
> Ce cas d'utilisation repose sur le fait de garder secrets le nom et la valeur de l'en-tête personnalisé. Si le nom et la valeur d'en-tête ne sont pas secrets, d'autres clients HTTP peuvent potentiellement les inclure dans les demandes qu'ils envoient directement à l'Application Load Balancer. Cela peut faire en sorte que l'Application Load Balancer se comporte comme si les demandes provenaient d'une CloudFront autre source. Pour éviter cela, gardez le nom et la valeur de l'en-tête personnalisé secrets.

Vous pouvez configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux demandes d'origine à l'aide de la CloudFront console ou de l' CloudFront API. AWS CloudFormation

Pour ajouter un en-tête HTTP personnalisé (CloudFront console)

Dans la CloudFront console, utilisez le paramètre Origin Custom Headers dans les paramètres d'Origin. Saisissez le nom de l'en-tête et sa valeur, comme illustré dans l'exemple suivant.

> **Note**
>
> Le nom et la valeur de l'en-tête dans cet exemple n’existent qu'à des fins de démonstration. En production, utilisez des valeurs générées aléatoirement. Traitez le nom et la valeur de l'en-tête en tant qu’informations d'identification sécurisées, comme un nom d'utilisateur et un mot de passe.

Vous pouvez modifier le paramètre Origin Custom Headers lorsque vous créez ou modifiez l'origine d'une CloudFront distribution existante, et lorsque vous créez une nouvelle distribution. Pour plus d'informations, consultez Mettre à jour une distribution et Créer une distribution.

Pour ajouter un en-tête HTTP personnalisé (AWS CloudFormation)

Dans un AWS CloudFormation modèle, utilisez la `OriginCustomHeaders` propriété, comme indiqué dans l'exemple suivant.

> **Note**
>
> Le nom et la valeur de l'en-tête dans cet exemple n'existent qu'à des fins de démonstration. En production, utilisez des valeurs générées aléatoirement. Traitez le nom et la valeur de l'en-tête en tant qu'informations d'identification sécurisées, comme un nom d'utilisateur et un mot de passe.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestDistribution:
    Type: 'AWS::CloudFront::Distribution'
    Properties:
      DistributionConfig:
        Origins:
          - DomainName: app-load-balancer.example.com
            Id: Example-ALB
            CustomOriginConfig:
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
               - HeaderName: X-Custom-Header
                 HeaderValue: random-value-1234567890
        Enabled: 'true'
        DefaultCacheBehavior:
          TargetOriginId: Example-ALB
          ViewerProtocolPolicy: allow-all
          CachePolicyId: 658327ea-f89d-4fab-a63d-7e88639e58f6
        PriceClass: PriceClass_All
        ViewerCertificate:
          CloudFrontDefaultCertificate: 'true'
```

Pour plus d'informations, consultez l'origine et les OriginCustomHeaderpropriétés dans le guide de AWS CloudFormation l'utilisateur.

Pour ajouter un en-tête HTTP personnalisé (CloudFront API)

Dans l' CloudFront API, utilisez l'`CustomHeaders`objet qu'il contient`Origin`. Pour plus d'informations, consultez CreateDistributionUpdateDistributionla référence des CloudFront API Amazon et la documentation de votre SDK ou de tout autre client d'API.

Il existe certains noms d'en-tête que vous ne pouvez pas spécifier en tant qu'en-têtes personnalisés d'origine. Pour plus d'informations, consultez En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine.

Configurer un Application Load Balancer pour transférer uniquement les demandes contenant un en-tête spécifique

Après avoir configuré CloudFront pour ajouter un en-tête HTTP personnalisé aux demandes qu'il envoie à votre Application Load Balancer (voir la section précédente), vous pouvez configurer l'équilibreur de charge pour ne transférer que les demandes contenant cet en-tête personnalisé. Pour ce faire, ajoutez une nouvelle règle et modifiez la règle par défaut dans l'écouteur de votre équilibreur de charge.

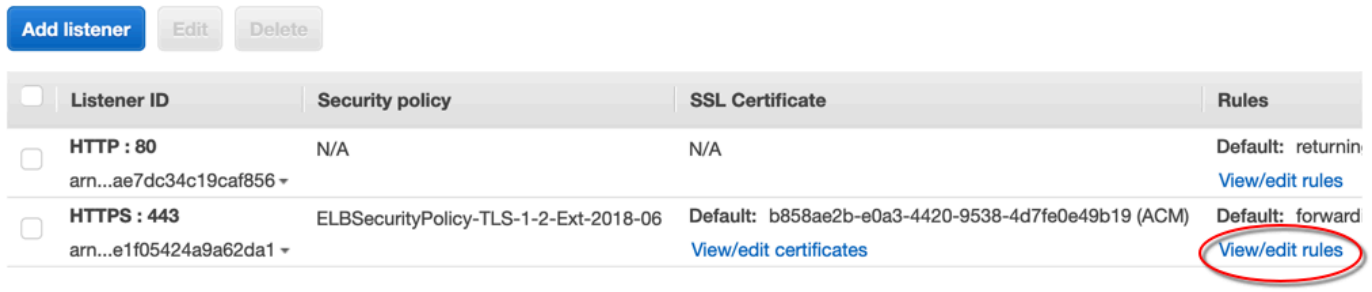
Prérequis

Pour utiliser les procédures suivantes, vous avez besoin d'un Application Load Balancer avec au moins un écouteur. Si vous n'en avez pas encore créé, reportez-vous à la section Créer un Application Load Balancer dans le guide de l'utilisateur pour les Application Load Balancers.

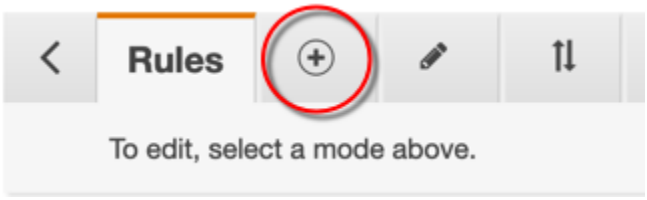
Les procédures suivantes modifient un écouteur HTTPS. Vous pouvez utiliser le même processus pour modifier un écouteur HTTP.

Pour mettre à jour les règles dans un écouteur d'Application Load Balancer

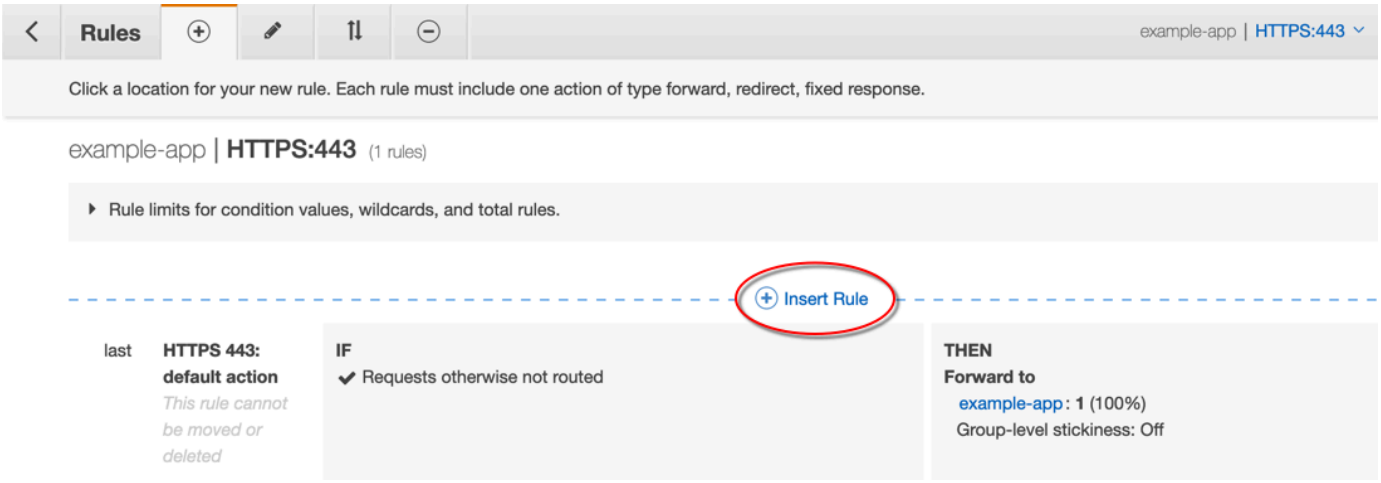
1. Ouvrez la pageÉquilibreurs de chargedans la console Amazon EC2.
2. Choisissez l'équilibreur de charge à l'origine de votre CloudFront distribution, puis cliquez sur l'onglet Listeners.
3. Pour l'écouteur que vous modifiez, choisissez Afficher/Modifier les règles.



4. Choisissez l'icône pour ajouter des règles.



5. Choisissez Insert Rule.

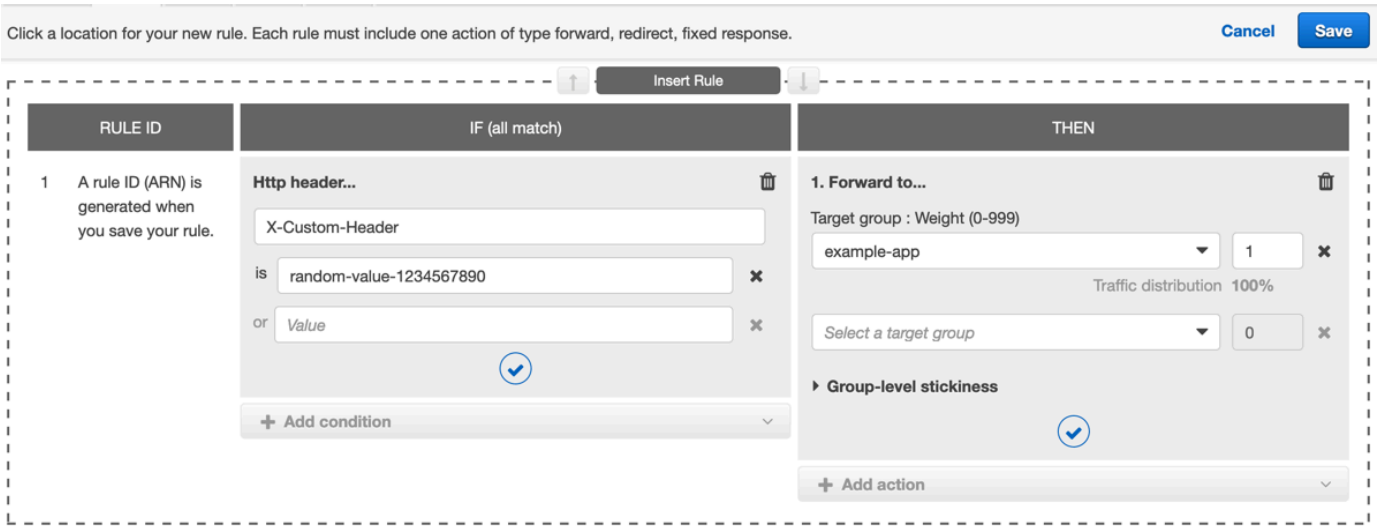


6. Pour la nouvelle règle, procédez comme suit :

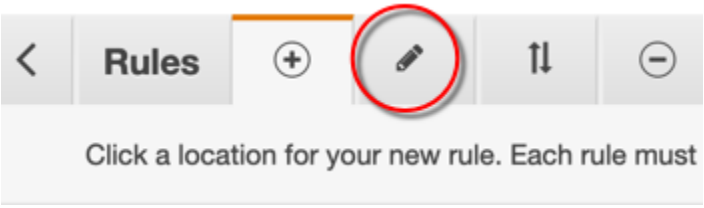
   a. Choisissez Ajouter une condition, puis En-tête Http. Spécifiez le nom et la valeur de l'en-tête HTTP que vous avez ajoutés en tant qu'en-tête personnalisé d'origine CloudFront.

   b. Choisissez Ajouter une action, puis Transférer à. Choisissez le groupe cible dans lequel vous souhaitez transférer les demandes.

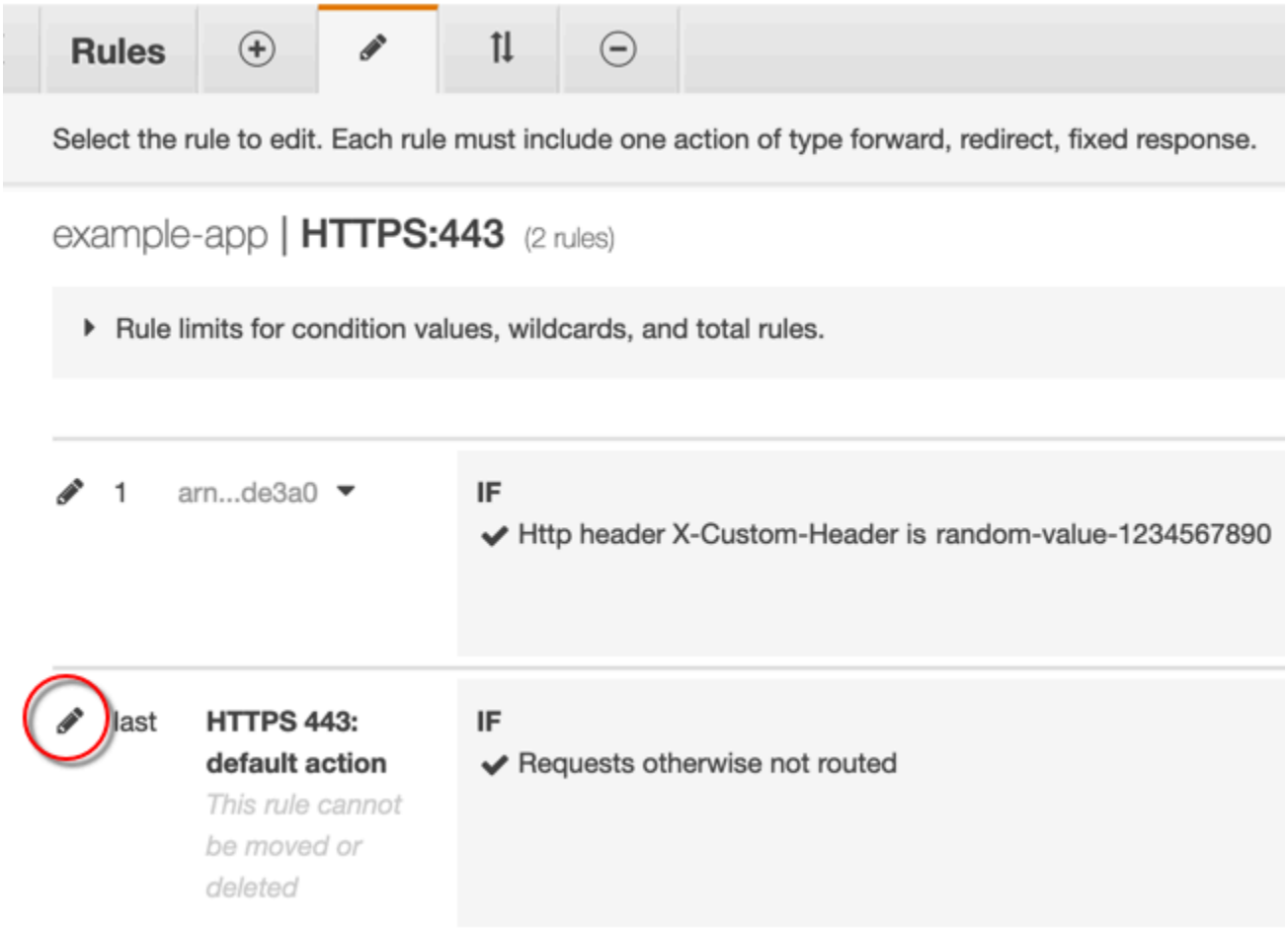
   c. Choisissez Enregistrer pour créer la nouvelle règle.



7. Choisissez l'icône pour modifier les règles.



8. Choisissez l'icône de modification de la règle par défaut.



9. Pour la règle par défaut, procédez comme suit :

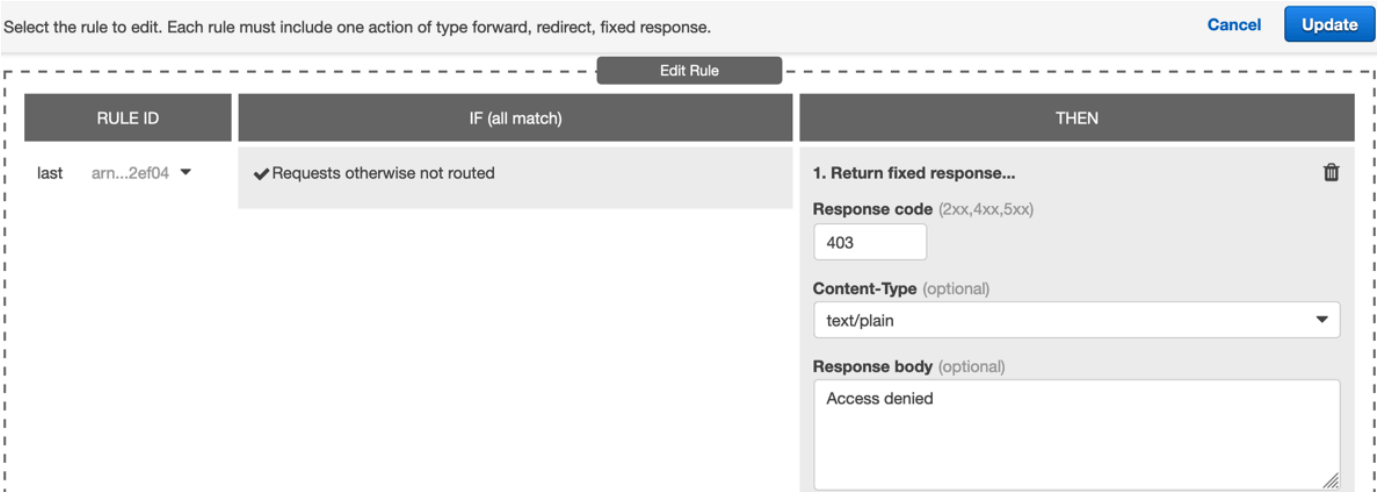
   a. Supprimez l'action par défaut.

   b. Choisissez Ajouter une action, puis Renvoyer une réponse fixe.

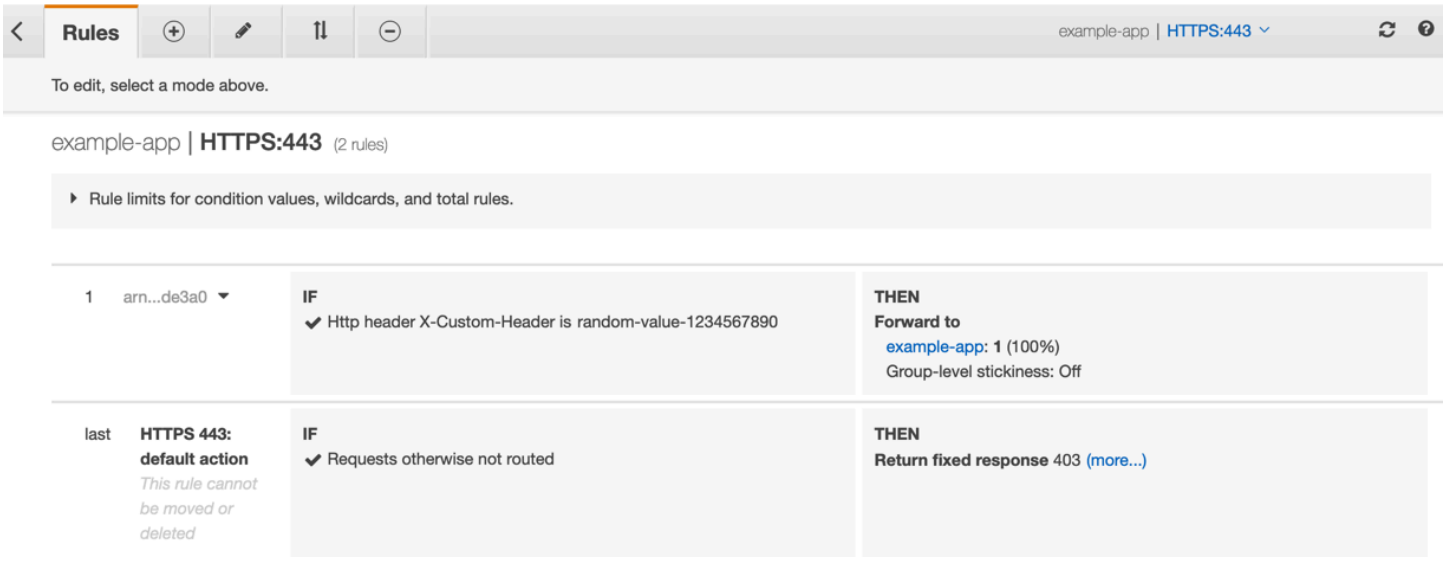
   c. Pour le Code de réponse, saisissez **`403`**.

   d. Pour Corps de réponse, saisissez **`Access denied`**.

   e. Choisissez Mettre à jour pour mettre à jour la règle par défaut.



Après avoir terminé ces étapes, votre écouteur d'équilibreur de charge dispose de deux règles, comme illustré dans l'image suivante. La première règle transmet les demandes contenant l'en-tête HTTP (demandes provenant de CloudFront). La deuxième règle envoie une réponse fixe à toutes les autres demandes (demandes qui ne proviennent pas de CloudFront).



Vous pouvez vérifier que la solution fonctionne en envoyant une demande à votre CloudFront distribution et une autre à votre Application Load Balancer. La demande de CloudFront renvoi de votre application Web ou de votre contenu, et celle envoyée directement à votre Application Load Balancer, renvoient une `403` réponse avec le message en texte brut. `Access denied`

(Facultatif) Améliorer la sécurité de cette solution

Pour améliorer la sécurité de cette solution, vous pouvez configurer votre CloudFront distribution pour qu'elle utilise toujours le protocole HTTPS lorsque vous envoyez des demandes à votre Application Load Balancer. N'oubliez pas que cette solution ne fonctionne que si vous gardez le nom et la valeur de l'en-tête personnalisé secrètes. L'utilisation de HTTPS peut aider à empêcher un compte-écoute de découvrir le nom et la valeur de l'en-tête. Nous vous recommandons également de faire changer périodiquement le nom et la valeur de l'en-tête.

Utiliser HTTPS pour les demandes d'origine

CloudFront Pour configurer l'utilisation du protocole HTTPS pour les demandes d'origine, définissez le paramètre Origin Protocol Policy sur HTTPS uniquement. Ce paramètre est disponible dans la CloudFront console et dans l' CloudFront API. AWS CloudFormation Pour plus d'informations, consultez Protocole (origines personnalisées uniquement).

Ce qui suit s'applique également lorsque vous configurez CloudFront l'utilisation du protocole HTTPS pour les demandes d'origine :

- Vous devez configurer CloudFront pour transmettre l'`Host`en-tête à l'origine avec la politique de demande d'origine. Vous pouvez utiliser la politique de AllViewer gestion des demandes d'origine.
- Assurez-vous que votre Application Load Balancer possède un écouteur HTTPS (comme indiqué dans la section précédente). Pour plus d'informations, consultez la section Création d'un écouteur HTTPS dans le guide de l'utilisateur pour les Application Load Balancers. L'utilisation d'un écouteur HTTPS nécessite que vous disposiez d'un certificat SSL/TLS correspondant au nom de domaine qui est acheminé vers votre Application Load Balancer.
- Les certificats SSL/TLS pour ne CloudFront peuvent être demandés (ou importés) que `us-east-1` Région AWS dans AWS Certificate Manager (ACM). Comme il CloudFront s'agit d'un service mondial, il distribue automatiquement le certificat de la `us-east-1` région à toutes les régions associées à votre CloudFront distribution.
  - Par exemple, si vous avez un Application Load Balancer (ALB) dans la `ap-southeast-2` région, vous devez configurer les certificats SSL/TLS à la fois dans la `ap-southeast-2` région (pour utiliser le protocole HTTPS entre CloudFront et l'origine de l'ALB) et dans la `us-east-1` région (pour utiliser le protocole HTTPS entre les utilisateurs et). CloudFront Les deux certificats doivent correspondre au nom de domaine qui est acheminé vers votre Application Load Balancer. Pour plus d'informations, consultez Région AWS pour AWS Certificate Manager.

- Si les utilisateurs finaux (également appelés spectateurs ou clients) de votre application Web peuvent utiliser le protocole HTTPS, vous pouvez également le configurer de manière CloudFront à préférer (voire à exiger) des connexions HTTPS de la part des utilisateurs finaux. Pour ce faire, utilisez le paramètre Stratégie de protocole d'utilisateur. Vous pouvez le définir pour rediriger les utilisateurs finaux de HTTP vers HTTPS ou pour rejeter les demandes utilisant HTTP. Ce paramètre est disponible dans la CloudFront console et dans l' CloudFront API. AWS CloudFormation Pour plus d'informations, consultez Viewer Protocol Policy.

Changer le nom et la valeur de l'en-tête

En plus d'utiliser HTTPS, nous vous recommandons également de changer périodiquement le nom et la valeur de l'en-tête. Les étapes de haut niveau pour ce faire sont les suivantes :

1. Configurez CloudFront pour ajouter un en-tête HTTP personnalisé supplémentaire aux demandes qu'il envoie à l'Application Load Balancer.
2. Mettez à jour la règle de l'écouteur de l'Application Load Balancer pour transférer les demandes contenant cet en-tête HTTP personnalisé supplémentaire.
3. Configurez CloudFront pour arrêter d'ajouter l'en-tête HTTP personnalisé d'origine aux demandes qu'il envoie à l'Application Load Balancer.
4. Mettez à jour la règle de l'écouteur de l'Application Load Balancer pour arrêter le transfert des demandes contenant l'en-tête HTTP personnalisé d'origine.

Pour plus d'informations sur la réalisation de ces étapes, consultez les sections précédentes.

(Facultatif) Limitez l'accès à l'origine en utilisant la liste de AWS préfixes -managed pour CloudFront

Pour restreindre davantage l'accès à votre Application Load Balancer, vous pouvez configurer le groupe de sécurité associé à l'Application Load Balancer de manière à ce qu'il n'accepte que le trafic CloudFront provenant de pays où le service utilise AWS une liste de préfixes gérée. Cela empêche le trafic qui ne CloudFront provient pas d'atteindre votre Application Load Balancer au niveau de la couche réseau (couche 3) ou de la couche transport (couche 4).

Pour plus d'informations, consultez le billet de CloudFront blog « Limiter l'accès à vos origines à l'aide de la liste de préfixes AWS-managed » pour Amazon.

Limitez la distribution géographique de votre contenu

Vous pouvez utiliser des restrictions géographiques, parfois appelées blocage géographique, pour empêcher les utilisateurs de zones géographiques spécifiques d'accéder au contenu que vous distribuez via une CloudFront distribution Amazon. Pour utiliser les restrictions géographiques, vous avez deux options :

- Utilisez la fonction de restrictions CloudFront géographiques. Choisissez cette option pour limiter l'accès à tous les fichiers associés à une distribution et pour limiter l'accès au niveau du pays.
- Utiliser un service de géolocalisation tiers. Utilisez cette option pour limiter l'accès à un sous-ensemble des fichiers associés à une distribution ou pour le limiter à un niveau de détail plus fin que le niveau pays.

Rubriques

Utiliser les restrictions CloudFront géographiques

Lorsqu'un utilisateur demande votre contenu, il diffuse CloudFront généralement le contenu demandé, quel que soit l'endroit où se trouve l'utilisateur. Si vous devez empêcher les utilisateurs de certains pays d'accéder à votre contenu, vous pouvez utiliser la fonctionnalité de restrictions CloudFront géographiques pour effectuer l'une des opérations suivantes :

- Accorder à vos utilisateurs l'autorisation d'accéder à votre contenu seulement s'ils résident dans un des pays figurant dans la liste des pays autorisés.
- Empêcher vos utilisateurs d'accéder à votre contenu s'ils résident dans un des pays interdits de la liste d'exclusion.

Par exemple, si une demande provient d'un pays dans lequel vous n'êtes pas autorisé à diffuser votre contenu, vous pouvez utiliser des restrictions CloudFront géographiques pour bloquer la demande.

> **Note**
>
> CloudFront détermine l'emplacement de vos utilisateurs à l'aide d'une base de données tierce. La précision de la correspondance entre les adresses IP et les pays varie selon la

région. Selon des tests récents, la précision globale est de 99,8 %. S'il n'est pas CloudFront possible de déterminer l'emplacement d'un utilisateur, CloudFront diffuse le contenu demandé par l'utilisateur.

Les restrictions géographiques fonctionnent comme suit :

1. Imaginons que vous n'ayez le droit de distribuer votre contenu qu'au Liechtenstein. Vous mettez à jour votre CloudFront distribution pour ajouter une liste d'autorisation contenant uniquement le Liechtenstein. (Vous pouvez, à la place, ajouter une liste d'exclusion contenant tous les pays, à l'exception du Liechtenstein.)
2. Un utilisateur monégasque demande votre contenu, et le DNS achemine la demande vers un emplacement CloudFront périphérique à Milan, en Italie.
3. L'emplacement périphérique de Milan recherche votre distribution et détermine que l'utilisateur de Monaco n'a pas l'autorisation de télécharger votre contenu.
4. CloudFront renvoie un code d'état HTTP `403 (Forbidden)` à l'utilisateur.

Vous pouvez éventuellement configurer CloudFront pour renvoyer un message d'erreur personnalisé à l'utilisateur, et vous pouvez spécifier la durée pendant laquelle vous souhaitez CloudFront mettre en cache la réponse d'erreur pour le fichier demandé. La valeur par défaut est de 10 secondes. Pour plus d'informations, consultez Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques.

Les restrictions géographiques s'appliquent à la totalité d'une distribution. Si vous devez appliquer une restriction à une partie de votre contenu et une restriction différente (ou aucune restriction) à une autre partie de votre contenu, vous devez créer des CloudFront distributions distinctes ou utiliser un service de géolocalisation tiers.

Si vous activez les journaux CloudFront standard (journaux d'accès), vous pouvez identifier les demandes CloudFront rejetées en recherchant les entrées de journal contenant la valeur de `sc-status` (le code d'état HTTP)`403`. Cependant, en utilisant uniquement les journaux standard, vous ne pouvez pas distinguer une demande CloudFront rejetée en fonction de l'emplacement de l'utilisateur d'une demande CloudFront rejetée parce que l'utilisateur n'était pas autorisé à accéder au fichier pour une autre raison. Si vous disposez d'un service de géolocalisation tiers tel que Digital Element or MaxMind, vous pouvez identifier l'emplacement des demandes en fonction de l'adresse IP figurant dans la colonne `c-ip` (IP du client) des journaux d'accès. Pour plus d'informations sur les

journaux CloudFront standard, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

La procédure suivante explique comment utiliser la CloudFront console pour ajouter des restrictions géographiques à une distribution existante. Pour plus d'informations sur l'utilisation de la console pour créer une distribution, consultez Créer une distribution.

Pour ajouter des restrictions géographiques à votre distribution CloudFront Web (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez mettre à jour.
3. Choisissez l'onglet Sécurité, puis sélectionnez Restrictions géographiques.
4. Choisissez Modifier.
5. Sélectionnez Allow list (Liste verte) pour créer une liste des pays autorisés, ou Liste rouge pour créer une liste des pays interdits.
6. Ajoutez les pays souhaités à la liste, puis choisissez Save changes (Enregistrer les modifications).

Utiliser un service de géolocalisation tiers

Grâce à la fonctionnalité de restrictions CloudFront géographiques, vous contrôlez la distribution de votre contenu au niveau du pays pour tous les fichiers que vous distribuez dans le cadre d'une distribution Web donnée. Si vous avez un cas d'utilisation pour des restrictions géographiques où les restrictions ne suivent pas les frontières nationales, ou si vous souhaitez restreindre l'accès à certains des fichiers que vous diffusez par une distribution donnée, vous pouvez combiner l'utilisation CloudFront d'un service de géolocalisation tiers. Vous pouvez ainsi contrôler l'accès à votre contenu en fonction non seulement du pays, mais aussi de la ville ou du code postal, voire de la latitude et de la longitude.

Lorsque vous utilisez un service de géolocalisation tiers, nous vous recommandons d'utiliser des URL CloudFront signées, avec lesquelles vous pouvez spécifier une date et une heure d'expiration après lesquelles l'URL n'est plus valide. En outre, nous vous recommandons d'utiliser un compartiment Amazon S3 comme origine, car vous pouvez ensuite utiliser un contrôle CloudFront d'accès à l'origine pour empêcher les utilisateurs d'accéder à votre contenu directement depuis l'origine. Pour

plus d'informations sur les URL signées et les contrôles d'accès à l'origine, consultez Diffusez du contenu privé avec des URL signées et des cookies signés.

Les étapes ci-après expliquent comment contrôler l'accès à vos fichiers à l'aide d'un service de géolocalisation tiers.

Utiliser un service de géolocalisation tiers pour restreindre l'accès aux fichiers d'une distribution CloudFront

1. Obtenez un compte avec un service de géolocalisation.
2. Chargez votre contenu sur un compartiment Amazon S3.
3. Configurez Amazon CloudFront et Amazon S3 pour diffuser du contenu privé. Pour plus d'informations, consultez Diffusez du contenu privé avec des URL signées et des cookies signés.
4. Ecrivez votre application web pour exécuter ce qui suit :

   - Envoyez l'adresse IP de chaque demande utilisateur au service de géolocalisation.
   - Évaluez la valeur renvoyée par le service de géolocalisation pour déterminer si l'utilisateur se trouve dans un endroit où vous CloudFront souhaitez diffuser votre contenu.
   - Si vous souhaitez distribuer votre contenu à l'adresse de l'utilisateur, générez une URL signée pour votre CloudFront contenu. Si vous ne souhaitez pas distribuer de contenu à cet emplacement, renvoyez le code d'état HTTP `403 (Forbidden)` à l'utilisateur. Vous pouvez également configurer CloudFront pour renvoyer un message d'erreur personnalisé. Pour plus d'informations, consultez the section called "Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques".

   Pour plus d'informations, consultez la documentation du service de géolocalisation que vous utilisez.

Vous pouvez utiliser une variable de serveur web pour obtenir les adresses IP des utilisateurs qui visitent votre site web. Notez les avertissements suivants :

- Si votre serveur web n'est pas connecté à Internet via un équilibreur de charge, vous pouvez utiliser une variable de serveur web pour obtenir l'adresse IP distante. Toutefois, cette adresse IP n'est pas toujours l'adresse IP de l'utilisateur. Il peut également s'agir de l'adresse IP d'un serveur proxy, selon la façon dont l'utilisateur est connecté à Internet.

- Si votre serveur web est connecté à Internet via un équilibreur de charge, une variable de serveur web peut contenir l'adresse IP de l'équilibreur de charge, et non celle de l'utilisateur. Dans cette configuration, nous vous recommandons d'utiliser la dernière adresse IP de l'en-tête HTTP `X-Forwarded-For`. Cet en-tête contient généralement plusieurs adresses IP, la plupart concernant des proxys ou des équilibreurs de charge. La dernière adresse IP de la liste est celle qui est très vraisemblablement associée à l'emplacement géographique de l'utilisateur.

Si votre serveur web n'est pas connecté à un équilibreur de charge, nous vous recommandons d'utiliser les variables de serveur web à la place de l'en-tête `X-Forwarded-For` pour éviter l'usurpation d'adresse IP.

Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles

Amazon CloudFront vous permet de sécuriser les end-to-end connexions aux serveurs d'origine en utilisant le protocole HTTPS. Le chiffrement au niveau du champ ajoute une couche de sécurité, qui vous permet de protéger des données spécifiques tout au long du traitement du système, pour que seules certaines applications puissent les voir.

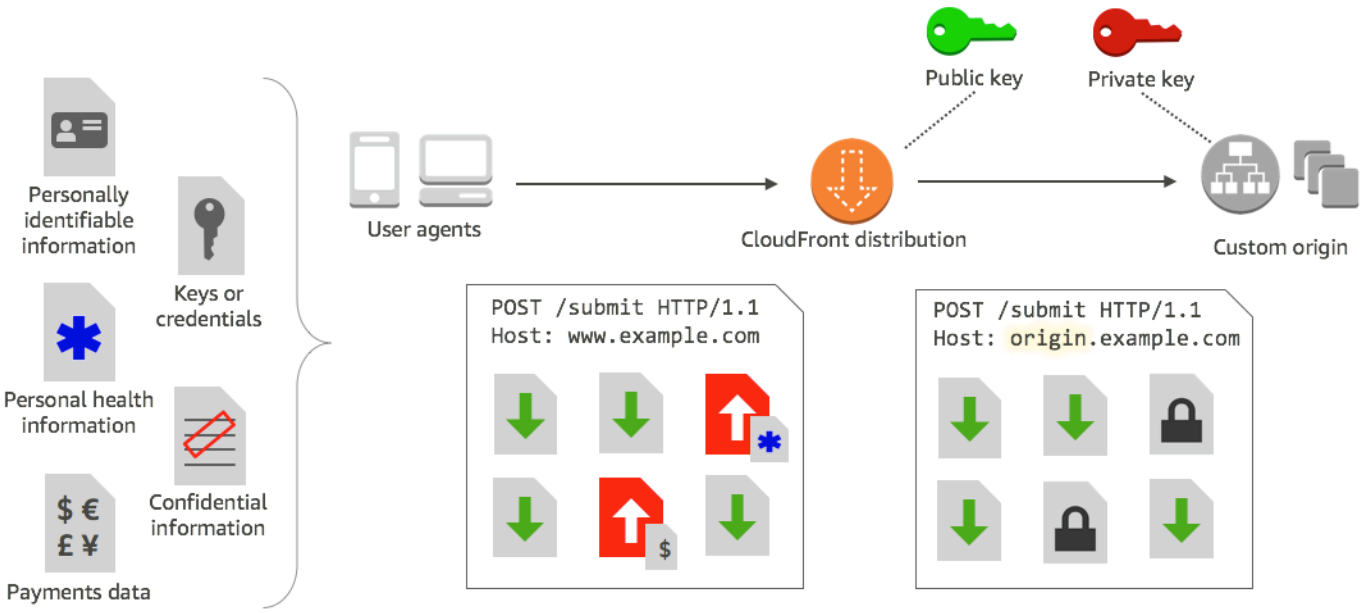
Grâce au chiffrement au niveau du champ, vous pouvez permettre à vos utilisateurs de charger de manière sécurisée des informations sensibles envoyées à vos serveurs web. Les informations sensibles fournies par vos utilisateurs sont chiffrées à la périphérie, à proximité de l'utilisateur, et restent chiffrées tout le long de votre pile d'applications. Ce chiffrement garantit que seules les applications qui ont besoin des données (et qui disposent des informations d'identification pour les déchiffrer) sont en mesure de le faire.

Pour utiliser le chiffrement au niveau des champs, lorsque vous configurez votre CloudFront distribution, spécifiez l'ensemble de champs que vous souhaitez chiffrer dans les requêtes POST, ainsi que la clé publique à utiliser pour les chiffrer. Vous pouvez chiffrer jusqu'à 10 champs de données dans une requête. (Vous ne pouvez pas chiffrer toutes les données dans une requête avec chiffrement au niveau du champ ; vous devez spécifier des champs individuels à chiffrer).

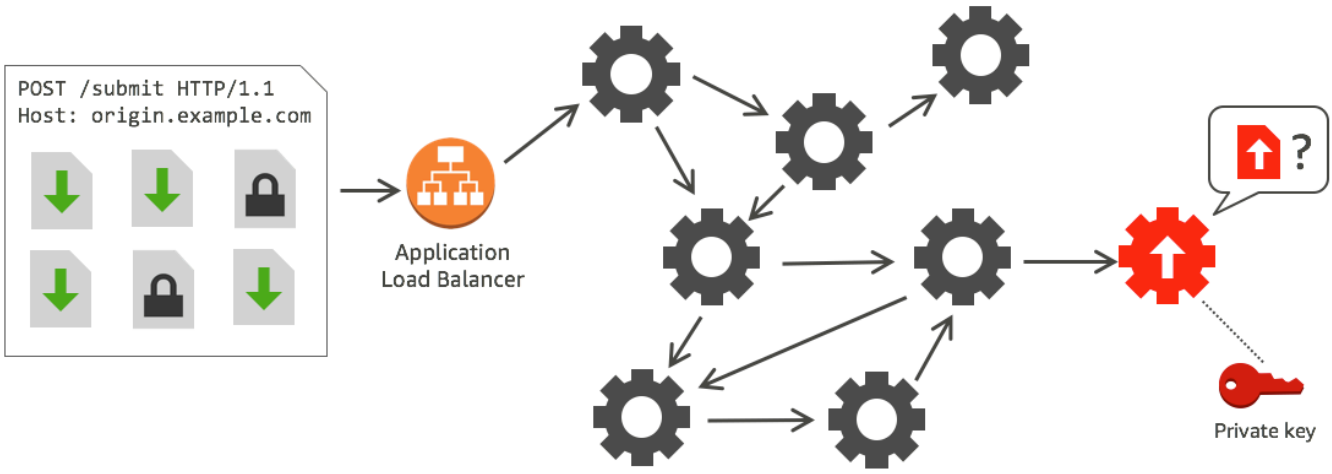
Lorsque la requête HTTPS avec chiffrement au niveau du champ est réacheminée vers l'origine, et que la requête est acheminée dans votre application ou sous-système d'origine, les données sensibles sont toujours chiffrées, ce qui réduit le risque de violation ou de perte accidentelle des données sensibles. Les composants devant accéder aux données sensibles pour des raisons

professionnelles, comme un système de traitement de paiement qui aurait besoin d'accéder à un numéro de crédit, peuvent utiliser la clé privée adéquate pour déchiffrer les données et y accéder.

> **Note**
>
> Pour utiliser le chiffrement au niveau du champ, votre origine doit prendre en charge l'encodage segmenté.



CloudFront le chiffrement au niveau du champ utilise le chiffrement asymétrique, également appelé chiffrement à clé publique. Vous fournissez une clé publique à CloudFront, et toutes les données sensibles que vous spécifiez sont cryptées automatiquement. La clé que vous fournissez CloudFront ne peut pas être utilisée pour déchiffrer les valeurs chiffrées ; seule votre clé privée peut le faire.



Rubriques

- Présentation du chiffrement au niveau du champ
- Configurer le chiffrement au niveau des champs
- Déchiffrez les champs de données à votre origine

Présentation du chiffrement au niveau du champ

Les étapes suivantes présentent la configuration de chiffrement au niveau du champ. Pour connaître les étapes spécifiques, consultez Configurer le chiffrement au niveau des champs.

1. Obtenez une paire de clés publique/clé privée. Vous devez obtenir et ajouter la clé publique avant de commencer à configurer le chiffrement au niveau des champs dans. CloudFront
2. Créez un profil de chiffrement au niveau du champs. Les profils de chiffrement au niveau des champs, que vous créez dans CloudFront, définissent les champs que vous souhaitez chiffrer.
3. Créez une configuration de chiffrement au niveau du champ. Une configuration spécifie les profils à utiliser selon le type de contenu de la requête ou un argument de requête pour chiffrer des champs de données spécifiques. Vous pouvez également choisir les options de comportement de transfert de demande que vous souhaitées pour différents scénarios. Par exemple, vous pouvez définir le comportement lorsque le nom de profil spécifié par l'argument de requête dans une URL de demande n'existe pas dans CloudFront.
4. Lien vers un comportement de cache. Liez la configuration à un comportement de cache pour une distribution, afin de spécifier à quel moment les données CloudFront doivent être cryptées.

Configurer le chiffrement au niveau des champs

Suivez ces étapes pour commencer à utiliser le chiffrement au niveau du champ. Pour en savoir plus sur les quotas (auparavant appelés limites) liés au chiffrement au niveau du champ, consultez Quotas.

Étape 1 : créer une paire de clés RSA

Pour commencer, vous devez créer une paire de clés RSA qui inclut une clé publique et une clé privée. La clé publique permet CloudFront de chiffrer les données, et la clé privée permet aux composants de votre origine de déchiffrer les champs qui ont été chiffrés. Vous pouvez utiliser OpenSSL ou un autre outil pour créer une paire de clés. La taille de la clé doit être de 2 048 bits.

Par exemple, si vous utilisez OpenSSL, vous pouvez exécuter la commande suivante pour générer une paire de clés avec une longueur de 2048 bits et l'enregistrer dans le fichier `private_key.pem`:

```
openssl genrsa -out private_key.pem 2048
```

Le fichier obtenu contient à la fois la clé publique et la clé privée. Pour extraire la clé publique de ce fichier, exécutez la commande suivante :

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Le fichier de clé publique (`public_key.pem`) contient la valeur de clé codée que vous collez à l'étape suivante.

Étape 2 : Ajoutez votre clé publique à CloudFront

Après avoir obtenu votre paire de clés RSA, ajoutez votre clé publique à CloudFront.

Pour ajouter votre clé publique à CloudFront (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Clé publique.
3. Choisissez Ajouter une clé publique.
4. Dans Nom de clé, tapez un nom unique pour la clé. Le nom ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.
5. Pour Key value (Valeur de clé), collez la valeur de clé encodée pour votre clé publique, y compris les lignes `-----BEGIN PUBLIC KEY-----` et `-----END PUBLIC KEY-----`.
6. Pour Commentaire, ajoutez un commentaire facultatif. Par exemple, vous pouvez inclure la date d'expiration pour la clé publique.
7. Choisissez Ajouter.

Vous pouvez ajouter d'autres clés à utiliser CloudFront en répétant les étapes de la procédure.

Étape 3 : créer un profil de chiffrement au niveau du champ

Après avoir ajouté au moins une clé publique CloudFront, créez un profil CloudFront indiquant les champs à chiffrer.

Créer un profil de chiffrement au niveau du champ (console)

1. Dans le volet de navigation, sélectionnez Chiffrement au niveau du champ.
2. Choisissez Créer un profil.
3. Remplissez les champs suivants :

   Profile name (Nom du profil)

   Saisissez un nom unique pour le profil. Le nom ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.

Nom de clé publique

Dans la liste déroulante, choisissez le nom d'une clé publique que vous avez ajoutée CloudFront à l'étape 2. CloudFront utilise la clé pour chiffrer les champs que vous spécifiez dans ce profil.

Nom du fournisseur

Saisissez une phrase facilitant l'identification de la clé, comme le fournisseur de la paire de clés. Ces informations, tout comme la clé privée, sont nécessaires lors du déchiffrement des champs de données par les applications. Le nom du fournisseur ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des deux-points (:), des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.

Modèle de nom de champ

Tapez les noms des champs de données, ou des modèles identifiant les noms des champs de données dans la demande, que vous CloudFront souhaitez chiffrer. Sélectionnez l'option + pour ajouter tous les champs que vous souhaitez chiffrer avec cette clé.

Pour le modèle de nom de champ, vous pouvez taper le nom complet du champ de données DateOfBirth, par exemple, ou simplement la première partie du nom avec un caractère générique (*), comme CreditCard *. Le modèle de champ de nom ne peut contenir que des caractères alphanumériques, des crochets ([et]), des points (.), des traits de soulignement (_) et des tirets (-) et en option, le métacaractère (*).

N'utilisez pas de caractères qui se chevauchent pour différents modèles de nom de champ. Par exemple, si vous avez un modèle de nom de champ ABC*, vous ne pouvez pas ajouter un autre modèle de nom de champ AB*. De plus, les noms de champ sont sensibles à la casse et le nombre maximum de caractères ne doit pas dépasser 128.

Commentaire

(Facultatif) Saisissez un commentaire sur ce profil. Le nombre maximum de caractères à utiliser est de 128.

4. Une fois les champs remplis, choisissez Créer un profil.
5. Pour ajouter d'autres profils, Sélectionnez Ajouter un profil.

Étape 4 : créer une configuration

Après avoir créé un ou plusieurs profils de chiffrement au niveau des champs, créez une configuration qui spécifie le type de contenu de la demande qui inclut les données à chiffrer, le profil à utiliser pour le chiffrement et les autres options qui spécifient la manière dont vous CloudFront souhaitez gérer le chiffrement.

Par exemple, lorsque vous ne CloudFront pouvez pas chiffrer les données, vous pouvez spécifier si vous CloudFront devez bloquer ou transférer une demande à votre origine dans les scénarios suivants :

- Lorsque le type de contenu d'une demande ne figure pas dans une configuration : si vous n'avez pas ajouté de type de contenu à une configuration, vous pouvez spécifier si vous CloudFront devez transmettre la demande contenant ce type de contenu à l'origine sans chiffrer les champs de données, ou bloquer la demande et renvoyer une erreur.

  > **Note**
  >
  > Si vous ajoutez un type de contenu à une configuration mais que vous n'avez pas spécifié de profil à utiliser avec ce type de contenu, CloudFront transférez toujours les demandes contenant ce type de contenu à l'origine.

- Lorsque le nom de profil fourni dans un argument de requête est inconnu : lorsque vous spécifiez à l'argument de `fle-profile` requête un nom de profil qui n'existe pas pour votre distribution, vous pouvez spécifier si vous CloudFront devez envoyer la demande à l'origine sans chiffrer les champs de données ou bloquer la demande et renvoyer une erreur.

Dans une configuration, vous pouvez également spécifier si fournir un profil en tant qu'argument de requête dans une URL substitue un profil que vous avez mappé vers le type de contenu de cette requête. Par défaut, CloudFront utilise le profil que vous avez mappé à un type de contenu, si vous en spécifiez un. Cela vous permet d'avoir un profil utilisé par défaut, mais de décider, pour certaines requêtes, d'appliquer un autre profil.

Donc, par exemple, vous pouvez spécifier (dans votre configuration) **`SampleProfile`** comme profil d'argument de requête à utiliser. Vous pouvez ensuite utiliser l'URL à la `https://d1234.cloudfront.net?fle-profile=SampleProfile` place de`https://d1234.cloudfront.net`, **`SampleProfile`** pour CloudFront utiliser cette demande, au lieu du profil que vous avez configuré pour le type de contenu de la demande.

Vous pouvez créer jusqu'à 10 configurations pour un seul compte, puis associer l'une des configurations au comportement de cache d'une distribution pour le compte.

Créer une configuration de chiffrement au niveau du champ (console)

1. Sur la page Chiffrement au niveau du champ, sélectionnez Créer la configuration.

   Remarque : Si vous n'avez pas créé de profil, vous ne verrez pas l'option permettant de créer une configuration.
2. Renseignez les champs suivants pour spécifier le profil à utiliser. (Certains champs ne peuvent être modifiés).

   Type de contenu (non modifiable)

   Le type de contenu est défini comme `application/x-www-form-urlencoded` et ne peut être modifié.

   ID de profil par défaut (facultatif)

   Dans la liste déroulante, sélectionnez le profil que vous souhaitez mapper au type de contenu dans le champ Type de contenu.

   Format de contenu (non modifiable)

   Le format du contenu est défini comme `URLencoded` et ne peut être modifié.
3. Si vous souhaitez modifier le comportement CloudFront par défaut des options suivantes, cochez la case appropriée.

   Réacheminer une requête vers l'origine lorsque le type de contenu de a requête n'est pas configuré

   Sélectionnez la case à cocher pour permettre à la requête d'atteindre votre origine si vous n'avez pas spécifié de profil à utiliser pour le type de contenu de la requête.

   Substituer le profil d'un type de contenu avec un argument de requête fourni

   Sélectionnez la case à cocher pour autoriser un profil fourni dans un argument de requête à substituer le profil que vous avez spécifié pour un type de contenu.
4. Si vous sélectionnez la case à cocher pour autoriser un argument de requête à remplacer le profil par défaut, vous devez renseigner les champs supplémentaires suivants pour la configuration. Vous pouvez créer jusqu'à cinq de ces mappages d'argument de requête à utiliser avec les requêtes.

Argument de requête

Saisissez la valeur que vous voulez inclure dans l'URL pour l'argument de requête de `fle-profile`. Cette valeur indique CloudFront d'utiliser l'ID de profil (que vous spécifiez dans le champ suivant) associé à cet argument de requête pour le chiffrement au niveau du champ pour cette requête.

Le nombre maximum de caractères à utiliser est de 128. La valeur ne doit pas contenir d'espaces et ne comporter que des caractères alphanumériques ou les caractères suivants : tiret (-), point (.), trait de soulignement (_), astérisque (*), signe plus (+), pourcentage (%).

ID de profil

Dans la liste déroulante, sélectionnez le profil à associer à la valeur que vous avez saisie pour Argument de requête.

Réacheminer une requête vers l'origine lorsque le profil spécifié dans un argument de requête n'existe pas

Cochez la case si vous souhaitez autoriser la demande à atteindre votre origine si le profil spécifié dans un argument de requête n'est pas défini dans CloudFront.

Étape 5 : ajouter une configuration à un comportement de cache

Pour utiliser le chiffrement au niveau du champ, associez une configuration à un comportement de cache pour une distribution en ajoutant l'ID de configuration en tant que valeur pour votre distribution.

Important

Pour associer une configuration de chiffrement au niveau du champ à un comportement de cache, la distribution doit être configurée pour toujours utiliser HTTPS et accepter des demandes HTTP `POST` et `PUT` des utilisateurs. Ainsi, les conditions suivantes doivent être vraies :

- La Viewer Protocol Policy (Politique de protocole d'utilisateur) du comportement de cache doit être définie sur Redirect HTTP vers HTTPS (Rediriger HTTP vers HTTPS) ou HTTPS Only (HTTPS uniquement). (Dans AWS CloudFormation ou dans l' CloudFront API, `ViewerProtocolPolicy` doit être défini sur `redirect-to-https` ou`https-only`.)

- Les Allowed HTTP Methods (Méthodes HTTP autorisées) du comportement du cache doivent être définies sur GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. (Dans AWS CloudFormation ou dans l' CloudFront API, `AllowedMethods` il doit être défini sur `GETHEAD,OPTIONS,PUT,POST,PATCH,DELETE`. Ils peuvent être spécifiés dans n'importe quel ordre.)
- La Origin Protocol Policy (Politique de protocole d'origine) du paramètre d'origine doit être définie sur Match Viewer (Correspond à l'utilisateur) ou HTTPS Only (HTTPS uniquement). (Dans AWS CloudFormation ou dans l' CloudFront API, `OriginProtocolPolicy` doit être défini sur `match-viewer` ou`https-only`.)

Pour plus d'informations, consultez Référence des paramètres de distribution.

Déchiffrez les champs de données à votre origine

CloudFront chiffre les champs de données à l'aide du AWS Encryption SDK. Les données restent chiffrées dans l'ensemble de votre pile d'applications et ne sont accessibles qu'aux applications possédant les informations d'identification pour les déchiffrer.

Après le chiffrement, le texte chiffré est encodé en base64. Lorsque vos applications déchiffrent le texte à l'origine, elles doivent d'abord décoder le texte chiffré, puis utiliser le kit SDK de chiffrement AWS pour déchiffrer les données.

L'exemple de code suivant illustre la façon dont les applications peuvent déchiffrer des données à votre origine. Remarques :

- Pour simplifier l'exemple, cet exemple charge des clés publiques et privées (au format DER) à partir de fichiers du répertoire de travail. En pratique, vous devez stocker la clé privée à un emplacement sécurisé hors ligne, par exemple un module de sécurité matérielle hors ligne, et distribuer la clé publique à votre équipe de développement.
- CloudFront utilise des informations spécifiques lors du chiffrement des données, et le même ensemble de paramètres doit être utilisé à l'origine pour les déchiffrer. Les paramètres CloudFront utilisés lors de l'initialisation MasterKey sont les suivants :
  - PROVIDER_NAME : Vous avez indiqué cette valeur lors de la création d'un profil de chiffrement au niveau du profil. Utilisez la même valeur ici.
  - KEY_NAME : vous avez créé un nom pour votre clé publique lorsque vous l'avez téléchargée CloudFront, puis vous l'avez spécifié dans le profil. Utilisez la même valeur ici.

- ALGORITHME : CloudFront utilisé `RSA/ECB/OAEPWithSHA-256AndMGF1Padding` comme algorithme de chiffrement, vous devez donc utiliser le même algorithme pour déchiffrer les données.

- Si vous exécutez l'exemple de programme suivant avec le texte chiffré en tant qu'entrée, les données déchiffrées constituent une sortie de votre console. Pour plus d'informations, consultez l'exemple de code Java dans le SDK de AWS chiffrement.

Exemple de code

```
import java.nio.file.Files;
import java.nio.file.Paths;
import java.security.KeyFactory;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;

import org.apache.commons.codec.binary.Base64;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;

/**
 * Sample example of decrypting data that has been encrypted by CloudFront field-level
 encryption.
 */
public class DecryptExample {

    private static final String PRIVATE_KEY_FILENAME = "private_key.der";
    private static final String PUBLIC_KEY_FILENAME = "public_key.der";
    private static PublicKey publicKey;
    private static PrivateKey privateKey;

    // CloudFront uses the following values to encrypt data, and your origin must use
 same values to decrypt it.
    // In your own code, for PROVIDER_NAME, use the provider name that you specified
 when you created your field-level
    // encryption profile. This sample uses 'DEMO' for the value.
    private static final String PROVIDER_NAME = "DEMO";
```

```
   // In your own code, use the key name that you specified when you added your public
key to CloudFront. This sample
   // uses 'DEMOKEY' for the key name.
   private static final String KEY_NAME = "DEMOKEY";
   // CloudFront uses this algorithm when encrypting data.
   private static final String ALGORITHM = "RSA/ECB/OAEPWithSHA-256AndMGF1Padding";

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

       final String dataToDecrypt = args[0];

       // This sample uses files to get public and private keys.
       // In practice, you should distribute the public key and save the private key
in secure storage.
       populateKeyPair();

       System.out.println(decrypt(debase64(dataToDecrypt)));
   }

   private static String decrypt(final byte[] bytesToDecrypt) throws Exception {
       // You can decrypt the stream only by using the private key.

       // 1. Instantiate the SDK
       final AwsCrypto crypto = new AwsCrypto();

       // 2. Instantiate a JCE master key
       final JceMasterKey masterKey = JceMasterKey.getInstance(
               publicKey,
               privateKey,
               PROVIDER_NAME,
               KEY_NAME,
               ALGORITHM);

       // 3. Decrypt the data
       final CryptoResult <byte[], ? > result = crypto.decryptData(masterKey,
bytesToDecrypt);
       return new String(result.getResult());
   }

   // Function to decode base64 cipher text.
   private static byte[] debase64(final String value) {
       return Base64.decodeBase64(value.getBytes());
   }
```

```
    private static void populateKeyPair() throws Exception {
        final byte[] PublicKeyBytes =
 Files.readAllBytes(Paths.get(PUBLIC_KEY_FILENAME));
        final byte[] privateKeyBytes =
 Files.readAllBytes(Paths.get(PRIVATE_KEY_FILENAME));
        publicKey = KeyFactory.getInstance("RSA").generatePublic(new
 X509EncodedKeySpec(PublicKeyBytes));
        privateKey = KeyFactory.getInstance("RSA").generatePrivate(new
 PKCS8EncodedKeySpec(privateKeyBytes));
    }
}
```

Vidéo à la demande et diffusion vidéo en direct avec CloudFront

Vous pouvez l'utiliser CloudFront pour diffuser de la vidéo à la demande (VOD) ou du streaming vidéo en direct en utilisant n'importe quelle origine HTTP. Vous pouvez notamment configurer des flux de travail vidéo dans le cloud en les utilisant CloudFront conjointement avec AWS Media Services.

Rubriques

À propos du streaming vidéo

Vous devez utiliser un encodeur pour empaqueter le contenu vidéo avant de CloudFront pouvoir le distribuer. Le processus d'empaquetage crée des segments qui contiennent vos contenus audio, vidéo et légendes. Il génère également des fichiers manifestes, qui décrivent dans un ordre spécifique les segments à lire et à quel moment. Les formats courants pour les packages sont MPEG DASH, Apple HLS, Microsoft Smooth Streaming et CMAF.

Streaming de VOD

Pour le streaming VOD, votre contenu vidéo est stocké sur un serveur et les spectateurs peuvent le visionner à tout moment. Pour créer une ressource que les spectateurs peuvent diffuser, utilisez un encodeur, par exemple AWS Elemental MediaConvert, pour formater et empaqueter vos fichiers multimédias.

Une fois que votre vidéo est empaquetée dans les bons formats, vous pouvez la stocker sur un serveur ou dans un compartiment Amazon S3, puis la diffuser à CloudFront la demande des spectateurs.

Diffusion de vidéo streaming en direct

Pour la diffusion de vidéo streaming en direct, votre contenu vidéo est diffusé en temps réel au fur et à mesure que les événements en direct se produisent, ou est configuré comme un canal en direct 24/24 , 7/7 j. Pour créer des sorties en direct destinées à la diffusion et à la diffusion en

continu, utilisez un encodeur tel que AWS Elemental MediaLive, pour compresser la vidéo et la formater pour les appareils de visualisation.

Une fois votre vidéo encodée, vous pouvez la stocker AWS Elemental MediaStore ou la convertir dans différents formats de diffusion en utilisant AWS Elemental MediaPackage. Utilisez l'une de ces origines pour configurer une CloudFront distribution destinée à diffuser le contenu. Pour connaître les étapes spécifiques et les conseils pour créer des distributions fonctionnant avec ces services, consultez Diffusez la vidéo en utilisant AWS Elemental MediaStore comme origine et Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.

Wowza et Unified Streaming fournissent également des outils que vous pouvez utiliser pour diffuser des vidéos. CloudFront Pour plus d'informations sur l'utilisation de Wowza avec CloudFront, consultez la section Apportez votre licence Wowza Streaming Engine au streaming HTTP en CloudFront direct sur le site Web de documentation de Wowza. Pour plus d'informations sur l'utilisation du streaming unifié CloudFront pour le streaming VOD, consultez CloudFrontle site Web de documentation du streaming unifié.

Diffusez des vidéos à la demande avec CloudFront

Pour diffuser de la vidéo à la demande (VOD) en streaming avec CloudFront, utilisez les services suivants :

- Amazon S3 pour stocker le contenu dans son format d'origine et pour stocker la vidéo transcodée.
- Un encodeur (tel que AWS Elemental MediaConvert) pour transcoder la vidéo en formats de streaming.
- CloudFront pour diffuser la vidéo transcodée aux spectateurs. Pour Microsoft Smooth Streaming, veuillez consulter Configuration de la vidéo à la demande pour Microsoft Smooth Streaming.

Pour créer une solution de VOD avec CloudFront

1. Chargez votre contenu sur un compartiment Amazon S3. Pour en savoir plus sur l'utilisation d'Amazon S3, veuillez consulter le Guide de l'utilisateur Amazon Simple Storage Service.
2. Transcodez votre contenu à l'aide d'une MediaConvert tâche. La tâche convertit votre vidéo dans les formats requis pour les lecteurs que vos spectateurs utilisent. Vous pouvez également utiliser la tâche pour créer des ressources dont la résolution et le débit varient. Ces ressources sont utilisées pour le streaming à débit adaptatif (ABR), qui ajuste la qualité de visionnage en fonction

de la bande passante disponible du spectateur. MediaConvert stocke la vidéo transcodée dans un compartiment S3.

3. Diffusez votre contenu converti en utilisant une CloudFront distribution. Les spectateurs peuvent regarder le contenu sur n'importe quel appareil, à tout moment.

> **Tip**
>
> Vous pouvez découvrir comment utiliser un AWS CloudFormation modèle pour déployer une AWS solution de VOD avec tous les composants associés. Pour voir les étapes d'utilisation du modèle, consultez Déploiement automatisé dans le guide Vidéo à la demande sur AWS.

Configuration de la vidéo à la demande pour Microsoft Smooth Streaming

Vous disposez des options suivantes pour distribuer du contenu vidéo CloudFront à la demande (VOD) que vous avez transcodé au format Microsoft Smooth Streaming :

- Spécifiez un serveur web qui exécute Microsoft IIS et prend en charge Smooth Streaming comme origine de votre distribution.
- Activez Smooth Streaming dans les comportements de cache d'une CloudFront distribution. Étant donné que vous pouvez utiliser plusieurs comportements de cache dans une distribution, vous pouvez utiliser une distribution pour les fichiers multimédias Smooth Streaming ainsi que pour d'autres contenus.

> **Important**
>
> Si vous spécifiez un serveur Web exécutant Microsoft IIS comme origine, n'activez pas Smooth Streaming dans les comportements de cache de votre CloudFront distribution. CloudFront vous ne pouvez pas utiliser un serveur Microsoft IIS comme origine si vous activez Smooth Streaming comme comportement de cache.

Si vous activez Smooth Streaming dans un comportement de cache (c'est-à-dire, si vous n'avez pas de serveur exécutant Microsoft IIS), notez les points suivants :

- Vous pouvez continuer à distribuer d'autres contenus à l'aide du même comportement de cache si le contenu correspond à la valeur de Modèle de chemin pour ce comportement de cache.
- CloudFront peut utiliser un compartiment Amazon S3 ou une origine personnalisée pour les fichiers multimédia Smooth Streaming. CloudFront Impossible d'utiliser un serveur Microsoft IIS comme origine si vous activez Smooth Streaming pour le comportement du cache.
- Vous ne pouvez pas invalider les fichiers multimédias au format Smooth Streaming. Si vous voulez mettre à jour les fichiers avant qu'ils n'expirent, vous devez les renommer. Pour plus d'informations, consultez Ajouter, supprimer ou remplacer du contenu CloudFront diffusé.

Pour plus d'informations sur les clients Smooth Streaming, consultez Smooth Streaming sur le site Web de documentation Microsoft.

À utiliser CloudFront pour distribuer des fichiers Smooth Streaming lorsqu'un serveur Web Microsoft IIS n'en est pas l'origine

1. Transcodez vos fichiers multimédias au format MP4 fragmenté Smooth Streaming.
2. Effectuez l'une des actions suivantes :
   - Si vous utilisez la CloudFront console : lorsque vous créez ou mettez à jour une distribution, activez Smooth Streaming dans un ou plusieurs comportements de cache de la distribution.
   - Si vous utilisez l' CloudFront API : ajoutez l'`SmoothStreaming`élément au type `DistributionConfig` complexe pour un ou plusieurs comportements de cache de la distribution.
3. Chargez les fichiers Smooth Streaming vers votre origine.
4. Créez un fichier `clientaccesspolicy.xml` ou `crossdomainpolicy.xml`, puis ajoutez-le à un emplacement accessible à la racine de votre distribution : par exemple, `https://d111111abcdef8.cloudfront.net/clientaccesspolicy.xml`. Voici un exemple de politique :

```
<?xml version="1.0" encoding="utf-8"?>
<access-policy>
<cross-domain-access>
<policy>
<allow-from http-request-headers="*">
<domain uri="*"/>
</allow-from>
<grant-to>
```

```
<resource path="/" include-subpaths="true"/>
</grant-to>
</policy>
</cross-domain-access>
</access-policy>
```

Pour plus d'informations, consultez Making a Service Available Across Domain Boundaries sur le site web Microsoft Developer Network.

5. Pour les liens dans votre application (un lecteur multimédia, par exemple), spécifiez l'URL du fichier multimédia au format suivant :

   ```
   https://d111111abcdef8.cloudfront.net/video/presentation.ism/Manifest
   ```

Diffusez des vidéos en direct avec CloudFront et AWS Media Services

Pour utiliser AWS Media Services CloudFront pour diffuser du contenu en direct à un public mondial, consultez les instructions suivantes.

Utilisez AWS Elemental MediaLive pour encoder les flux vidéo en direct en temps réel. Pour encoder un flux vidéo volumineux, MediaLive compressez-le en versions plus petites (encodages) qui peuvent être distribuées à vos spectateurs.

Après avoir compressé un flux vidéo en direct, vous disposez des deux options principales suivantes pour préparer et diffuser le contenu :

- Convertissez votre contenu dans les formats requis, puis diffusez-le : si vous avez besoin de contenu dans plusieurs formats, utilisez le package AWS Elemental MediaPackagepour différents types d'appareils. Lorsque vous empaquetez le contenu, vous pouvez également implémenter des fonctionnalités supplémentaires et ajouter la gestion des droits numériques (DRM) pour empêcher l'utilisation non autorisée de votre contenu. Pour step-by-step obtenir des instructions d'utilisation CloudFront pour diffuser du contenu MediaPackage formaté, consultezDiffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.
- Stockez et diffusez votre contenu à l'aide d'une origine évolutive : si le contenu est MediaLive codé dans les formats requis par tous les appareils utilisés par vos spectateurs, utilisez une origine hautement évolutive, par exemple AWS Elemental MediaStorepour diffuser le contenu. Pour step-by-step obtenir des instructions CloudFront d'utilisation pour diffuser du contenu stocké dans

un MediaStore conteneur, voirDiffusez la vidéo en utilisant AWS Elemental MediaStore comme origine.

Après avoir configuré votre origine à l'aide de l'une de ces options, vous pouvez diffuser des vidéos en direct aux spectateurs en utilisant CloudFront.

> **Tip**
>
> Découvrez une AWS solution qui déploie automatiquement des services pour créer une expérience de visionnage en temps réel hautement disponible. Pour connaître les étapes permettant de déployer automatiquement cette solution, veuillez consulter Déploiement automatisé de streaming en direct.

Rubriques

- Diffusez la vidéo en utilisant AWS Elemental MediaStore comme origine
- Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage

Diffusez la vidéo en utilisant AWS Elemental MediaStore comme origine

Si vous avez une vidéo stockée dans un AWS Elemental MediaStoreconteneur, vous pouvez créer une CloudFront distribution pour diffuser le contenu.

Pour commencer, vous autorisez CloudFront l'accès à votre MediaStore conteneur. Ensuite, vous créez une CloudFront distribution et vous la configurez pour qu'elle fonctionne avec MediaStore.

Pour diffuser le contenu d'un AWS Elemental MediaStore conteneur

1. Suivez la procédure décrite dans Autoriser Amazon CloudFront à accéder à votre AWS Elemental MediaStore conteneur, puis revenez à ces étapes pour créer votre distribution.
2. Créez une distribution avec les paramètres suivants :

    a. Domaine d'origine : point de terminaison de données attribué à votre MediaStore conteneur. Dans la liste déroulante, choisissez le MediaStore conteneur pour votre vidéo en direct.

    b. Chemin d'origine : structure des dossiers du MediaStore conteneur dans lequel sont stockés vos objets. Pour plus d’informations, consultez the section called “Chemin d’origine”.

c. Ajouter un en-tête personnalisé : ajoutez des noms et des valeurs d'en-tête si vous CloudFront souhaitez ajouter des en-têtes personnalisés lorsqu'il transmet des demandes à votre origine.

d. Politique du protocole Viewer — Choisissez Rediriger le HTTP vers HTTPS. Pour plus d'informations, consultez the section called “Viewer Protocol Policy”.

e. Politique de cache et politique de demande d'origine

- PourCache policy (Politique de cache), choisissez Create policy (Créer une politique), puis créez une politique de cache adaptée à vos besoins de mise en cache et aux durées de segment. Une fois la politique créée, actualisez la liste des politiques de cache et choisissez la politique que vous venez de créer.
- Pour la politique de demande Origin, choisissez CORS- CustomOrigin dans la liste déroulante.

Pour les autres paramètres, vous pouvez définir des valeurs spécifiques selon d'autres exigences techniques ou selon les besoins de votre entreprise. Afin d'obtenir une liste de toutes les options pour les distributions ainsi que leurs informations de configuration, veuillez consulter the section called “Paramètres de distribution”.

3. Pour les liens de votre application (par exemple, un lecteur multimédia), spécifiez le nom du fichier multimédia dans le même format que celui que vous utilisez pour les autres objets que vous distribuez CloudFront.

Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage

Si vous avez formaté un flux en direct à l'aide de AWS Elemental MediaPackage, vous pouvez créer une CloudFront distribution et configurer les comportements de cache pour diffuser le flux en direct. Le processus suivant suppose que vous avez déjà créé une chaîne et ajouté des points de terminaison pour votre vidéo en direct à l'aide MediaPackage de.

Pour créer une CloudFront distribution pour MediaPackage manuellement, procédez comme suit :

Étapes

- Étape 1 : Création et configuration d'une CloudFront distribution
- Étape 2 : ajouter des origines pour les domaines de vos points de MediaPackage terminaison

- Étape 3 : Configurer les comportements de cache pour tous les points de terminaison
- Étape 4 : activer l'autorisation CDN basée sur l'en-tête MediaPackage
- Étape 5 : Utiliser CloudFront pour diffuser la chaîne de diffusion en direct

Étape 1 : Création et configuration d'une CloudFront distribution

Procédez comme suit pour configurer une CloudFront distribution pour la chaîne vidéo en direct que vous avez créée avec MediaPackage.

Pour créer une distribution pour votre canal vidéo en direct

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Choisissez les paramètres de la distribution, en particulier les suivants :

   Domaine de l’origine

   L'origine de votre chaîne vidéo MediaPackage en direct et de vos points de terminaison. Choisissez le champ de texte, puis dans la liste déroulante, choisissez le domaine MediaPackage d'origine de votre vidéo en direct. Vous pouvez mapper un domaine à plusieurs points de terminaison d'origine.

   Si vous avez créé votre domaine d'origine à partir d'un autre compte AWS , saisissez la valeur d'URL de l'origine dans le champ. L’origine doit être une URL HTTPS.

   Par exemple, pour un point de terminaison HLS comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, le domaine d'origine est `3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com`.

   Pour plus d’informations, consultez the section called “Domaine d'origine”.

   Chemin d’origine

   Le chemin d'accès au MediaPackage point de terminaison à partir duquel le contenu est diffusé.

Le champ Chemin de l'origine n'est pas rempli automatiquement. C'est à vous de le saisir manuellement.

Pour de plus amples informations sur le fonctionnement d'un chemin d'origine, veuillez consulter the section called "Chemin d'origine".

> **Important**
>
> Le chemin générique * est obligatoire pour acheminer quelque part dans la CloudFront distribution. Pour éviter que les requêtes qui ne correspondent pas à un chemin explicite ne soient routées vers l'origine réelle, créez une origine « fictive » pour ce chemin générique.

Example : Création d'une origine « fictive »

Si, dans l'exemple suivant, les points de terminaison `abc123` et `def456` routent vers l'origine « réelle », les demandes de contenu vidéo de tout autre point de terminaison sont routées vers `mediapackage.us-west-2.amazonaws.com` sans le sous-domaine approprié, ce qui entraîne un HTTP `404`.

MediaPackage points de terminaison :

```
https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/
index.m3u8
https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/def456/
index.m3u8
```

CloudFront Origine A :

```
Domain: 3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com
Path: None
```

CloudFront Origine B :

```
Domain: mediapackage.us-west-2.amazonaws.com
Path: None
```

CloudFront comportement du cache :

```
1. Path: /out/v1/abc123/* forward to Origin A
2. Path: /out/v1/def456/* forward to Origin A
3. Path: * forward to Origin B
```

Pour les autres paramètres de distribution, définissez des valeurs spécifiques en fonction des autres exigences techniques ou des besoins de votre entreprise. Afin d'obtenir une liste de toutes les options pour les distributions ainsi que leurs informations de configuration, veuillez consulter the section called "Paramètres de distribution".

Lorsque vous avez terminé de choisir les autres paramètres de distribution, choisissez Create distribution (Créer une distribution).

4. Choisissez la distribution que vous venez de créer, puis choisissez Behaviors (Comportements).
5. Sélectionnez le comportement du cache par défaut, puis choisissez Edit (Modifier). Spécifiez les paramètres de comportement du cache corrects pour le canal que vous avez choisi pour l'origine. Vous ajouterez ensuite une ou plusieurs autres origines supplémentaires et modifierez les paramètres de comportement du cache pour ces origines.
6. Accédez à la page CloudFront des distributions.
7. Attendez que la valeur de la colonne Dernière modification de votre distribution passe de Déploiement à une date et une heure indiquant que votre distribution CloudFront a été créée.

Étape 2 : ajouter des origines pour les domaines de vos points de MediaPackage terminaison

Répétez les étapes ci-dessous pour ajouter chacun des points de terminaison de votre MediaPackage chaîne à votre distribution, en gardant à l'esprit la nécessité de créer une origine « fictive ».

Pour ajouter d'autres points de terminaison en tant qu'origines

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Origins (Origines), puis Create origin (Créer une origine).
3. Pour le domaine Origin, dans la liste déroulante, choisissez un MediaPackage point de terminaison pour votre chaîne.

4. Pour les autres paramètres, définissez les valeurs en fonction des autres exigences techniques ou des besoins de votre entreprise. Pour plus d'informations, consultez the section called "Paramètres d'origine".
5. Choisissez Create origin (Créer une origine).

Étape 3 : Configurer les comportements de cache pour tous les points de terminaison

Pour chaque point de terminaison, vous devez configurer les comportements de cache pour ajouter des modèles de chemin qui acheminent les requêtes correctement. Les modèles de chemin que vous spécifiez dépendent du format vidéo que vous diffusez. La procédure suivante inclut les informations de modèle de chemin à utiliser pour les formats Apple HLS, CMAF, DASH et Microsoft Smooth Streaming.

Vous configurez généralement deux comportements de cache pour chaque point de terminaison :

- Le manifeste parent, qui est l'index pour vos fichiers.
- Les segments, qui sont les fichiers du contenu vidéo.

Pour créer un comportement de cache pour un point de terminaison

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Behaviors (Comportements), puis Create Behavior (Créer un comportement).
3. Pour le modèle de chemin, utilisez un MediaPackage `OriginEndpoint` GUID spécifique comme préfixe de chemin.

   Modèles de chemin

   Pour un point de terminaison HLS
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, créez les deux comportements de cache suivants :
   - Pour les manifestes parents et enfants, utilisez `/out/v1/abc123/*.m3u8`.
   - Pour les segments de contenu, utilisez `/out/v1/abc123/*.ts`.

   Pour un point de terminaison CMAF
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, créez les deux comportements de cache suivants :
   - Pour les manifestes parents et enfants, utilisez `/out/v1/abc123/*.m3u8`.

- Pour les segments de contenu, utilisez `/out/v1/abc123/*.mp4`.

Pour un point de terminaison DASH comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.mpd`, créez les deux comportements de cache suivants :

- Pour le manifeste parent, utilisez `/out/v1/abc123/*.mpd`.
- Pour les segments de contenu, utilisez `/out/v1/abc123/*.mp4`.

Pour un point de terminaison Microsoft Smooth Streaming comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.ism`, seul un manifeste est diffusé. Vous ne créez donc qu'un seul comportement de cache : `out/v1/abc123/index.ism/*`.

4. Renseignez les valeurs des paramètres suivants pour chaque comportement de cache :

   Viewer Protocol Policy

   Choisissez Rediriger HTTP vers HTTPS.

   Politique de cache et de demande d'origine

   Pour Cache policy (Politique de cache), choisissez Create policy (Créer une poliltique). Pour votre nouvelle politique de cache, spécifiez les paramètres suivants :

   Durée de vie minimale

   Définissez sur 5 secondes ou moins pour éviter la diffusion de contenu obsolète.

   Chaînes de requête

   Pour Query strings (Chaînes de requête) (dans Cache key settings (Paramètres de clé de cache), choisissez Include specified query strings (Inclure des chaînes de requête spécifiées). Pour Allow (Autoriser), ajoutez les valeurs suivantes en les saisissant, puis choisissez Add item (Ajouter un élément) :

   - Ajoutez `m` en tant que chaîne de requête un paramètre que vous CloudFront souhaitez utiliser comme base pour la mise en cache. La MediaPackage réponse inclut toujours le tag permettant `?m=###` de saisir l'heure de modification du point de terminaison. Si le contenu est déjà mis en cache avec une valeur différente pour cette balise, CloudFront demande un nouveau manifeste au lieu de diffuser la version mise en cache.
   - Si vous utilisez la fonctionnalité d'affichage décalé dans le temps dans MediaPackage, spécifiez `start` et en `end` tant que paramètres de chaîne de requête supplémentaires

sur le comportement du cache pour les demandes de manifeste (`*.m3u8*.mpd`, et`index.ism/*`). De cette façon, le contenu diffusé est spécifique à la période demandée dans la requête de manifeste. Pour en savoir plus sur le visionnage en différé et sur le formatage des paramètres de demande de début et de fin de contenu, consultez Visionnage en différé dans le Guide de l'utilisateur AWS Elemental MediaPackage .

- Si vous utilisez la fonctionnalité de filtrage des manifestes dans MediaPackage, spécifiez `aws.manifestfilter` comme paramètre de chaîne de requête supplémentaire la politique de cache que vous utilisez avec le comportement du cache pour les demandes de manifeste (`*.m3u8*.mpd`, et`index.ism/*`). Cela configure votre distribution pour transmettre la chaîne de `aws.manifestfilter` requête à votre MediaPackage origine, ce qui est nécessaire au fonctionnement de la fonctionnalité de filtrage des manifestes. Pour en savoir plus, consultez Filtrage des manifestes dans le Guide de l'utilisateur AWS Elemental MediaPackage .
- Si vous utilisez le protocole HLS à faible latence (LL-HLS), spécifiez `_HLS_msn` et `_HLS_part` comme paramètres de chaîne de requête supplémentaires pour la politique de cache que vous utilisez avec le comportement de cache pour les demandes de manifeste (`*.m3u8`). Cela configure votre distribution pour qu'elle transmette les chaînes `_HLS_msn` et les chaînes de `_HLS_part` requête à votre MediaPackage origine, ce qui est nécessaire au fonctionnement de la fonctionnalité de blocage des demandes de playlist LL-HLS.

5. Choisissez Créer.
6. Après avoir créé la politique de cache, revenez au flux de création de comportements de cache. Actualisez la liste des politiques de cache, puis choisissez la politique que vous venez de créer.
7. Choisissez Create behavior (Créer un comportement).
8. Si votre point de terminaison n'est pas un point de terminaison Microsoft Smooth Streaming, répétez ces étapes pour créer un second comportement de cache.

Étape 4 : activer l'autorisation CDN basée sur l'en-tête MediaPackage

Nous recommandons d'activer l'autorisation MediaPackage CDN basée sur les en-têtes entre les MediaPackage points de terminaison et la distribution. CloudFront Pour plus d'informations, voir Activer l'autorisation CDN MediaPackage dans le guide de l'AWS Elemental MediaPackage utilisateur.

Étape 5 : Utiliser CloudFront pour diffuser la chaîne de diffusion en direct

Après avoir créé la distribution, ajouté les origines, créé les comportements de cache et activé l'autorisation CDN basée sur les en-têtes, vous pouvez diffuser le canal de diffusion en direct à l'aide de. CloudFront CloudFront achemine les demandes des utilisateurs vers les MediaPackage points de terminaison appropriés en fonction des paramètres que vous avez configurés pour les comportements du cache.

Pour les liens dans votre application (par exemple, un lecteur multimédia), spécifiez l'URL du fichier multimédia au format standard pour les CloudFront URL. Pour plus d'informations, voir the section called “Personnaliser les URL des fichiers”.

Personnalisez à la périphérie grâce à des fonctions

Avec Amazon CloudFront, vous pouvez écrire votre propre code pour personnaliser la façon dont vos CloudFront distributions traitent les requêtes et réponses HTTP. Le code s'exécute à proximité de vos utilisateurs pour minimiser la latence, et vous n'avez pas à gérer de serveurs ou toute autre infrastructure. Vous pouvez écrire du code pour manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP à la périphérie, etc.

Le code que vous écrivez et attachez à votre CloudFront distribution est appelé fonction de périphérie. CloudFront propose deux méthodes pour écrire et gérer les fonctions de périphérie :

CloudFront Fonctions

Vous pouvez y intégrer des fonctions légères JavaScript pour des personnalisations de CDN à grande échelle et sensibles à la latence. L'environnement d'exécution CloudFront Functions offre des temps de démarrage inférieurs à la milliseconde, s'adapte immédiatement pour traiter des millions de requêtes par seconde et est hautement sécurisé. CloudFront Functions est une fonctionnalité native de CloudFront, ce qui signifie que vous pouvez créer, tester et déployer votre code entièrement en interne CloudFront.

Lambda@Edge

Lambda @Edge est une extension AWS Lambdaqui offre une solution informatique puissante et flexible pour des fonctions complexes ainsi qu'une logique d'application complète plus proche de vos utilisateurs, tout en étant hautement sécurisée. Les fonctions Lambda@Edge s'exécutent dans un environnement d'exécution Node.js ou Python. Vous les publiez en un seul Région AWS, mais lorsque vous associez la fonction à une CloudFront distribution, Lambda @Edge réplique automatiquement votre code dans le monde entier.

Si vous l'exécutez AWS WAF CloudFront, vous pouvez utiliser des en-têtes AWS WAF insérés à la fois pour CloudFront Functions et Lambda @Edge. Cela fonctionne pour les demandes et réponses du visiteur et de l'origine.

Rubriques

- Différences entre CloudFront Functions et Lambda @Edge
- Personnalisez à la périphérie avec CloudFront Functions

- Personnalisez à la périphérie avec Lambda @Edge
- Restrictions sur les fonctions périphériques

Différences entre CloudFront Functions et Lambda @Edge

CloudFront Functions et Lambda @Edge fournissent tous deux un moyen d'exécuter du code en réponse à CloudFront des événements.

CloudFront Functions est idéal pour les fonctions légères et de courte durée dans les cas d'utilisation suivants :

- Normalisation des clés de cache : transformez les attributs des requêtes HTTP (en-têtes, chaînes de requête, cookies et même le chemin de l'URL) pour créer une clé de cache optimale, ce qui peut améliorer le taux de réussite de votre cache.
- Manipulation des en-têtes : insérez, modifiez ou supprimez des en-têtes HTTP dans la demande ou la réponse. Par exemple, vous pouvez ajouter un en-tête `True-Client-IP` à chaque requête.
- Redirections ou réécritures d'URL : redirigez les visiteurs vers d'autres pages en fonction des informations contenues dans la demande, ou réécrivez toutes les demandes d'un chemin à un autre.
- Demande d'autorisation — Validez les jetons d'autorisation hachés, tels que les jetons Web JSON (JWT), en inspectant les en-têtes d'autorisation ou d'autres métadonnées de demande.

Pour commencer à utiliser CloudFront Functions, voirPersonnalisez à la périphérie avec CloudFront Functions.

Lambda @Edge est idéal pour les cas d'utilisation suivants :

- Fonctions dont l'exécution prend plusieurs millisecondes ou plus
- Fonctions nécessitant un processeur ou une mémoire ajustable
- Fonctions qui dépendent de bibliothèques tierces (y compris le AWS SDK, pour l'intégration avec d'autres Services AWS bibliothèques)
- Fonctions nécessitant un accès au réseau pour utiliser des services externes pour le traitement
- Fonctions nécessitant un accès au système de fichiers ou au corps des requêtes HTTP

Pour démarrer avec Lambda@Edge, consultez Personnalisez à la périphérie avec Lambda @Edge.

Pour vous aider à choisir l'option adaptée à votre cas d'utilisation, utilisez le tableau suivant pour comprendre les différences entre CloudFront Functions et Lambda @Edge.

	CloudFront Fonctions	Lambda@Edge
Langages de programmation	JavaScript (compatible avec ECMAScript 5.1)	Node.js et Python
Sources des évènements	• Requête utilisateur • Réponse utilisateur	• Requête utilisateur • Réponse utilisateur • Requête de l'origine • Réponse de l’origine
Supports Amazon CloudFront KeyValueStore	Oui CloudFront KeyValueStore ne prend en charge que le JavaScript runtime 2.0	Non
Évolutivité	10 000 000 de requêtes par seconde ou plus	Jusqu'à 10 000 requêtes par seconde et par région
Durée de la fonction	Inférieure à une milliseconde	Jusqu'à 5 secondes (requête utilisateur et réponse utilisateur) Jusqu'à 30 secondes (requête de l'origine et réponse de l'origine)
Mémoire maximale Pour plus d’informations, consultez Quotas Lambda.	2 Mo	128 MO — 10 240 MO (10 GO)
Taille maximale du code de fonction et des bibliothèques incluses	10 Ko	1 Mo (requête utilisateur et réponse utilisateur)

	CloudFront Fonctions	Lambda@Edge
		50 Mo (requête de l'origine et réponse de l'origine)
Accès réseau	Non	Oui
Accès au système de fichiers	Non	Oui
Accès au corps de la requête	Non	Oui
Accès à la géolocalisation et aux données de l'appareil	Oui	Non (demande du téléspectateur et réponse du téléspectateur) Oui (demande d'origine et réponse d'origine)
Peut être entièrement construit et testé dans CloudFront	Oui	Non
Journalisation et métriques des fonctions	Oui	Oui
Tarification	Offre gratuite disponible ; facturation à la requête	Pas d'offre gratuite ; facturation à la requête et durée de fonction

Personnalisez à la périphérie avec CloudFront Functions

Avec CloudFront Functions, vous pouvez écrire des fonctions légères JavaScript pour des personnalisations de CDN à grande échelle et sensibles à la latence. Vos fonctions peuvent manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP à la périphérie, etc. L'environnement d'exécution CloudFront Functions offre des temps de démarrage inférieurs à la milliseconde, s'adapte immédiatement pour traiter des millions de requêtes par seconde et est hautement sécurisé. CloudFront Functions est une fonctionnalité native de CloudFront, ce qui signifie que vous pouvez créer, tester et déployer votre code entièrement en son sein CloudFront.

Lorsque vous associez une CloudFront fonction à une CloudFront distribution, CloudFront intercepte les demandes et les réponses à des emplacements CloudFront périphériques et les transmet à votre fonction. Vous pouvez appeler CloudFront Functions lorsque les événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un téléspectateur (demande du téléspectateur)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)

Pour plus d'informations sur CloudFront les fonctions, consultez les rubriques suivantes :

Rubriques

- Tutoriel : Création d'une fonction simple avec CloudFront Functions
- Tutoriel : Création d'une CloudFront fonction incluant des valeurs clés
- Écrire le code de la fonction
- Création de fonctions
- Fonctions de test
- Fonctions de mise à jour
- Fonctions de publication
- Associer des fonctions à des distributions
- Amazon CloudFront KeyValueStore

Tutoriel : Création d'une fonction simple avec CloudFront Functions

Ce didacticiel explique comment démarrer avec CloudFront Functions. Vous pouvez créer une fonction simple qui redirige le lecteur vers une autre URL et qui renvoie également un en-tête de réponse personnalisé.

Table des matières

Prérequis

Pour utiliser CloudFront Functions, vous avez besoin d'une CloudFront distribution. Si vous n'en avez pas, consultez Commencez avec une CloudFront distribution de base.

Créer la fonction

Vous pouvez utiliser la CloudFront console pour créer une fonction simple qui redirige le lecteur vers une autre URL et renvoie également un en-tête de réponse personnalisé.

Pour créer une CloudFront fonction

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Functions, puis Create function.
3. Sur la page Créer une fonction, pour Nom, entrez un nom de fonction tel que *MyFunctionName*.
4. (Facultatif) Dans Description, entrez une description de la fonction, telle que**Simple test function**.
5. Pour Runtime, conservez la JavaScript version sélectionnée par défaut.
6. Choisissez Créer une fonction.
7. Copiez le code de fonction suivant. Ce code de fonction redirige l'utilisateur vers une URL différente et renvoie également un en-tête de réponse personnalisé.

```
function handler(event) {
    // NOTE: This example function is for a viewer request event trigger.
    // Choose viewer request for event trigger when you associate this function
 with a distribution.
    var response = {
        statusCode: 302,
        statusDescription: 'Found',
        headers: {
            'cloudfront-functions': { value: 'generated-by-CloudFront-Functions' },
            'location': { value: 'https://aws.amazon.com/cloudfront/' }
        }
    };
    return response;
}
```

8. Pour le code de fonction, collez le code dans l'éditeur de code pour remplacer le code par défaut.

9. Sélectionnez Enregistrer les modifications.
10. (Facultatif) Vous pouvez tester la fonction avant de la publier. Ce didacticiel ne décrit pas comment tester une fonction. Pour plus d'informations, consultez Fonctions de test.
11. Choisissez l'onglet Publier, puis choisissez la fonction Publier. Vous devez publier la fonction avant de pouvoir l'associer à votre CloudFront distribution.
12. Vous pouvez ensuite associer la fonction à un comportement de distribution ou de cache. Sur la *MyFunctionName*page, choisissez l'onglet Publier.

    > ⚠ Warning
    >
    > Dans les étapes suivantes, choisissez une distribution ou un comportement de cache à utiliser pour les tests. N'associez pas cette fonction de test à un comportement de distribution ou de cache utilisé en production.

13. Choisissez Ajouter une association.
14. Dans la boîte de dialogue Associer, choisissez une distribution et/ou un comportement de cache. Pour le type d'événement, conservez la valeur par défaut.
15. Choisissez Ajouter une association.

    La table Distributions associées indique la distribution associée.
16. Attendez quelques minutes pour que la distribution associée termine son déploiement. Pour vérifier le statut de la distribution, sélectionnez la distribution dans le tableau des distributions associées, puis choisissez Afficher la distribution.

    Lorsque l'état de la distribution est Déployé, vous êtes prêt à vérifier que la fonction fonctionne.

Vérifiez le fonctionnement

Après avoir déployé la fonction, vous pouvez vérifier qu'elle fonctionne pour votre distribution.

Pour vérifier le fonctionnement

1. Dans votre navigateur Web, accédez au nom de domaine de votre distribution (par exemple,`https://d111111abcdef8.cloudfront.net`).

   La fonction renvoie une redirection vers le navigateur, de sorte que le navigateur ouvre automatiquement `https://aws.amazon.com/cloudfront/`.

2. Dans une fenêtre de ligne de commande, vous pouvez utiliser un outil tel que curl l'envoi d'une demande au nom de domaine de votre distribution.

```
curl -v https://d111111abcdef8.cloudfront.net/
```

Dans la réponse, vous pouvez voir la réponse de redirection (`302 Found`) et les en-têtes de réponse personnalisés ajoutés par la fonction. Votre réponse peut ressembler à l'exemple suivant.

Example

```
curl -v https://d111111abcdef8.cloudfront.net/
> GET / HTTP/1.1
> Host: d111111abcdef8.cloudfront.net
> User-Agent: curl/7.64.1
> Accept: */*
>
< HTTP/1.1 302 Found
< Server: CloudFront
< Date: Tue, 16 Mar 2021 18:50:48 GMT
< Content-Length: 0
< Connection: keep-alive
< Location: https://aws.amazon.com/cloudfront/
< Cloudfront-Functions: generated-by-CloudFront-Functions
< X-Cache: FunctionGeneratedResponse from cloudfront
< Via: 1.1 3035b31bddaf14eded329f8d22cf188c.cloudfront.net (CloudFront)
< X-Amz-Cf-Pop: PHX50-C2
< X-Amz-Cf-Id: ULZdIz6j43uGBlXyob_JctF9x7CCbwpNniiMlmNbmwzH1YWP9FsEHg==
```

Tutoriel : Création d'une CloudFront fonction incluant des valeurs clés

Ce didacticiel explique comment inclure des valeurs clés dans une CloudFront fonction. Les valeurs clés font partie d'une paire clé-valeur. Vous incluez le nom (issu de la paire clé-valeur) dans le code de fonction. Lorsque la fonction s'exécute, CloudFront remplace le nom par la valeur.

Les paires clé-valeur sont des variables stockées dans un magasin clé-valeur. Lorsque vous utilisez une clé dans votre fonction (à la place de valeurs codées en dur), votre fonction est plus flexible. Vous pouvez modifier la valeur de la clé sans avoir à déployer de modifications de code. Les paires

clé-valeur peuvent également réduire la taille de votre fonction. Pour plus d'informations, consultez ???.

Table des matières

Prérequis

Si vous découvrez les CloudFront fonctions et le magasin de valeurs clés pour la première fois, nous vous recommandons de suivre le didacticiel dansthe section called "Tutoriel : Création d'une CloudFront fonction simple".

Après avoir terminé ce didacticiel, vous pouvez suivre ce didacticiel pour étendre la fonction que vous avez créée. Pour ce didacticiel, nous vous recommandons de créer d'abord le magasin de valeurs clés.

Créez le magasin de valeur clé

Créez d'abord le magasin de valeurs clés à utiliser pour votre fonction.

Pour créer le magasin de valeurs clés

1. Planifiez les paires clé-valeur que vous souhaitez inclure dans la fonction. Notez les noms de clés. Les paires clé-valeur que vous souhaitez utiliser dans une fonction doivent se trouver dans un seul magasin clé-valeur.
2. Décidez de l'ordre de travail. Il existe deux façons de procéder :
   - Créez un magasin clé-valeur et ajoutez-y des paires clé-valeur. Créez (ou modifiez) ensuite la fonction et incorporez les noms des clés.
   - Ou, créez (ou modifiez) la fonction et incorporez les noms des clés que vous voulez utiliser. Créez ensuite un magasin clé-valeur et ajoutez les paires clé-valeur.
3. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

4. Dans le volet de navigation, choisissez Functions, puis sélectionnez l'KeyValueStoresonglet.
5. Choisissez Créer KeyValueStore et saisissez les champs suivants :
   - Entrez un nom et une description (facultative) pour le magasin.
   - Laissez l'URI S3 vide. Dans ce didacticiel, vous allez saisir les paires clé-valeur manuellement.
6. Choisissez Créer. La page de détails du nouveau magasin de clés-valeurs apparaît. Cette page inclut une section Paires clé-valeur qui est actuellement vide.

Ajouter des paires clé-valeur au magasin clé-valeur

Ajoutez ensuite manuellement une liste de paires clé-valeur au magasin clé-valeur que vous avez créé précédemment.

Pour ajouter des paires clé-valeur au magasin clé-valeur

1. Dans la section Paires clé-valeur, choisissez Ajouter des paires clé-valeur.
2. Choisissez Ajouter une paire, puis entrez une clé et une valeur. Cochez la case pour confirmer vos modifications et répétez cette étape pour en ajouter d'autres.
3. Lorsque vous avez terminé, choisissez Enregistrer les modifications pour enregistrer les paires clé-valeur dans le magasin clé-valeur. Dans la boîte de dialogue de confirmation, choisissez OK.

Vous disposez désormais d'un magasin clé-valeur qui contient un groupe de paires clé-valeur.

Associez le magasin de valeurs clés à la fonction

Vous avez maintenant créé le magasin de clés-valeurs. Vous avez également créé ou modifié une fonction qui inclut les noms des clés à partir du magasin de clés-valeurs. Vous pouvez maintenant associer le magasin de clés-valeurs et la fonction. Vous créez cette association à partir de la fonction.

Pour associer le magasin de valeurs clés à la fonction

1. Dans le volet de navigation, choisissez Fonctions. L’onglet Fonctions apparaît en haut, par défaut.
2. Choisissez le nom de la fonction, puis dans la KeyValueStore section Associé, sélectionnez Associer existant KeyValueStore.
3. Sélectionnez le magasin de valeurs clés, puis choisissez Associer KeyValueStore.

> **Note**
>
> Vous ne pouvez associer qu'une seule banque de valeurs clés à chaque fonction.

Testez et publiez le code de fonction

Après avoir associé le magasin de valeurs clés à votre fonction, vous pouvez tester et publier le code de la fonction. Vous devez tester le code de la fonction chaque fois que vous le modifiez, y compris lorsque vous effectuez les opérations suivantes :

- Association d'un magasin de clés-valeurs à la fonction.
- Modifiez la fonction et son magasin de valeurs clés pour inclure une nouvelle paire clé-valeur.
- Modifiez la valeur d'une paire clé-valeur.

Pour tester et publier le code de fonction

1. Pour en savoir plus sur la façon de tester une fonction, consultez the section called "Fonctions de test". Assurez-vous de choisir de tester la fonction dans la phase `DEVELOPMENT`.
2. Publiez la fonction lorsque vous êtes prêt à l'utiliser (avec les paires clé-valeur nouvelles ou révisées) dans un `LIVE` environnement.

   Lorsque vous publiez, CloudFront copie la version de la fonction de la `DEVELOPMENT` scène vers la scène en direct. La fonction possède le nouveau code et est associée au magasin de clés-valeurs. (Il n'est pas nécessaire de répéter l'association, dans la phase en direct.)

   Pour en savoir plus sur la façon de publier la fonction, consultez the section called "Fonctions de publication".

Écrire le code de la fonction

Vous pouvez utiliser CloudFront Functions pour écrire des fonctions légères dans le cadre de personnalisations JavaScript de CDN à grande échelle et sensibles à la latence. Votre code de fonction peut manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP à la périphérie, etc.

Pour vous aider à écrire du code de fonction pour CloudFront Functions, consultez les rubriques suivantes.

Rubriques

Déterminez l'objectif de votre fonction

Avant d'écrire votre code de fonction, déterminez le but de votre fonction. La plupart des CloudFront fonctions de Functions ont l'un des objectifs suivants.

Rubriques

Quel que soit le but de votre fonction, `handler` est le point d'entrée pour n'importe quelle fonction. Il prend un seul argument appelé`event`, qui est transmis à la fonction par CloudFront. `event` est un objet JSON qui contient une représentation de la requête HTTP (et la réponse, si votre fonction modifie la réponse HTTP).

Modification de la requête HTTP dans un type d'événement de demande de visionnage

Votre fonction peut modifier la requête HTTP envoyée CloudFront par le visualiseur (client) et renvoyer la demande modifiée CloudFront pour un traitement continu. Par exemple, votre code de fonction peut normaliser la clé de cache ou modifier les en-têtes de requêtes.

Lorsque vous créez une fonction qui modifie la requête HTTP, veillez à choisir le type d'évènement requête utilisateur. Cela signifie que la fonction s'exécute chaque fois qu' CloudFront elle reçoit une demande d'un visualiseur, avant de vérifier si l'objet demandé se trouve dans le CloudFront cache.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui modifie la requête HTTP.

```
function handler(event) {
    var request = event.request;

    // Modify the request object here.

    return request;
}
```

La fonction renvoie l'`request`objet modifié à CloudFront. CloudFrontpoursuit le traitement de la demande renvoyée en vérifiant la CloudFront présence d'un accès au cache et en envoyant la demande à l'origine si nécessaire.

Génération d'une réponse HTTP dans un type d'événement de demande de visionnage

Votre fonction peut générer une réponse HTTP à la périphérie et la renvoyer directement au visualiseur (client) sans vérifier la présence d'une réponse en cache ni aucun autre traitement par CloudFront. Par exemple, votre code de fonction peut rediriger la requête vers une nouvelle URL, ou vérifier l'autorisation et renvoyer une réponse `401` ou `403` à des requêtes non autorisées.

Lorsque vous créez une fonction qui génère une réponse HTTP, veillez à choisir le type d'évènement requête utilisateur. Cela signifie que la fonction s'exécute chaque fois qu' CloudFront elle reçoit une demande d'un utilisateur, avant CloudFront de poursuivre le traitement de la demande.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui génère une réponse HTTP.

```
function handler(event) {
    var request = event.request;

    var response = ...; // Create the response object here,
                        // using the request properties if needed.

    return response;
}
```

La fonction renvoie un `response` objet à CloudFront, qui revient CloudFront immédiatement au visualiseur sans vérifier le CloudFront cache ni envoyer de demande à l'origine.

Modification de la réponse HTTP dans un type d'événement de demande de visionnage

Votre fonction peut modifier la réponse HTTP avant de l' CloudFront envoyer au visualiseur (client), que la réponse provienne du CloudFront cache ou de l'origine. Par exemple, votre code de fonction peut ajouter ou modifier des en-têtes de réponse, des codes de statut et le contenu du corps.

Lorsque vous créez une fonction qui modifie la réponse HTTP, veillez à choisir le type d'évènement réponse utilisateur. Cela signifie que la fonction s'exécute avant de CloudFront renvoyer une réponse au visualiseur, que la réponse provienne du CloudFront cache ou de l'origine.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui modifie la réponse HTTP.

```
function handler(event) {
    var request = event.request;
    var response = event.response;

    // Modify the response object here,
    // using the request properties if needed.

    return response;
}
```

La fonction renvoie l'`response`objet modifié à CloudFront, qui revient CloudFront immédiatement au visualiseur.

Informations connexes

Pour plus d'informations sur l'utilisation des CloudFront fonctions, consultez les rubriques suivantes :

- Structure d'évènements
- JavaScript fonctionnalités d'exécution
- Exemple de code
- Restrictions sur les fonctions périphériques

CloudFront Fonctions, structure de l'événement

CloudFront Functions transmet un `event` objet à votre code de fonction en entrée lors de l'exécution de la fonction. Lorsque vous testez une fonction, vous créez l'objet `event` et le transférez à votre

fonction. Lorsque vous créez un objet `event` pour tester une fonction, vous pouvez omettre les champs `distributionDomainName`, `distributionId` et `requestId` de l'objet `context`. Assurez-vous que les noms des en-têtes sont en minuscules, ce qui est toujours le cas dans l'`event`objet que CloudFront Functions transmet à votre fonction en production.

La section suivante présente une vue d'ensemble de la structure de cet objet d'évènement.

```
{
    "version": "1.0",
    "context": {
        <context object>
    },
    "viewer": {
        <viewer object>
    },
    "request": {
        <request object>
    },
    "response": {
        <response object>
    }
}
```

Pour plus d’informations, consultez les rubriques suivantes :

Rubriques

- Champ Version
- Objet Contexte
- Objet Utilisateur
- Objet Requête
- Objet Réponse
- Code de statut et corps
- Structure d'une chaîne de requête, d'un en-tête ou d'un cookie
- Exemple d'objet de réponse
- Exemple d'objet d'événement

Champ Version

Le `version` champ contient une chaîne qui indique la version de l'objet d'événement CloudFront Functions. La version actuelle est `1.0`.

Objet Contexte

L'objet `context` contient des informations contextuelles sur l'évènement. Il inclut les champs suivants :

`distributionDomainName`

Le nom CloudFront de domaine (par exemple, d111111abcdef8.cloudfront.net) de la distribution associée à l'événement.

`distributionId`

ID de la distribution (par exemple EDFDVBD6EXAMPLE) associée à l'événement.

`eventType`

Le type d'évènement, `viewer-request` ou `viewer-response`.

`requestId`

Chaîne qui identifie de manière unique une CloudFront demande (et la réponse qui lui est associée).

Objet Utilisateur

L'objet `viewer` comporte un champ `ip` dont la valeur est l'adresse IP de l'utilisateur (client) qui a envoyé la requête. Si la requête utilisateur a été envoyée via un proxy HTTP ou un équilibreur de charge, la valeur correspond à l'adresse IP du proxy ou de l'équilibreur de charge.

Objet Requête

L'`request`objet contient une représentation d'une requête HTTP entre un visualiseur et un utilisateur. CloudFront Dans l'`event`objet transmis à votre fonction, l'`request`objet représente la demande réelle CloudFront reçue du visualiseur.

Si le code de votre fonction renvoie un `request` objet à CloudFront, il doit utiliser cette même structure.

L'objet `request` comporte les champs suivants :

`method`

Méthode HTTP de la demande. Si votre code de fonction renvoie un`request`, il ne peut pas modifier ce champ. Il s'agit du seul champ en lecture seule de l'objet `request`.

`uri`

Chemin d'accès relatif de l'objet demandé.

> **Note**
>
> Si votre fonction modifie la `uri` valeur, les règles suivantes s'appliquent :
>
> - La nouvelle valeur `uri` doit commencer par une barre oblique (`/`).
> - Lorsqu'une fonction modifie la valeur `uri`, elle change l'objet que l'utilisateur demande.
> - Quand une fonction modifie la valeur `uri`, elle ne modifie pas le comportement de cache pour la demande ni l'origine vers laquelle la demande d'origine est envoyée.

`querystring`

Objet qui représente la chaîne de requête dans la requête. Si la demande n'inclut pas de chaîne de requête, l'objet `request` inclut néanmoins un objet `querystring` vide.

L'objet `querystring` comporte un champ pour chaque paramètre de chaîne de requête dans la requête.

`headers`

Objet qui représente les en-têtes HTTP dans la requête. Si la requête contient des en-têtes `Cookie`, ces derniers ne font pas partie de l'objet `headers`. Les cookies sont représentés séparément dans l'objet `cookies`.

L'objet `headers` comporte un champ pour chaque en-tête de la requête. Les noms des en-têtes sont convertis en minuscules dans l'objet d'événement, et les noms des en-têtes doivent être en minuscules lorsqu'ils sont ajoutés par votre code de fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en requête HTTP, la première lettre de chaque mot dans les noms d'en-tête est mise en majuscule. Les mots sont séparés par un trait d'union (`-`). Par exemple, si votre code de fonction ajoute un en-tête nommé`example-header-name`, il le CloudFront convertit en en-tête `Example-Header-Name` dans la requête HTTP.

`cookies`

Objet qui représente les cookies dans la requête (en-têtes `Cookie`).

L'objet `cookies` comporte un champ pour chaque cookie dans la requête.

Pour plus d'informations sur la structure des chaînes de requêtes, des en-têtes et des cookies, consultez Structure d'une chaîne de requête, d'un en-tête ou d'un cookie.

Pour un exemple d'objet `event`, consultez Exemple d'objet d'événement.

Objet Réponse

L'`response`objet contient une représentation d'une réponse HTTP CloudFront à l'utilisateur. Dans l'`event`objet transmis à votre fonction, l'`response`objet représente la réponse réelle CloudFront de l'utilisateur à une demande de consultation.

Si votre code de fonction renvoie un objet `response`, il doit utiliser cette même structure.

L'objet `response` comporte les champs suivants :

`statusCode`

Code de statut HTTP de la réponse. Cette valeur est un entier, pas une chaîne.

Votre fonction peut générer ou modifier le `statusCode`.

`statusDescription`

Description de l'état HTTP de la réponse. Si votre code de fonction génère une réponse, ce champ est facultatif.

`headers`

Objet qui représente les en-têtes HTTP dans la réponse. Si la réponse contient des en-têtes `Set-Cookie`, ces derniers ne font pas partie de l'objet `headers`. Les cookies sont représentés séparément dans l'objet `cookies`.

L'objet `headers` comporte un champ pour chaque en-tête de la réponse. Les noms des en-têtes sont convertis en minuscules dans l'objet d'événement, et les noms des en-têtes doivent être en minuscules lorsqu'ils sont ajoutés par votre code de fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en réponse HTTP, la première lettre de chaque mot des noms

d'en-tête est mise en majuscule. Les mots sont séparés par un trait d'union (-). Par exemple, si votre code de fonction ajoute un en-tête nomméeexample-header-name, il le CloudFront convertit en Example-Header-Name dans la réponse HTTP.

cookies

Objet qui représente les cookies dans la réponse (en-têtes Set-Cookie).

L'objet cookies comporte un champ pour chaque cookie dans la réponse.

body

L'ajout du champ body est facultatif et il ne sera pas présent dans l'objet response à moins que vous ne le spécifiiez dans votre fonction. Votre fonction n'a pas accès au corps d'origine renvoyé par le CloudFront cache ou l'origine. Si vous ne spécifiez pas le body champ dans votre fonction de réponse du spectateur, le corps d'origine renvoyé par le CloudFront cache ou l'origine est renvoyé au visualiseur.

Si vous CloudFront souhaitez renvoyer un corps personnalisé au visualiseur, spécifiez le contenu du corps dans le data champ et le codage du corps dans le encoding champ. Vous pouvez spécifier le codage sous forme de texte brut ("encoding": "text") ou de contenu codé en Base64 ("encoding": "base64").

Comme raccourci, vous pouvez également spécifier le contenu du corps directement dans le champ body ("body": "<specify the body content here>"). Lorsque vous effectuez cette opération, omettez les encoding champs data et. CloudFront traite le corps comme du texte brut dans ce cas.

encoding

Codage du contenu de body (champ data). Les seuls encodages valides sont text et base64.

Si vous spécifiez encoding as base64 mais que le corps n'est pas valide en base64, CloudFront renvoie une erreur.

data

Contenu de body.

Pour plus d'informations sur les codes de statut modifiés et le contenu du corps, consultez Code de statut et corps.

Pour plus d'informations sur la structure des en-têtes et des cookies, consultez Structure d'une chaîne de requête, d'un en-tête ou d'un cookie.

Pour un exemple d'objet `response`, consultez Exemple d'objet de réponse.

Code de statut et corps

Avec CloudFront Functions, vous pouvez mettre à jour le code d'état de la réponse du lecteur, remplacer l'intégralité du corps de la réponse par un nouveau ou supprimer le corps de la réponse. Parmi les scénarios courants de mise à jour de la réponse du spectateur après avoir évalué certains aspects de la réponse provenant du CloudFront cache ou de l'origine, citons les suivants :

- Modification du statut pour définir un code de statut HTTP 200 et création d'un contenu de corps statique à renvoyer à l'utilisateur.
- Modification du statut pour définir un code de statut HTTP 301 ou 302 afin de rediriger l'utilisateur vers un autre site Web.
- Décider de diffuser ou de supprimer le corps de la réponse d'utilisateur.

> **Note**
>
> Si l'origine renvoie une erreur HTTP supérieure ou égale à 400, la CloudFront fonction ne sera pas exécutée. Pour plus d'informations, consultez Restrictions sur toutes les fonctions périphériques.

Lorsque vous travaillez avec la réponse HTTP, CloudFront Functions n'a pas accès au corps de la réponse. Vous pouvez remplacer le contenu du corps en lui attribuant la valeur souhaitée, ou supprimer le corps en définissant une valeur vide. Si vous ne mettez pas à jour le champ body de votre fonction, le corps d'origine renvoyé par le CloudFront cache ou l'origine est renvoyé au visualiseur.

> **Tip**
>
> Lorsque vous utilisez CloudFront des fonctions pour remplacer un corps, veillez à aligner les en-têtes correspondants, tels que`content-encoding`, ou `content-type``content-length`, sur le nouveau contenu du corps.

Par exemple, si l' CloudFront origine ou le cache sont renvoyés `content-encoding: gzip` mais que la fonction de réponse de l'utilisateur définit un corps en texte brut, la fonction doit également modifier `content-type` les en-têtes `content-encoding` et en conséquence.

Si votre CloudFront fonction est configurée pour renvoyer une erreur HTTP de 400 ou plus, votre lecteur ne verra pas la page d'erreur personnalisée que vous avez spécifiée pour le même code d'état.

Structure d'une chaîne de requête, d'un en-tête ou d'un cookie

Les chaînes de requête, les en-têtes et les cookies partagent la même structure. Les chaînes de requête peuvent apparaître dans les demandes. Les en-têtes apparaissent dans les demandes et les réponses. Les cookies apparaissent dans les demandes et les réponses.

Chaque chaîne de requête, en-tête ou cookie est un champ unique au sein de l'objet parent `querystring`, `headers` ou `cookies`. Le nom du champ est le nom de la chaîne de requête, de l'en-tête ou du cookie. Chaque champ comporte une propriété `value` avec la valeur de la chaîne de requête, de l'en-tête ou du cookie.

Table des matières

Valeurs de chaînes de requête ou objets de chaîne de requête

Une fonction peut renvoyer une valeur de chaîne de requête en plus d'un objet de chaîne de requête. La valeur de chaîne de requête peut être utilisée pour organiser les paramètres de chaîne de requête dans n'importe quel ordre personnalisé.

Example Exemple

Pour modifier une chaîne de requête dans le code de votre fonction, utilisez le code suivant.

```
var request = event.request;
request.querystring =
 'ID=42&Exp=1619740800&TTL=1440&NoValue=&querymv=val1&querymv=val2,val3';
```

Considérations spéciales pour les en-têtes

Pour les en-têtes uniquement, les noms des en-têtes sont convertis en minuscules dans l'objet d'événement, et les noms des en-têtes doivent être en minuscules lorsqu'ils sont ajoutés par votre code de fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en requête ou réponse HTTP, la première lettre de chaque mot des noms d'en-tête est mise en majuscule. Les mots sont séparés par un trait d'union (`-`). Par exemple, si votre code de fonction ajoute un en-tête nomméexample-header-name, il le CloudFront convertit `Example-Header-Name` dans la requête ou la réponse HTTP.

Example Exemple

Tenez compte de l'`Host`en-tête suivant dans une requête HTTP.

```
Host: video.example.com
```

Cet en-tête est représenté comme suit dans l'objet `request` :

```
"headers": {
    "host": {
        "value": "video.example.com"
    }
}
```

Pour accéder à l'en-tête `Host` dans votre code de fonction, utilisez le code comme suit :

```
var request = event.request;
var host = request.headers.host.value;
```

Pour ajouter ou modifier un en-tête dans votre code de fonction, utilisez le code suivant (ce code ajoute un en-tête nommé `X-Custom-Header` avec la valeur `example value`) :

```
var request = event.request;
request.headers['x-custom-header'] = {value: 'example value'};
```

Dupliquer les chaînes de requêtes, les en-têtes et les cookies (tableau **`multiValue`**)

Une requête ou une réponse HTTP peut contenir plusieurs chaînes de requêtes, en-têtes ou cookies portant le même nom. Dans ce cas, les chaînes de requêtes, les en-têtes ou les cookies en double sont regroupés dans un champ de l'objet `request` ou `response`, mais ce champ comporte une

propriété supplémentaire nommée `multiValue`. La propriété `multiValue` contient un tableau avec les valeurs de chacun des en-têtes, cookies ou chaînes de requêtes dupliqués.

Example Exemple

Prenons l'exemple d'une requête HTTP avec les `Accept` en-têtes suivants.

```
Accept: application/json
Accept: application/xml
Accept: text/html
```

Ces en-têtes sont représentés comme suit dans l'`request`objet.

```
"headers": {
    "accept": {
        "value": "application/json",
        "multiValue": [
            {
                "value": "application/json"
            },
            {
                "value": "application/xml"
            },
            {
                "value": "text/html"
            }
        ]
    }
}
```

> **Note**
>
> La première valeur d'en-tête (dans ce cas,`application/json`) est répétée à la fois dans les `multiValue` propriétés `value` et. Cela vous permet d'accéder à toutes les valeurs en faisant une boucle dans le tableau `multiValue`.

Si le code de votre fonction modifie une chaîne de requête, un en-tête ou un cookie contenant un `multiValue` tableau, CloudFront Functions applique les règles suivantes pour appliquer les modifications :

1. Si le tableau `multiValue` existe et comporte des modifications, ces dernières sont appliquées. Le premier élément de la propriété `value` est ignoré.
2. Sinon, toute modification apportée à la propriété `value` est appliquée, et les valeurs suivantes (si elles existent) restent inchangées.

La propriété `multiValue` est utilisée uniquement lorsque la requête ou la réponse HTTP contient des chaînes de requêtes, des en-têtes ou des cookies en double portant le même nom, comme indiqué dans l'exemple précédent. Toutefois, s'il existe plusieurs valeurs dans un seul en-tête, cookie ou chaîne de requête, la propriété `multiValue` n'est pas utilisée.

Example Exemple

Prenons l'exemple d'une demande avec un `Accept` en-tête contenant trois valeurs.

```
Accept: application/json, application/xml, text/html
```

Cet en-tête est représenté comme suit dans l'`request`objet.

```
"headers": {
    "accept": {
        "value": "application/json, application/xml, text/html"
    }
}
```

Attributs de cookies

Dans un en-tête `Set-Cookie` d'une réponse HTTP, l'en-tête contient la paire nom-valeur du cookie et éventuellement un ensemble d'attributs séparés par des points-virgules.

Example Exemple

```
Set-Cookie: cookie1=val1; Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT
```

Dans l'objet `response`, ces attributs sont représentés dans la propriété `attributes` du champ cookie. Par exemple, l'en-tête `Set-Cookie` précédent est représenté comme suit :

```
"cookie1": {
    "value": "val1",
```

```
    "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
}
```

Exemple d'objet de réponse

L'exemple suivant montre un objet `response` (la sortie d'une fonction de réponse d'utilisateur) dans lequel le corps a été remplacé par une fonction de réponse d'utilisateur.

```
{
  "response": {
    "statusCode": 200,
    "statusDescription": "OK",
    "headers": {
      "date": {
        "value": "Mon, 04 Apr 2021 18:57:56 GMT"
      },
      "server": {
        "value": "gunicorn/19.9.0"
      },
      "access-control-allow-origin": {
        "value": "*"
      },
      "access-control-allow-credentials": {
        "value": "true"
      },
      "content-type": {
        "value": "text/html"
      },
      "content-length": {
        "value": "86"
      }
    },
    "cookies": {
      "ID": {
        "value": "id1234",
        "attributes": "Expires=Wed, 05 Apr 2021 07:28:00 GMT"
      },
      "Cookie1": {
        "value": "val1",
        "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT",
        "multiValue": [
```

```
          {
            "value": "val1",
            "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
          },
          {
            "value": "val2",
            "attributes": "Path=/cat; Domain=example.com; Expires=Wed, 10 Jan 2021
 07:28:00 GMT"
          }
        ]
      }
    },

    // Adding the body field is optional and it will not be present in the response
 object
    // unless you specify it in your function.
    // Your function does not have access to the original body returned by the
 CloudFront
    // cache or origin.
    // If you don't specify the body field in your viewer response function, the
 original
    // body returned by the CloudFront cache or origin is returned to viewer.

     "body": {
      "encoding": "text",
      "data": "<!DOCTYPE html><html><body><p>Here is your custom content.</p></body></
html>"
    }
  }
}
```

Exemple d'objet d'événement

L'exemple suivant illustre un objet `event` complet.

> **Note**
>
> L'objet `event` représente l'entrée de votre fonction. Votre fonction renvoie uniquement l'objet `request` ou `response`, et non l'objet `event` complet.

```
{
    "version": "1.0",
    "context": {
        "distributionDomainName": "d111111abcdef8.cloudfront.net",
        "distributionId": "EDFDVBD6EXAMPLE",
        "eventType": "viewer-response",
        "requestId": "EXAMPLEntjQpEXAMPLE_SG5Z-EXAMPLEPmPfEXAMPLEu3EqEXAMPLE=="
    },
    "viewer": {"ip": "198.51.100.11"},
    "request": {
        "method": "GET",
        "uri": "/media/index.mpd",
        "querystring": {
            "ID": {"value": "42"},
            "Exp": {"value": "1619740800"},
            "TTL": {"value": "1440"},
            "NoValue": {"value": ""},
            "querymv": {
                "value": "val1",
                "multiValue": [
                    {"value": "val1"},
                    {"value": "val2,val3"}
                ]
            }
        },
        "headers": {
            "host": {"value": "video.example.com"},
            "user-agent": {"value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
 Gecko/20100101 Firefox/83.0"},
            "accept": {
                "value": "application/json",
                "multiValue": [
                    {"value": "application/json"},
                    {"value": "application/xml"},
                    {"value": "text/html"}
                ]
            },
            "accept-language": {"value": "en-GB,en;q=0.5"},
            "accept-encoding": {"value": "gzip, deflate, br"},
            "origin": {"value": "https://website.example.com"},
            "referer": {"value": "https://website.example.com/videos/12345678?
action=play"},
            "cloudfront-viewer-country": {"value": "GB"}
```

```
        },
        "cookies": {
            "Cookie1": {"value": "value1"},
            "Cookie2": {"value": "value2"},
            "cookie_consent": {"value": "true"},
            "cookiemv": {
                "value": "value3",
                "multiValue": [
                    {"value": "value3"},
                    {"value": "value4"}
                ]
            }
        }
    },
    "response": {
        "statusCode": 200,
        "statusDescription": "OK",
        "headers": {
            "date": {"value": "Mon, 04 Apr 2021 18:57:56 GMT"},
            "server": {"value": "gunicorn/19.9.0"},
            "access-control-allow-origin": {"value": "*"},
            "access-control-allow-credentials": {"value": "true"},
            "content-type": {"value": "application/json"},
            "content-length": {"value": "701"}
        },
        "cookies": {
            "ID": {
                "value": "id1234",
                "attributes": "Expires=Wed, 05 Apr 2021 07:28:00 GMT"
            },
            "Cookie1": {
                "value": "val1",
                "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr
2021 07:28:00 GMT",
                "multiValue": [
                    {
                        "value": "val1",
                        "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed,
05 Apr 2021 07:28:00 GMT"
                    },
                    {
                        "value": "val2",
                        "attributes": "Path=/cat; Domain=example.com; Expires=Wed, 10
Jan 2021 07:28:00 GMT"
```

```
                    }
                ]
            }
        }
    }
}
```

JavaScript fonctionnalités d'exécution pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 12.

Pour la plupart des up-to-date fonctionnalités, nous vous recommandons JavaScript d'utiliser Runtime 2.0.

Les fonctionnalités JavaScript d'exécution 2.0 présentent les modifications suivantes par rapport à la version 1.0 :

- Les méthodes du module tampon sont disponibles
- Les méthodes de prototype de chaîne non standard suivantes ne sont pas disponibles :
  - `String.prototype.bytesFrom()`
  - `String.prototype.fromBytes()`
  - `String.prototype.fromUTF8()`
  - `String.prototype.toBytes()`
  - `String.prototype.toUTF8()`
- Voici les nouveautés du module cryptographique :
  - `hash.digest()`— Le type de retour est changé en `Buffer` si aucun encodage n'est fourni
  - `hmac.digest()`— Le type de retour est changé en `Buffer` si aucun encodage n'est fourni
- Pour plus d'informations sur les nouvelles fonctionnalités supplémentaires, consultezJavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

Rubriques

- JavaScript fonctionnalités de Runtime 1.0 pour CloudFront Functions
- JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions

JavaScript fonctionnalités de Runtime 1.0 pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 9. Il fournit également des méthodes non standard qui ne font pas partie des spécifications ES.

Les rubriques suivantes répertorient toutes les fonctions de langages prises en charge.

Rubriques

Fonctions de base

Les fonctions de base suivantes d'ES sont prises en charge.

Types

Tous les types ES 5.1 sont pris en charge, notamment les valeurs booléennes, les nombres, les chaînes, les objets, les tableaux, les fonctions, les constructeurs de fonctions et les expressions régulières.

Opérateurs

Tous les opérateurs ES 5.1 sont pris en charge.

L'opérateur d'exponentiation ES 7 (`**`) est pris en charge.

Instructions

> **Note**
>
> Les instructions `const` et `let` ne sont pas prises en charge.

Les instructions ES 5.1 suivantes sont prises en charge :

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`
- `for`
- `for-in`
- `if`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`
- Instructions étiquetées

Littéraux

Les littéraux de modèles ES 6 sont pris en charge : chaînes multiligne, interpolation d'expression et modèles d'imbrication.

Fonctions

Toutes les fonctions ES 5.1 sont prises en charge.

Les fonctions de flèche ES 6 ainsi que la syntaxe des paramètres du reste ES 6 sont prises en charge.

Unicode

Le texte source et les littéraux de chaînes peuvent contenir des caractères Unicode. Les séquences d'échappement de points de code Unicode de six caractères (par exemple `\uXXXX`) sont également prises en charge.

Mode strict

Les fonctions opèrent en mode strict par défaut. Vous n’avez donc pas besoin d’ajouter une instruction `use strict` dans votre code de fonction. Elles ne peuvent pas être modifiées.

Objets primitifs

Les objets primitifs suivants d'ES sont pris en charge.

Objet

Les méthodes ES 5.1 suivantes sur les objets sont prises en charge :

- `create` (sans liste de propriétés)
- `defineProperties`
- `defineProperty`
- `freeze`
- `getOwnPropertyDescriptor`
- `getOwnPropertyNames`
- `getPrototypeOf`
- `hasOwnProperty`
- `isExtensible`
- `isFrozen`
- `prototype.isPrototypeOf`
- `isSealed`
- `keys`
- `preventExtensions`
- `prototype.propertyIsEnumerable`
- `seal`
- `prototype.toString`
- `prototype.valueOf`

Les méthodes ES 6 suivantes sur les objets sont prises en charge :

- `assign`

- `is`
- `prototype.setPrototypeOf`

Les méthodes ES 8 suivantes sur les objets sont prises en charge :

- `entries`
- `values`

String

Les méthodes ES 5.1 suivantes sur les chaînes sont prises en charge :

- `fromCharCode`
- `prototype.charAt`
- `prototype.concat`
- `prototype.indexOf`
- `prototype.lastIndexOf`
- `prototype.match`
- `prototype.replace`
- `prototype.search`
- `prototype.slice`
- `prototype.split`
- `prototype.substr`
- `prototype.substring`
- `prototype.toLowerCase`
- `prototype.trim`
- `prototype.toUpperCase`

Les méthodes ES 6 suivantes sur les chaînes sont prises en charge :

- `fromCodePoint`
- `prototype.codePointAt`
- `prototype.endsWith`
- `prototype.includes`
- `prototype.repeat`

- `prototype.startsWith`

Les méthodes ES 8 suivantes sur les chaînes sont prises en charge :

- `prototype.padStart`
- `prototype.padEnd`

Les méthodes ES 9 suivantes sur les chaînes sont prises en charge :

- `prototype.trimStart`
- `prototype.trimEnd`

Les méthodes non standard suivantes sur les chaînes sont prises en charge :

- `prototype.bytesFrom(`*`array | string, encoding`*`)`

  Crée une chaîne d'octets à partir d'un tableau d'octets ou d'une chaîne encodée. Les options d'encodage de chaînes sont `hex`, `base64` et `base64url`.

- `prototype.fromBytes(`*`start`*`[, `*`end`*`])`

  Crée une chaîne Unicode à partir d'une chaîne d'octets où chaque octet est remplacé par le point de code Unicode correspondant.

- `prototype.fromUTF8(`*`start`*`[, `*`end`*`])`

  Crée une chaîne Unicode à partir d'une chaîne d'octets encodée en UTF-8. Si l'encodage est incorrect, il renvoie `null`.

- `prototype.toBytes(start[, end])`

  Crée une chaîne d'octets à partir d'une chaîne Unicode. Tous les caractères doivent être dans la plage [0,255]. Dans le cas contraire, `null` est renvoyé.

- `prototype.toUTF8(start[, `*`end`*`])`

  Crée une chaîne d'octets encodée en UTF-8 à partir d'une chaîne Unicode.

Nombre

Toutes les méthodes ES 5.1 sur les nombres sont prises en charge.

Les méthodes ES 6 suivantes sur les nombres sont prises en charge :

- `isFinite`
- `isInteger`

- `isNaN`
- `isSafeInteger`
- `parseFloat`
- `parseInt`
- `prototype.toExponential`
- `prototype.toFixed`
- `prototype.toPrecision`
- `EPSILON`
- `MAX_SAFE_INTEGER`
- `MAX_VALUE`
- `MIN_SAFE_INTEGER`
- `MIN_VALUE`
- `NEGATIVE_INFINITY`
- `NaN`
- `POSITIVE_INFINITY`

Objets intégrés

Les objets intégrés suivants d'ES sont pris en charge.

Mathématiques

Toutes les méthodes mathématiques ES 5.1 sont prises en charge.

> **Note**
>
> Dans l'environnement d'exécution de CloudFront Functions, l'`Math.random()`implémentation utilise `arc4random` OpenBSD prédéfini avec l'horodatage de l'exécution de la fonction.

Les méthodes mathématiques ES 6 suivantes sont prises en charge :

- `acosh`
- `asinh`

- `atanh`
- `cbrt`
- `clz32`
- `cosh`
- `expm1`
- `fround`
- `hypot`
- `imul`
- `log10`
- `log1p`
- `log2`
- `sign`
- `sinh`
- `tanh`
- `trunc`
- `E`
- `LN10`
- `LN2`
- `LOG10E`
- `LOG2E`
- `PI`
- `SQRT1_2`
- `SQRT2`

Date

Toutes les fonctions `Date` ES 5.1 sont prises en charge.

> **Note**
>
> Pour des raisons de sécurité, `Date` renvoie toujours la même valeur (l'heure de début de la fonction) pendant la durée de vie d'une même exécution de la fonction. Pour plus d'informations, consultez Fonctions limitées.

Fonction

Les méthodes `apply`, `bind` et `call` sont prises en charge.

Les constructeurs de fonctions ne sont pas pris en charge.

Expressions régulières

Toutes les fonctions d'expression régulière ES 5.1 sont prises en charge. Le langage d’expression régulière est compatible Perl. Les groupes de capture nommés ES 9 sont pris en charge.

JSON

Toutes les fonctions JSON ES 5.1 sont prises en charge, notamment `parse` et `stringify`.

Array

Les méthodes ES 5.1 suivantes sur les tableaux sont prises en charge :

- `isArray`
- `prototype.concat`
- `prototype.every`
- `prototype.filter`
- `prototype.forEach`
- `prototype.indexOf`
- `prototype.join`
- `prototype.lastIndexOf`
- `prototype.map`
- `prototype.pop`
- `prototype.push`
- `prototype.reduce`
- `prototype.reduceRight`
- `prototype.reverse`
- `prototype.shift`
- `prototype.slice`
- `prototype.some`

- `prototype.sort`
- `prototype.splice`
- `prototype.unshift`

Les méthodes ES 6 suivantes sur les tableaux sont prises en charge :

- `of`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.find`
- `prototype.findIndex`

Les méthodes ES 7 suivantes sur les tableaux sont prises en charge :

- `prototype.includes`

Tableaux typés

Les tableaux typés ES 6 suivants sont pris en charge :

- `Int8Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Int16Array`
- `Uint16Array`
- `Int32Array`
- `Uint32Array`
- `Float32Array`
- `Float64Array`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.join`
- `prototype.set`
- `prototype.slice`
- `prototype.subarray`

- `prototype.toString`

ArrayBuffer

Les méthodes suivantes sur `ArrayBuffer` sont prises en charge :

- `prototype.isView`
- `prototype.slice`

Promesse

Les méthodes suivantes sur les promesses sont prises en charge :

- `reject`
- `resolve`
- `prototype.catch`
- `prototype.finally`
- `prototype.then`

Cryptographie

Le module cryptographique fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`. Le module fournit les méthodes suivantes, qui se comportent exactement comme leurs homologues Node.js :

- `createHash(`*`algorithm`*`)`
- `hash.update(`*`data`*`)`
- `hash.digest([`*`encoding`*`])`
- `createHmac(`*`algorithm, secret key`*`)`
- `hmac.update(`*`data`*`)`
- `hmac.digest([`*`encoding`*`])`

Pour plus d'informations, consultez Cryptographie (hachage et HMAC) dans la section Modules intégrés.

Console

Il s'agit d'un objet d'aide pour le débogage. Il ne prend en charge que la méthode `log()`, pour enregistrer les messages de journaux.

> **Note**
>
> CloudFront Les fonctions ne prennent pas en charge la syntaxe des virgules, telle que`console.log('a', 'b')`. Utilisez plutôt le `console.log('a' + ' ' + 'b')` format.

Types d'erreurs

Les objets d'erreurs suivants sont pris en charge :

- `Error`
- `EvalError`
- `InternalError`
- `MemoryError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

L'objet `globalThis` est pris en charge.

Les fonctions globales ES 5.1 suivantes sont prises en charge :

- `decodeURI`
- `decodeURIComponent`
- `encodeURI`
- `encodeURIComponent`
- `isFinite`
- `isNaN`
- `parseFloat`

- `parseInt`

Les constantes globales suivantes sont prises en charge :

- `NaN`
- `Infinity`
- `undefined`

Modules intégrés

Les modules intégrés suivants sont pris en charge.

Modules

- Cryptographie (hachage et HMAC)
- Chaîne de requête

Cryptographie (hachage et HMAC)

Le module cryptographique (`crypto`) fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`. Le module fournit les méthodes suivantes, qui se comportent exactement comme leurs homologues Node.js.

Méthodes de hachage

`crypto.createHash(`*`algorithm`*`)`

Crée et renvoie un objet de hachage que vous pouvez utiliser pour générer des résumés de hachage à l'aide de l'algorithme donné : `md5`, `sha1` ou `sha256`.

`hash.update(`*`data`*`)`

Met à jour le contenu de hachage avec les `data` données

`hash.digest([`*`encoding`*`])`

Calcule le résumé de toutes les données transmises à l'aide de `hash.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Méthodes HMAC

`crypto.createHmac(algorithm, secret key)`

Crée et renvoie un objet HMAC qui utilise le `algorithm` et la `secret key` données. L'algorithme peut être `md5`, `sha1` ou `sha256`.

`hmac.update(data)`

Met à jour le contenu HMAC avec les `data` données.

`hmac.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hmac.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Chaîne de requête

> **Note**
>
> L'objet d'événement CloudFront Functions analyse automatiquement les chaînes de requête d'URL pour vous. Cela signifie que, dans la plupart des cas, vous n'avez pas besoin d'utiliser ce module.

Le module de chaînes de requêtes (`querystring`) fournit des méthodes d'analyse et de formatage des chaînes de requêtes URL. Vous pouvez charger le module en utilisant `require('querystring')`. Le module fournit les méthodes suivantes :

`querystring.escape(string)`

Encode par URL la `string` donnée, en renvoyant une chaîne de requêtes échappée. La méthode est utilisée par `querystring.stringify()` et ne doit pas être utilisée directement.

`querystring.parse(string[, separator[, equal[, options]]])`

Analyse une chaîne de requêtes (`string`) et renvoie un objet.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`decodeURIComponent` *function*

Fonction pour décoder les caractères encodés en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.unescape()`.

`maxKeys` *number*

Nombre maximal de clés à analyser. Par défaut, il s'agit de `1000`. Utilisez une valeur de `0` pour supprimer les limitations pour le comptage des clés.

Par défaut, les caractères encodés en pourcentage dans la chaîne de requêtes sont supposés utiliser l'encodage UTF-8. Les séquences UTF-8 non valides sont remplacées par le caractère de remplacement `U+FFFD`.

Par exemple, pour la chaîne de requêtes suivante :

```
'name=value&abc=xyz&abc=123'
```

La valeur renvoyée de `querystring.parse()` est :

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` est un alias pour `querystring.parse()`.

`querystring.stringify(`*object*`[, `*separator*`[, `*equal*`[, `*options*`]]])`

Sérialise un `object` et renvoie une chaîne de requêtes.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de `&`.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de `=`.

Le paramètre `options` est un objet avec les clés suivantes :

`encodeURIComponent` *function*

Fonction à utiliser pour convertir des caractères non sûrs pour une URL en encodage en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.escape()`.

Par défaut, les caractères qui nécessitent un encodage en pourcentage dans la chaîne de requêtes sont encodés en UTF-8. Pour utiliser un encodage différent, spécifiez l'option `encodeURIComponent`.

Par exemple, pour le code suivant :

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

La valeur renvoyée est :

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` est un alias pour `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Décode les caractères encodés en pourcentage URL dans la `string` donnée, en renvoyant une chaîne de requêtes non échappée. Cette méthode est utilisée par `querystring.parse()` et ne doit pas être utilisée directement.

Fonctions limitées

Les fonctionnalités JavaScript linguistiques suivantes ne sont pas prises en charge ou sont restreintes pour des raisons de sécurité.

Évaluation dynamique du code

L'évaluation dynamique du code n'est pas prise en charge. Les deux constructeurs `eval()` et `Function` renvoient une erreur en cas de tentative. Par exemple, `const sum = new Function('a', 'b', 'return a + b')` renvoie une erreur.

Temporisateurs

Les fonctions `setTimeout()`, `setImmediate()` et `clearTimeout()` ne sont pas prises en charge. Il n'y a aucune disposition relative au report ou au produit dans une exécution de fonction. Votre fonction doit s'exécuter de manière synchrone jusqu'à la fin.

Horodatages

Pour des raisons de sécurité, il n'y a pas d'accès aux temporisateurs haute résolution. Toutes les méthodes `Date` pour interroger l'heure actuelle retournent toujours la même valeur pendant la

durée de vie d'une même exécution de la fonction. L'horodatage renvoyé est l'heure à laquelle la fonction a commencé à s'exécuter. Par conséquent, vous ne pouvez pas mesurer le temps écoulé dans votre fonction.

Accès au système de fichiers

Il n'y a pas d'accès au système de fichiers. Par exemple, il n'y a pas de module `fs` pour l'accès au système de fichiers comme dans Node.js.

Accès réseau

Les appels réseau ne sont pas pris en charge. Par exemple, XHR, HTTP(S) et socket ne sont pas pris en charge.

JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 12. Il fournit également des méthodes non standard qui ne font pas partie des spécifications ES. Les rubriques suivantes répertorient toutes les fonctionnalités de cet environnement d'exécution.

Rubriques

- Fonctions de base
- Objets primitifs
- Objets intégrés
- Types d'erreurs
- Globals
- Modules intégrés
- Fonctions limitées

Fonctions de base

Les fonctions de base suivantes d'ES sont prises en charge.

Types

Tous les types ES 5.1 sont pris en charge, notamment les valeurs booléennes, les nombres, les chaînes, les objets, les tableaux, les fonctions et les expressions régulières.

Opérateurs

Tous les opérateurs ES 5.1 sont pris en charge.

L'opérateur d'exponentiation ES 7 (`**`) est pris en charge.

Instructions

Les instructions ES 5.1 suivantes sont prises en charge :

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`
- `for`
- `for-in`
- `if`
- `label`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`

Les instructions ES 6 suivantes sont prises en charge :

- `async`
- `await`
- `const`
- `let`

> **Note**
>
> `async`, `awaitconst`, et `let` sont nouveaux dans JavaScript Runtime 2.0.

Littéraux

Les littéraux de modèles ES 6 sont pris en charge : chaînes multiligne, interpolation d'expression et modèles d'imbrication.

Fonctions

Toutes les fonctions ES 5.1 sont prises en charge.

Les fonctions de flèche ES 6 ainsi que la syntaxe des paramètres du reste ES 6 sont prises en charge.

Unicode

Le texte source et les littéraux de chaînes peuvent contenir des caractères Unicode. Les séquences d'échappement de points de code Unicode de six caractères (par exemple \uXXXX) sont également prises en charge.

Mode strict

Les fonctions opèrent en mode strict par défaut. Vous n'avez donc pas besoin d'ajouter une instruction `use strict` dans votre code de fonction. Elles ne peuvent pas être modifiées.

Objets primitifs

Les objets primitifs suivants d'ES sont pris en charge.

Objet

Les méthodes ES 5.1 suivantes sur les objets sont prises en charge :

- `Object.create()` (sans liste de propriétés)
- `Object.defineProperties()`
- `Object.defineProperty()`
- `Object.freeze()`
- `Object.getOwnPropertyDescriptor()`
- `Object.getOwnPropertyDescriptors()`
- `Object.getOwnPropertyNames()`
- `Object.getPrototypeOf()`
- `Object.isExtensible()`

- `Object.isFrozen()`
- `Object.isSealed()`
- `Object.keys()`
- `Object.preventExtensions()`
- `Object.seal()`

Les méthodes ES 6 suivantes sur les objets sont prises en charge :

- `Object.assign()`

Les méthodes ES 8 suivantes sur les objets sont prises en charge :

- `Object.entries()`
- `Object.values()`

Les méthodes de prototype d'ES 5.1 suivantes sur les objets sont prises en charge :

- `Object.prototype.hasOwnProperty()`
- `Object.prototype.isPrototypeOf()`
- `Object.prototype.propertyIsEnumerable()`
- `Object.prototype.toString()`
- `Object.prototype.valueOf()`

Les méthodes de prototype d'ES 6 suivantes sur les objets sont prises en charge :

- `Object.prototype.is()`
- `Object.prototype.setPrototypeOf()`

String

Les méthodes ES 5.1 suivantes sur les chaînes sont prises en charge :

- `String.fromCharCode()`

Les méthodes ES 6 suivantes sur les chaînes sont prises en charge :

- `String.fromCodePoint()`

Les méthodes de prototype d'ES 5.1 suivantes sur les chaînes sont prises en charge :

- `String.prototype.charAt()`
- `String.prototype.concat()`
- `String.prototype.indexOf()`

- `String.prototype.lastIndexOf()`
- `String.prototype.match()`
- `String.prototype.replace()`
- `String.prototype.search()`
- `String.prototype.slice()`
- `String.prototype.split()`
- `String.prototype.substr()`
- `String.prototype.substring()`
- `String.prototype.toLowerCase()`
- `String.prototype.trim()`
- `String.prototype.toUpperCase()`

Les méthodes de prototype d'ES 6 suivantes sur les chaînes sont prises en charge :

- `String.prototype.codePointAt()`
- `String.prototype.endsWith()`
- `String.prototype.includes()`
- `String.prototype.repeat()`
- `String.prototype.startsWith()`

Les méthodes de prototype d'ES 8 suivantes sur les chaînes sont prises en charge :

- `String.prototype.padStart()`
- `String.prototype.padEnd()`

Les méthodes de prototype d'ES 9 suivantes sur les chaînes sont prises en charge :

- `String.prototype.trimStart()`
- `String.prototype.trimEnd()`

Les méthodes de prototype d'ES 12 suivantes sur les chaînes sont prises en charge :

- `String.prototype.replaceAll()`

> **Note**
>
> `String.prototype.replaceAll()`est nouveau dans JavaScript Runtime 2.0.

Nombre

TOUS les nombres d'ES 5 sont pris en charge.

Les propriétés d'ES 6 suivantes sur les nombres sont prises en charge :

- `Number.EPSILON`
- `Number.MAX_SAFE_INTEGER`
- `Number.MIN_SAFE_INTEGER`
- `Number.MAX_VALUE`
- `Number.MIN_VALUE`
- `Number.NaN`
- `Number.NEGATIVE_INFINITY`
- `Number.POSITIVE_INFINITY`

Les méthodes ES 6 suivantes sur les nombres sont prises en charge :

- `Number.isFinite()`
- `Number.isInteger()`
- `Number.isNaN()`
- `Number.isSafeInteger()`
- `Number.parseInt()`
- `Number.parseFloat()`

Les méthodes de prototype d'ES 5.1 suivantes sur les nombres sont prises en charge :

- `Number.prototype.toExponential()`
- `Number.prototype.toFixed()`
- `Number.prototype.toPrecision()`

Les séparateurs numériques d'ES 12 sont pris en charge.

> **Note**
>
> Les séparateurs numériques ES 12 sont nouveaux dans JavaScript Runtime 2.0.

Objets intégrés

Les objets intégrés suivants d'ES sont pris en charge.

Mathématiques

Toutes les méthodes mathématiques ES 5.1 sont prises en charge.

> **Note**
>
> Dans l'environnement d'exécution de CloudFront Functions, l'`Math.random()`implémentation utilise `arc4random` OpenBSD prédéfini avec l'horodatage de l'exécution de la fonction.

Les propriétés mathématiques d’ES 6 suivantes sont prises en charge :

- `Math.E`
- `Math.LN10`
- `Math.LN2`
- `Math.LOG10E`
- `Math.LOG2E`
- `Math.PI`
- `Math.SQRT1_2`
- `Math.SQRT2`

Les méthodes mathématiques ES 6 suivantes sont prises en charge :

- `Math.abs()`
- `Math.acos()`
- `Math.acosh()`
- `Math.asin()`
- `Math.asinh()`
- `Math.atan()`
- `Math.atan2()`
- `Math.atanh()`

- `Math.cbrt()`
- `Math.ceil()`
- `Math.clz32()`
- `Math.cos()`
- `Math.cosh()`
- `Math.exp()`
- `Math.expm1()`
- `Math.floor()`
- `Math.fround()`
- `Math.hypot()`
- `Math.imul()`
- `Math.log()`
- `Math.log1p()`
- `Math.log2()`
- `Math.log10()`
- `Math.max()`
- `Math.min()`
- `Math.pow()`
- `Math.random()`
- `Math.round()`
- `Math.sign()`
- `Math.sinh()`
- `Math.sin()`
- `Math.sqrt()`
- `Math.tan()`
- `Math.tanh()`
- `Math.trunc()`

Date

Toutes les fonctions `Date` ES 5.1 sont prises en charge.

> **Note**
>
> Pour des raisons de sécurité, `Date` renvoie toujours la même valeur (l'heure de début de la fonction) pendant la durée de vie d'une même exécution de la fonction. Pour plus d'informations, consultez Fonctions limitées.

Fonction

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `Function.prototype.apply()`
- `Function.prototype.bind()`
- `Function.prototype.call()`

Les constructeurs de fonctions ne sont pas pris en charge.

Expressions régulières

Toutes les fonctions d'expression régulière ES 5.1 sont prises en charge. Le langage d'expression régulière est compatible Perl.

Les propriétés d'accesseur de prototype d'ES 5.1 suivantes sont prises en charge :

- `RegExp.prototype.global`
- `RegExp.prototype.ignoreCase`
- `RegExp.protoype.multiline`
- `RegExp.protoype.source`
- `RegExp.prototype.sticky`
- `RegExp.prototype.flags`

> **Note**
>
> `RegExp.prototype.sticky`et `RegExp.prototype.flags` sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `RegExp.prototype.exec()`

- `RegExp.prototype.test()`
- `RegExp.prototype.toString()`
- `RegExp.prototype[@@replace]()`
- `RegExp.prototype[@@split]()`

> **Note**
>
> `RegExp.prototype[@@split]()`est nouveau dans JavaScript Runtime 2.0.

Les propriétés d'instance d'ES 5.1 suivantes sont prises en charge :

- `lastIndex`

Les groupes de capture nommés ES 9 sont pris en charge.

JSON

Les méthodes d'ES 5.1 suivantes sont prises en charge :

- `JSON.parse()`
- `JSON.stringify()`

Array

Les méthodes ES 5.1 suivantes sur les tableaux sont prises en charge :

- `Array.isArray()`

Les méthodes ES 6 suivantes sur les tableaux sont prises en charge :

- `Array.of()`

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `Array.prototype.concat()`
- `Array.prototype.every()`
- `Array.prototype.filter()`
- `Array.prototype.forEach()`
- `Array.prototype.indexOf()`
- `Array.prototype.join()`
- `Array.prototype.lastIndexOf()`

- `Array.prototype.map()`
- `Array.prototype.pop()`
- `Array.prototype.push()`
- `Array.prototype.reduce()`
- `Array.prototype.reduceRight()`
- `Array.prototype.reverse()`
- `Array.prototype.shift()`
- `Array.prototype.slice()`
- `Array.prototype.some()`
- `Array.prototype.sort()`
- `Array.prototype.splice()`
- `Array.prototype.unshift()`

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `Array.prototype.copyWithin()`
- `Array.prototype.fill()`
- `Array.prototype.find()`
- `Array.prototype.findIndex()`

Les méthodes de prototype d'ES 7 suivantes sont prises en charge :

- `Array.prototype.includes()`

Tableaux typés

Les constructeurs de tableaux typés d'ES 6 suivants sont pris en charge :

- `Float32Array`
- `Float64Array`
- `Int8Array`
- `Int16Array`
- `Int32Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Uint16Array`

- `Uint32Array`

Les méthodes d'ES 6 suivantes sont prises en charge :

- `TypedArray.from()`
- `TypedArray.of()`

> **Note**
>
> `TypedArray.from()`et `TypedArray.of()` sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `TypedArray.prototype.copyWithin()`
- `TypedArray.prototype.every()`
- `TypedArray.prototype.fill()`
- `TypedArray.prototype.filter()`
- `TypedArray.prototype.find()`
- `TypedArray.prototype.findIndex()`
- `TypedArray.prototype.forEach()`
- `TypedArray.prototype.includes()`
- `TypedArray.prototype.indexOf()`
- `TypedArray.prototype.join()`
- `TypedArray.prototype.lastIndexOf()`
- `TypedArray.prototype.map()`
- `TypedArray.prototype.reduce()`
- `TypedArray.prototype.reduceRight()`
- `TypedArray.prototype.reverse()`
- `TypedArray.prototype.some()`
- `TypedArray.prototype.set()`
- `TypedArray.prototype.slice()`
- `TypedArray.prototype.sort()`
- `TypedArray.prototype.subarray()`

- `TypedArray.prototype.toString()`

> **Note**
>
> `TypedArray.prototype.every()`,`TypedArray.prototype.fill()`,`TypedArray.proto`
> et `TypedArray.prototype.some()` sont nouveaux dans JavaScript Runtime 2.0.

ArrayBuffer

Les méthodes ES 6 suivantes ArrayBuffer sont prises en charge :

- `isView()`

Les méthodes de prototypage ES 6 suivantes ArrayBuffer sont prises en charge :

- `ArrayBuffer.prototype.slice()`

Promesse

Les méthodes d'ES 6 suivantes sur les promesses sont prises en charge :

- `Promise.all()`
- `Promise.allSettled()`
- `Promise.any()`
- `Promise.reject()`
- `Promise.resolve()`
- `Promise.race()`

> **Note**
>
> `Promise.all()`, `Promise.allSettled()Promise.any()`, et `Promise.race()`
> sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 6 suivantes sur les promesses sont prises en charge :

- `Promise.prototype.catch()`
- `Promise.prototype.finally()`
- `Promise.prototype.then()`

DataView

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `DataView.prototype.getFloat32()`
- `DataView.prototype.getFloat64()`
- `DataView.prototype.getInt16()`
- `DataView.prototype.getInt32()`
- `DataView.prototype.getInt8()`
- `DataView.prototype.getUint16()`
- `DataView.prototype.getUint32()`
- `DataView.prototype.getUint8()`
- `DataView.prototype.setFloat32()`
- `DataView.prototype.setFloat64()`
- `DataView.prototype.setInt16()`
- `DataView.prototype.setInt32()`
- `DataView.prototype.setInt8()`
- `DataView.prototype.setUint16()`
- `DataView.prototype.setUint32()`
- `DataView.prototype.setUint8()`

> **Note**
>
> Toutes les méthodes de prototypage de Dataview ES 6 sont nouvelles dans JavaScript Runtime 2.0.

Symbol

Les méthodes d'ES 6 suivantes sont prises en charge :

- `Symbol.for()`
- `Symbol.keyfor()`

> **Note**
>
> Toutes les méthodes Symbol ES 6 sont nouvelles dans JavaScript Runtime 2.0.

TextDecoder

Les méthodes de prototype suivantes sont prises en charge :

- `TextDecoder.prototype.decode()`

Les propriétés d'accesseur de prototype suivantes sont prises en charge :

- `TextDecoder.prototype.encoding`
- `TextDecoder.prototype.fatal`
- `TextDecoder.prototype.ignoreBOM`

TextEncoder

Les méthodes de prototype suivantes sont prises en charge :

- `TextEncoder.prototype.encode()`
- `TextEncoder.prototype.encodeInto()`

Types d'erreurs

Les objets d'erreurs suivants sont pris en charge :

- `Error`
- `EvalError`
- `InternalError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

L'objet `globalThis` est pris en charge.

Les fonctions globales ES 5.1 suivantes sont prises en charge :

- `decodeURI()`
- `decodeURIComponent()`
- `encodeURI()`

- `encodeURIComponent()`
- `isFinite()`
- `isNaN()`
- `parseFloat()`
- `parseInt()`

Les fonctions globales d'ES 6 suivantes sont prises en charge :

- `atob()`
- `btoa()`

> **Note**
>
> `atob()`et `btoa()` sont nouveaux dans JavaScript Runtime 2.0.

Les constantes globales suivantes sont prises en charge :

- `NaN`
- `Infinity`
- `undefined`
- `arguments`

Modules intégrés

Les modules intégrés suivants sont pris en charge.

Modules

- Buffer
- Chaîne de requête
- Cryptographie

Buffer

Le module fournit les méthodes suivantes :

- `Buffer.alloc(size[, fill[, encoding]])`

  Allouez un élément `Buffer`.

  - `size` : taille du tampon. Entrez un entier.
  - `fill` : facultatif. Entrez une chaîne, un élément `Buffer`, un élément Uint8Array ou un entier. La valeur par défaut est `0`.
  - `encoding` : facultatif. Quand `fill` est une chaîne, entrez l'une des valeurs suivantes : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.allocUnsafe(size)`

  Allouez un élément `Buffer` non initialisé.

  - `size` : entrez un entier.
- `Buffer.byteLength(value[, encoding])`

  Renvoie la longueur d'une valeur, en octets.

  - `value`: chaîne, `Buffer` TypedArray, Dataview ou Arraybuffer.
  - `encoding` : Facultatif. Quand `value` est une chaîne, entrez l'une des valeurs suivantes : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.compare(buffer1, buffer2)`

  Comparez deux éléments `Buffer` pour faciliter le tri des tableaux. Renvoie `0` s'ils sont identiques, `-1` si `buffer1` figure en premier, ou `1` si `buffer2` figure en premier.

  - `buffer1` : entrez un élément `Buffer`.
  - `buffer2` : entrez un autre élément `Buffer`.
- `Buffer.concat(list[, totalLength])`

  Concaténez plusieurs éléments `Buffer`. Renvoie `0` s'il n'y en a aucun. Renvoie jusqu'à `totalLength`.

  - `list` : entrez une liste d'éléments `Buffer`. Notez que cela sera tronqué à `totalLength`.
  - `totalLength` : facultatif. Entrez un entier non signé. Utilisez la somme des instances `Buffer` dans la liste si le paramètre est vide.
- `Buffer.from(array)`

  Créez un élément `Buffer` à partir d'un tableau.

  - `array` : entrez un tableau d'octets de `0` à `255`.

- `Buffer.from(arrayBuffer, byteOffset[, length]))`

  Créez une vue à partir de `arrayBuffer`, en commençant par le décalage `byteOffset` avec la longueur `length`.

  - `arrayBuffer` : entrez un tableau `Buffer`.
  - `byteOffset` : entrez un entier.
  - `length` : facultatif. Entrez un entier.
- `Buffer.from(buffer)`

  Créez une copie de l'élément `Buffer`.

  - `buffer` : entrez un élément `Buffer`.
- `Buffer.from(object[, offsetOrEncoding[, length]])`

  Créez un élément `Buffer` à partir d'un objet. Renvoie `Buffer.from(object.valueOf(), offsetOrEncoding, length)` si `valueOf()` n'est pas égal à l'objet.

  - `object` : entrez un objet.
  - `offsetOrEncoding` : facultatif. Entrez un entier ou une chaîne d'encodage.
  - `length` : facultatif. Entrez un entier.
- `Buffer.from(string[, encoding])`

  Créez un élément `Buffer` à partir d'une chaîne.

  - `string` : entrez une chaîne.
  - `encoding` : Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.isBuffer(object)`

  Vérifiez si `object` est un tampon. Renvoie `true` ou `false`.

  - `object` : entrez un objet.
- `Buffer.isEncoding(encoding)`

  Vérifiez si `encoding` est pris en charge. Renvoie `true` ou `false`.

  - `encoding` : Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.

Le module fournit les méthodes de prototype de tampon suivantes :

- `Buffer.prototype.compare(target[, targetStart[, targetEnd[, sourceStart[, sourceEnd]]]])`

  Comparez `Buffer` avec la cible. Renvoie `0` s'ils sont identiques, `1` si `buffer` figure en premier, ou `-1` si `target` figure en premier.

  - `target` : entrez un élément `Buffer`.
  - `targetStart` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `targetEnd` : facultatif. Entrez un entier. La valeur par défaut est la longueur `target`.
  - `sourceStart` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceEnd` : facultatif. Entrez un entier. La valeur par défaut est la longueur de `Buffer`.
- `Buffer.prototype.copy(target[, targetStart[, sourceStart[, sourceEnd]]])`

  Copiez le tampon dans `target`.

  - `target` : entrez un élément `Buffer` ou `Uint8Array`.
  - `targetStart` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceStart` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceEnd` : facultatif. Entrez un entier. La valeur par défaut est la longueur de `Buffer`.
- `Buffer.prototype.equals(otherBuffer)`

  Comparez `Buffer` à `otherBuffer`. Renvoie `true` ou `false`.

  - `otherBuffer` : entrez une chaîne.
- `Buffer.prototype.fill(value[, offset[, end][, encoding])`

  Remplissez `Buffer` avec `value`.

  - `value` : entrez une chaîne, `Buffer` ou un entier.
  - `offset` : facultatif. Entrez un entier.
  - `end` : facultatif. Entrez un entier.
  - `encoding` : facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.includes(value[, byteOffset][, encoding])`

  Recherchez `value` dans `Buffer`. Renvoie `true` ou `false`.

  - `value` : entrez une chaîne, un élément `Buffer`, `Uint8Array` ou un entier.
  - `byteOffset` : facultatif. Entrez un entier.

  - `encoding` : facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.indexOf(value[, byteOffset][, encoding])`

  Recherchez le premier élément `value` dans `Buffer`. Retourne `index` s'il est trouvé ou `-1` dans le cas contraire.
  - `value` : entrez une chaîne, `Buffer`, Unit8Array ou un entier compris entre 0 et 255.
  - `byteOffset` : facultatif. Entrez un entier.
  - `encoding` : facultatif. Entrez l'un des éléments suivants si `value` est une chaîne : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.lastIndexOf(value[, byteOffset][, encoding])`

  Recherchez le dernier élément `value` dans `Buffer`. Retourne `index` s'il est trouvé ou `-1` dans le cas contraire.
  - `value` : entrez une chaîne, `Buffer`, Unit8Array ou un entier compris entre 0 et 255.
  - `byteOffset` : facultatif. Entrez un entier.
  - `encoding` : facultatif. Entrez l'un des éléments suivants si `value` est une chaîne : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.readInt8(offset)`

  Lisez `Int8` à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
- `Buffer.prototype.readIntBE(offset, byteLength)`

  Lisez `Int` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
  - `byteLength` : facultatif. Entrez un entier compris entre 1 et 6.
- `Buffer.prototype.readInt16BE(offset)`

  Lisez `Int16` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
- `Buffer.prototype.readInt32BE(offset)`

  Lisez `Int32` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.

- `Buffer.prototype.readIntLE(offset, byteLength)`

  Lisez `Int` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.readInt16LE(offset)`

  Lisez `Int16` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readInt32LE(offset)`

  Lisez `Int32` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUInt8(offset)`

  Lisez `UInt8` à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUIntBE(offset, byteLength)`

  Lisez `UInt` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.readUInt16BE(offset)`

  Lisez `UInt16` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

- • `offset` : entrez un entier.
- `Buffer.prototype.readUInt32BE(offset)`

  Lisez `UInt32` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUIntLE(offset, byteLength)`

  Lisez `UInt` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.readUInt16LE(offset)`

  Lisez `UInt16` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUInt32LE(offset)`

  Lisez `UInt32` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readDoubleBE([offset])`

  Lisez une valeur double 64 bits dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : facultatif. Entrez un entier.
- `Buffer.prototype.readDoubleLE([offset])`

  Lisez une valeur double 64 bits dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : facultatif. Entrez un entier.
- `Buffer.prototype.readFloatBE([offset])`

  Lisez une valeur float 32 bits dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : facultatif. Entrez un entier.
- `Buffer.prototype.readFloatLE([offset])`

  Lisez une valeur float 32 bits dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : facultatif. Entrez un entier.
- `Buffer.prototype.subarray([start[, end]])`

  Renvoie une copie de l'élément `Buffer` décalée et recadrée avec de nouveaux éléments `start` et `end`.

  - `start` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `end` : facultatif. Entrez un entier. La valeur par défaut est la longueur du tampon.
- `Buffer.prototype.swap16()`

  Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 16 bits. La longueur de `Buffer` doit être divisible par 2, sans quoi vous recevrez une erreur.
- `Buffer.prototype.swap32()`

Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 32 bits. La longueur de `Buffer` doit être divisible par 4, sans quoi vous recevrez une erreur.

- `Buffer.prototype.swap64()`

  Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 64 bits. La longueur de `Buffer` doit être divisible par 8, sans quoi vous recevrez une erreur.

- `Buffer.prototype.toJSON()`

  Renvoie l'élément `Buffer` au format JSON.

- `Buffer.prototype.toString([encoding[, start[, end]]])`

  Convertissez l'élément `Buffer`, de `start` à `end`, en chaîne encodée.

  - `encoding` : Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64` ou `base64url`. La valeur par défaut est `utf8`.
  - `start` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `end` : facultatif. Entrez un entier. La valeur par défaut est la longueur du tampon.

- `Buffer.prototype.write(string[, offset[, length]][, encoding])`

  Écrivez l'élément `string` encodé dans `Buffer` s'il y a de l'espace, ou un élément `string` tronqué s'il n'y a pas assez d'espace.

  - `string` : entrez une chaîne.
  - `offset` : facultatif. Entrez un entier. La valeur par défaut est 0.
  - `length` : facultatif. Entrez un entier. La valeur par défaut est la longueur de la chaîne.
  - `encoding` : facultatif. Entrez éventuellement l'un des éléments suivants : `utf8`, `hex`, `base64` ou `base64url`. La valeur par défaut est `utf8`.

- `Buffer.prototype.writeInt8(value, offset, byteLength)`

  Écrivez l'élément `value` `Int8` de `byteLength` à la position `offset` dans l'élément `Buffer`.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeIntBE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt16BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.
  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt32BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.
  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeIntLE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt16LE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt32LE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt8(value, offset, byteLength)`

  Écrivez l'élément `value` `UInt8` de `byteLength` à la position `offset` dans `Buffer`.
  - `value` : entrez un entier.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUIntBE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt16BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt32BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUIntLE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt16LE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeUInt32LE(value, offset, byteLength)`

Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

- `value` : entrez un entier.
- `offset` : entrez un entier.
- `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeDoubleBE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeDoubleLE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeFloatBE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeFloatLE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : facultatif. Entrez un entier. La valeur par défaut est 0.

Les méthodes d'instance suivantes sont prises en charge :

- `buffer[index]`

  Obtenez et définissez l'octet (byte) à la position `index` dans l'élément `Buffer`.

  - Obtenez un nombre entre `0` et `255`. Ou définissez un nombre entre `0` et `255`.

Les propriétés d'instance suivantes sont prises en charge :

- `buffer`

  Obtenez l'objet `ArrayBuffer` pour le tampon.

- `byteOffset`

  Obtenez l'élément `byteOffset` de l'objet `Arraybuffer` du tampon.

- `length`

  Obtenez le nombre d'octets du tampon.

> **Note**
>
> Toutes les méthodes du module Buffer sont nouvelles dans JavaScript Runtime 2.0.

Chaîne de requête

> **Note**
>
> L'objet d'événement CloudFront Functions analyse automatiquement les chaînes de requête d'URL pour vous. Cela signifie que, dans la plupart des cas, vous n'avez pas besoin d'utiliser ce module.

Le module de chaînes de requêtes (`querystring`) fournit des méthodes d'analyse et de formatage des chaînes de requêtes URL. Vous pouvez charger le module en utilisant `require('querystring')`. Le module fournit les méthodes suivantes :

`querystring.escape(`*`string`*`)`

Encode par URL la `string` donnée, en renvoyant une chaîne de requêtes échappée. La méthode est utilisée par `querystring.stringify()` et ne doit pas être utilisée directement.

`querystring.parse(`*`string`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Analyse une chaîne de requêtes (`string`) et renvoie un objet.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`decodeURIComponent` *`function`*

Fonction pour décoder les caractères encodés en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.unescape()`.

`maxKeys` *`number`*

Nombre maximal de clés à analyser. Par défaut, il s'agit de `1000`. Utilisez une valeur de `0` pour supprimer les limitations pour le comptage des clés.

Par défaut, les caractères encodés en pourcentage dans la chaîne de requêtes sont supposés utiliser l'encodage UTF-8. Les séquences UTF-8 non valides sont remplacées par le caractère de remplacement `U+FFFD`.

Par exemple, pour la chaîne de requêtes suivante :

```
'name=value&abc=xyz&abc=123'
```

La valeur renvoyée de `querystring.parse()` est :

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` est un alias pour `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Sérialise un `object` et renvoie une chaîne de requêtes.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`encodeURIComponent` *function*

Fonction à utiliser pour convertir des caractères non sûrs pour une URL en encodage en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.escape()`.

Par défaut, les caractères qui nécessitent un encodage en pourcentage dans la chaîne de requêtes sont encodés en UTF-8. Pour utiliser un encodage différent, spécifiez l'option `encodeURIComponent`.

Par exemple, pour le code suivant :

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

La valeur renvoyée est :

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` est un alias pour `querystring.stringify()`.

`querystring.unescape(`*string*`)`

Décode les caractères encodés en pourcentage URL dans la `string` donnée, en renvoyant une chaîne de requêtes non échappée. Cette méthode est utilisée par `querystring.parse()` et ne doit pas être utilisée directement.

Cryptographie

Le module cryptographique (`crypto`) fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`.

Méthodes de hachage

`crypto.createHash(`*algorithm*`)`

Crée et renvoie un objet de hachage que vous pouvez utiliser pour générer des résumés de hachage à l'aide de l'algorithme donné : `md5`, `sha1` ou `sha256`.

`hash.update(`*data*`)`

Met à jour le contenu de hachage avec les `data` données

`hash.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hash.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Méthodes HMAC

`crypto.createHmac(algorithm, secret key)`

Crée et renvoie un objet HMAC qui utilise le `algorithm` et la `secret key` donnés. L'algorithme peut être `md5`, `sha1` ou `sha256`.

`hmac.update(data)`

Met à jour le contenu HMAC avec les `data` données.

`hmac.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hmac.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Fonctions limitées

Les fonctionnalités JavaScript linguistiques suivantes ne sont pas prises en charge ou sont restreintes pour des raisons de sécurité.

Évaluation dynamique du code

L'évaluation dynamique du code n'est pas prise en charge. Les deux constructeurs `eval()` et `Function` renvoient une erreur en cas de tentative. Par exemple, `const sum = new Function('a', 'b', 'return a + b')` renvoie une erreur.

Temporisateurs

Les fonctions `setTimeout()`, `setImmediate()` et `clearTimeout()` ne sont pas prises en charge. Il n'y a aucune disposition relative au report ou au produit dans une exécution de fonction. Votre fonction doit s'exécuter de manière synchrone jusqu'à la fin.

Horodatages

Pour des raisons de sécurité, il n'y a pas d'accès aux temporisateurs haute résolution. Toutes les méthodes `Date` pour interroger l'heure actuelle retournent toujours la même valeur pendant la

durée de vie d'une même exécution de la fonction. L'horodatage renvoyé est l'heure à laquelle la fonction a commencé à s'exécuter. Par conséquent, vous ne pouvez pas mesurer le temps écoulé dans votre fonction.

Accès au système de fichiers

Il n'y a pas d'accès au système de fichiers.

Accès réseau

Les appels réseau ne sont pas pris en charge. Par exemple, XHR, HTTP(S) et socket ne sont pas pris en charge.

Méthodes d'aide pour les magasins de clés-valeurs

Cette section s'applique si vous utilisez le CloudFront Key Value Store pour inclure des valeurs clés dans la fonction que vous créez. CloudFront Functions possède un module qui fournit trois méthodes d'assistance pour lire les valeurs du magasin de valeurs clés.

Pour utiliser ce module dans le code de fonction, assurez-vous d'avoir associé un magasin de valeurs clés à la fonction.

Ajoutez ensuite les instructions suivantes dans les premières lignes du code de fonction :

```
import cf from 'cloudfront';
const kvsId = "key value store ID";
const kvsHandle = cf.kvs(kvsId);
```

L'*identifiant de votre boutique de valeurs clés* peut ressembler à ce qui suit : `a1b2c3d4-5678-90ab-cdef-EXAMPLE1`

Méthode **`get()`**

Utilisez cette méthode pour renvoyer la valeur de clé pour le nom de clé que vous spécifiez.

Demande

```
get("key", options);
```

- `key` : nom de la clé dont la valeur doit être extraite

- `options`: Il y a une option,`format`. Elle garantit que la fonction analyse correctement les données. Valeurs possibles :
  - `string` : (par défaut) encodé en UTF8
  - `json`
  - `bytes` : tampon de données binaires brutes

Exemple de demande

```
const value = await kvsHandle.get("myFunctionKey", { format: "string"});
```

Réponse

La réponse est une `promise` qui aboutit à une valeur au format demandé en utilisant`options`. Par défaut, la valeur est renvoyée sous forme de chaîne.

Méthode **`exists()`**

Utilisez cette méthode pour déterminer si la clé existe ou non dans le magasin de valeurs clés.

Demande

```
exists("key");
```

Exemple de demande

```
const exist = await kvsHandle.exists("myFunctionkey");
```

Réponse

La réponse est un `promise` qui renvoie une valeur booléenne (`trueoufalse`). Cette valeur indique si la clé existe ou non dans le magasin de valeurs clés.

Gestion des erreurs

La `get()` méthode renvoie une erreur lorsque la clé que vous avez demandée n'existe pas dans le magasin de valeurs clé associé. Pour gérer ce cas d'utilisation, vous pouvez ajouter un `catch` bloc `try` et à votre code.

Méthode **`meta()`**

Utilisez cette méthode pour renvoyer des métadonnées relatives au magasin de valeurs clés.

Demande

```
meta();
```

Exemple de demande

```
const meta = await kvsHandle.meta();
```

Réponse

La réponse est un élément `promise` qui se résout à un objet doté des propriétés suivantes :

- `creationDateTime` : date et heure de création du magasin de clés-valeurs, au format ISO 8601.
- `lastUpdatedDateTime` : date et heure de la dernière synchronisation du magasin de clés-valeurs depuis la source, au format ISO 8601. La valeur n'inclut pas la durée de propagation jusqu'à la périphérie.
- `keyCount` : nombre total de clés dans le magasin de clés-valeurs après la dernière synchronisation depuis la source.

Exemple de réponse

```
{keyCount:3,creationDateTime:2023-11-30T23:07:55.765Z,lastUpdatedDateTime:2023-12-15T03:57:52.4
```

Exemple de code pour CloudFront Functions

Pour vous aider à commencer à écrire du code de fonction pour CloudFront Functions, consultez les exemples suivants. Vous pouvez également trouver ces exemples dans le amazon-cloudfront-functions référentiel sur GitHub.

Rubriques

- Ajouter un en-tête Cache-Control à la réponse
- Ajouter un en-tête CORS (Cross-Origin Resource Sharing) à la réponse
- Ajouter un en-tête CORS (Cross-Origin Resource Sharing) à la requête

- Ajouter des en-têtes de sécurité à la réponse
- Ajouter un en-tête True-Client-IP à la requête
- Rediriger l'utilisateur vers une nouvelle URL
- Ajouter index.html aux URL de requêtes qui n'incluent pas de nom de fichier
- Valider un jeton simple dans la requête
- Utilisation de async et await
- Normalisation des paramètres de chaîne de requête
- Utiliser des paires clé-valeur dans une fonction

Ajouter un en-tête Cache-Control à la réponse

La fonction de réponse du spectateur suivante ajoute un en-tête `Cache-Control` HTTP à la réponse. L'en-tête utilise la directive `max-age` pour indiquer aux navigateurs Web de mettre en cache la réponse pendant un maximum de deux ans (63 072 000 secondes). Pour plus d'informations, consultez Cache-Control sur le site Web MDN Web Docs.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    const response = event.response;
    const headers = response.headers;

    // Set the cache-control header
     headers['cache-control'] = {value: 'public, max-age=63072000'};

    // Return response to viewers
    return response;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set the cache-control header
```

```
    headers['cache-control'] = {value: 'public, max-age=63072000'};

    // Return response to viewers
    return response;
}
```

Ajouter un en-tête CORS (Cross-Origin Resource Sharing) à la réponse

La fonction de réponse du spectateur suivante ajoute un en-tête `Access-Control-Allow-Origin` HTTP à la réponse si celle-ci ne contient pas déjà cet en-tête. Cet en-tête fait partie du mécanisme CORS (Cross-Origin Resource Sharing). La valeur de l'en-tête (*) indique aux navigateurs Web d'autoriser le code de n'importe quelle origine à accéder à cette ressource. Pour plus d'informations, consultez Access-Control-Allow-Origin sur le site Web MDN Web Docs.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event)  {
    const request = event.request;
    const response  = event.response;

    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!response.headers['access-control-allow-origin'] &&
 request.headers['origin']) {
        response.headers['access-control-allow-origin'] = {value:
 request.headers['origin'].value};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

JavaScript runtime 1.0

```
function handler(event)  {
    var response  = event.response;
    var headers  = response.headers;
```

```
    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!headers['access-control-allow-origin']) {
        headers['access-control-allow-origin'] = {value: "*"};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

Ajouter un en-tête CORS (Cross-Origin Resource Sharing) à la requête

La fonction de demande d'affichage suivante ajoute un en-tête `Origin` HTTP à la demande si celle-ci ne contient pas déjà cet en-tête. Cet en-tête fait partie du mécanisme CORS (Cross-Origin Resource Sharing). Cet exemple montre comment définir la valeur de l'en-tête sur la valeur de l'en-tête `Host` de la requête. Pour plus d'informations, consultez Origin sur le site Web MDN Web Docs.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const host = request.headers.host.value;

   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;
```

```
   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

Ajouter des en-têtes de sécurité à la réponse

La fonction de réponse du lecteur suivante ajoute à la réponse plusieurs en-têtes HTTP courants liés à la sécurité. Pour plus d'informations, consultez les pages suivantes du site Web MDN Web Docs :

- Strict-Transport-Security
- Content-Security-Policy
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    const response = event.response;
    const headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'; frame-ancestors
 'none'"};
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};
    headers['referrer-policy'] = {value: 'same-origin'};

    // Return the response to viewers
```

```
    return response;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'"};
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};

    // Return the response to viewers
    return response;
}
```

Ajouter un en-tête True-Client-IP à la requête

La fonction de demande de visionneuse suivante ajoute un en-tête `True-Client-IP` HTTP à la demande, avec l'adresse IP de l'afficheur comme valeur d'en-tête. Lors de l' CloudFront envoi d'une demande à une origine, celle-ci peut déterminer l'adresse IP de l' CloudFront hôte qui a envoyé la demande, mais pas l'adresse IP du spectateur (client) à qui la demande d'origine a été envoyée CloudFront. Cette fonction ajoute l'en-tête `True-Client-IP` afin que l'origine puisse voir l'adresse IP de l'utilisateur.

> **Important**
>
> Pour vous assurer que cet en-tête est CloudFront inclus dans les demandes d'origine, vous devez l'ajouter à la liste des en-têtes autorisés dans une politique de demande d'origine.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

Rediriger l'utilisateur vers une nouvelle URL

La fonction de demande du spectateur suivante génère une réponse pour rediriger le visiteur vers une URL spécifique au pays lorsque la demande provient d'un pays en particulier. Cette fonction repose sur la valeur de l'en-tête `CloudFront-Viewer-Country` pour déterminer le pays de l'utilisateur.

> **Important**
>
> Pour que cette fonction fonctionne, vous devez configurer CloudFront pour ajouter l'`CloudFront-Viewer-Country`en-tête aux demandes entrantes en l'ajoutant aux en-têtes autorisés dans une politique de cache ou une politique de demande d'origine.

Cet exemple redirige l'utilisateur vers une URL spécifique à l'Allemagne lorsque la requête de ce dernier provient d'Allemagne. Si la requête utilisateur ne provient pas d'Allemagne, la fonction renvoie la requête d'origine non modifiée.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const host = request.headers.host.value;
    const country = Symbol.for('DE'); // Choose a country code
    const newurl = `https://${host}/de/index.html`; // Change the redirect URL to
 your choice

    if (headers['cloudfront-viewer-country']) {
        const countryCode = Symbol.for(headers['cloudfront-viewer-country'].value);
        if (countryCode === country) {
            const response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;
    var country = 'DE' // Choose a country code
    var newurl = `https://${host}/de/index.html` // Change the redirect URL to your
 choice

    if (headers['cloudfront-viewer-country']) {
```

```
        var countryCode = headers['cloudfront-viewer-country'].value;
        if (countryCode === country) {
            var response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

Pour plus d'informations sur les réécritures et les redirections, voir Gestion des réécritures et des redirections à l'aide des fonctions Edge dans le studio Workshop. AWS

Ajouter index.html aux URL de requêtes qui n'incluent pas de nom de fichier

La fonction de demande d'affichage suivante s'ajoute `index.html` aux demandes qui n'incluent pas de nom de fichier ou d'extension dans l'URL. Cette fonction peut être utile pour les applications d'une seule page ou les sites Web générés statiquement qui sont hébergés dans un compartiment Amazon S3.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }
```

```
    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }

    return request;
}
```

Valider un jeton simple dans la requête

La fonction de demande d'affichage suivante valide un jeton Web JSON (JWT) dans la chaîne de requête d'une demande. Si le jeton est valide, la fonction renvoie la demande originale non modifiée à CloudFront. Si le jeton n'est pas valide, la fonction génère une réponse d'erreur. Cette fonction utilise le module `crypto`. Pour plus d'informations, consultez Modules intégrés.

Cette fonction suppose que les requêtes contiennent une valeur JWT dans un paramètre de chaîne de requêtes nommé `jwt`.

> **Warning**
>
> Pour utiliser cette fonction, vous devez mettre votre clé secrète dans le code de la fonction.

Consultez cet exemple sur GitHub.

JavaScript runtime 2.0

```
const crypto = require('crypto');
```

```
//Response when JWT is not valid.
const response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    const segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
    }

    // All segment should be base64
    const headerSeg = segments[0];
    const payloadSeg = segments[1];
    const signatureSeg = segments[2];

    // base64 decode and parse JSON
    const header = JSON.parse(_base64urlDecode(headerSeg));
    const payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        const signingMethod = 'sha256';
        const signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        const signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType, signatureSeg)) {
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }
```

```
        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }

    return payload;
}

//Function to ensure a constant time comparison to prevent
//timing side channels.
function _constantTimeEquals(a, b) {
    if (a.length != b.length) {
        return false;
    }

    var xor = 0;
    for (var i = 0; i < a.length; i++) {
    xor |= (a.charCodeAt(i) ^ b.charCodeAt(i));
    }

    return 0 === xor;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return _constantTimeEquals(signature, _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}

function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return Buffer.from(str, 'base64url')
}

function handler(event) {
    const request = event.request;
    //Secret key used to verify JWT token.
    //Update with your own key.
```

```
    var key = "LzdWGpAToQ1DqYuzHxE6YOqi7G3X2yvNBot9mCXfx5k";

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        console.log("Error: No JWT in the querystring");
        return response401;
    }

    const jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, key);
    }
    catch(e) {
        console.log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    console.log("Valid JWT token");
    return request;
}
```

JavaScript runtime 1.0

```
var crypto = require('crypto');

//Response when JWT is not valid.
var response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    var segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
```

```
    }

    // All segment should be base64
    var headerSeg = segments[0];
    var payloadSeg = segments[1];
    var signatureSeg = segments[2];

    // base64 decode and parse JSON
    var header = JSON.parse(_base64urlDecode(headerSeg));
    var payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        var signingMethod = 'sha256';
        var signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        var signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType, signatureSeg)) {
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }

        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }

    return payload;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return (signature === _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}
```

```
function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return String.bytesFrom(str, 'base64url')
}

function handler(event) {
    var request = event.request;

    //Secret key used to verify JWT token.
    //Update with your own key.
    var key = "LzdWGpAToQ1DqYuzHxE6YOqi7G3X2yvNBot9mCXfx5k";

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        console.log("Error: No JWT in the querystring");
        return response401;
    }

    var jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, key);
    }
    catch(e) {
        console.log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    console.log("Valid JWT token");
    return request;
}
```

Utilisation de async et await

CloudFront Fonctions fournies par JavaScript Runtime Functions 2.0 `async` et `await` syntaxe permettant de gérer `Promise` les objets. Les promesses représentent des résultats différés

accessibles via le mot clé `await` dans les fonctions marquées comme `async`. Diverses nouvelles WebCrypto fonctions utilisent Promises.

Pour plus d'informations sur les objets `Promise`, consultez Promise.

> **Note**
>
> Vous devez utiliser JavaScript Runtime 2.0 pour les exemples de code suivants.

```
async function answer() {
    return 42;
}

// Note: async, await can be used only inside an async function.

async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

L'exemple de JavaScript code suivant montre comment afficher les promesses avec la méthode de la `then` chaîne. Vous pouvez utiliser `catch` pour visualiser les erreurs.

```
async function answer() {
    return 42;
}

async function squared_answer() {
   return answer().then(value => value * value)
}
// note async, await can be used only inside async function
async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await squared_answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
```

```
}
```

Normalisation des paramètres de chaîne de requête

Vous pouvez normaliser les paramètres de chaîne de requête pour améliorer le taux d'accès au cache.

L'exemple suivant fonctionne avec les environnements JavaScript d'exécution 1.0 et 2.0. L'exemple montre comment améliorer le taux de réussite de votre cache en classant les chaînes de requête par ordre alphabétique avant de CloudFront transmettre les demandes à votre origine.

```
function handler(event) {
     var qs=[];
     for (var key in event.request.querystring) {
         if (event.request.querystring[key].multiValue) {
             event.request.querystring[key].multiValue.forEach((mv) => {qs.push(key +
 "=" + mv.value)});
         } else {
             qs.push(key + "=" + event.request.querystring[key].value);
         }
     };

     event.request.querystring = qs.sort().join('&');


     return event.request;
}
```

Utiliser des paires clé-valeur dans une fonction

Vous pouvez utiliser des paires clé-valeur provenant d'un magasin de valeurs clés dans une fonction.

> **Note**
>
> Vous devez utiliser JavaScript Runtime 2.0 pour l'exemple de code suivant.

L'exemple montre une fonction qui utilise le contenu de l'URL dans la requête HTTP pour rechercher un chemin personnalisé dans le magasin de valeurs clés. CloudFront utilise ensuite ce chemin personnalisé pour effectuer la demande. Cette fonction permet de gérer les multiples chemins qui font partie d'un site Web.

```
import cf from 'cloudfront';

// Declare the ID of the key value store that you have associated with this function
// The import fails at runtime if the specified key value store is not associated with
 the function

const kvsId = "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111";

const kvsHandle = cf.kvs(kvsId);

async function handler(event) {
    const request = event.request;
    // Use the first segment of the pathname as key
    // For example http(s)://domain/<key>/something/else
    const pathSegments = request.uri.split('/')
    const key = pathSegments[1]
    try {
        // Replace the first path of the pathname with the value of the key
        // For example http(s)://domain/<value>/something/else
        pathSegments[1] = await kvsHandle.get(key);
        const newUri = pathSegments.join('/');
        console.log(`${request.uri} -> ${newUri}`)
        request.uri = newUri;
    } catch (err) {
        // No change to the pathname if the key is not found
        console.log(`${request.uri} | ${err}`);
    }
    return request;
}
```

Création de fonctions

Vous créez une fonction en deux étapes :

1. Créez le code de fonction sous la forme JavaScript. Vous pouvez utiliser l'exemple par défaut de la CloudFront console ou écrire le vôtre. Pour plus d’informations, consultez les rubriques suivantes :
   - Écrire le code de la fonction
   - the section called “Structure d'évènements”
   - Exemple de code pour CloudFront Functions
2. CloudFront À utiliser pour créer la fonction et inclure votre code. Le code existe à l’intérieur de la fonction (et non en tant que référence).

Console

Pour créer une fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez Créer une fonction.
3. Entrez un nom de fonction unique dans le Compte AWS, choisissez la JavaScript version, puis choisissez Continuer. La page de détails s'affiche pour la nouvelle fonction.

   > **Note**
   >
   > Pour utiliser des paires clé-valeur dans la fonction, vous devez choisir JavaScript runtime 2.0.

4. Dans la section Code de fonction, choisissez l'onglet Créer et entrez votre code de fonction. L'exemple de code inclus dans l'onglet Création illustre la syntaxe de base du code de fonction.
5. Sélectionnez Enregistrer les modifications.
6. Si le code de fonction utilise des paires clé-valeur, vous devez associer un magasin clé-valeur.

   Vous pouvez associer le magasin de valeurs clés lorsque vous créez la fonction pour la première fois. Vous pouvez également l'associer ultérieurement, en mettant à jour la fonction.

   Pour associer un magasin de clés-valeurs dès maintenant, procédez comme suit :

   - Accédez à la KeyValueStore section Associer et choisissez Associer existant KeyValueStore.
   - Sélectionnez le magasin clé-valeur qui contient les paires clé-valeur de la fonction, puis choisissez Associer. KeyValueStore

   CloudFront associe immédiatement le magasin à la fonction. Vous n'avez pas besoin d'enregistrer la fonction.

CLI

Si vous utilisez la CLI, vous commencez généralement par créer le code de fonction dans un fichier, puis vous créez la fonction avec AWS CLI.

Pour créer une fonction

1. Créez le code de fonction dans un fichier et stockez-le dans un répertoire auquel votre ordinateur peut se connecter.
2. Exécutez la commande, comme illustré dans l'exemple. Cet exemple utilise la `fileb://` notation pour transmettre le fichier. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront create-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
[{"KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"}]}}' \
    --function-code fileb://function-max-age-v1.js
```

> **Remarques**
>
> - `Runtime`— La version de JavaScript. Pour utiliser des paires clé-valeur dans la fonction, vous devez spécifier la version 2.0.
> - `KeyValueStoreAssociations`— Si votre fonction utilise des paires clé-valeur, vous pouvez associer le magasin de valeurs clé lorsque vous créez la fonction pour la première fois. Vous pouvez également l'associer ultérieurement, en utilisantupdate-function. `Quantity` a toujours pour valeur 1, car chaque fonction peut être associée uniquement à un seul magasin de clés-valeurs.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
ETag: ETVABCEXAMPLE
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years
    Runtime: cloudfront-js-2.0
    KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
  FunctionMetadata:
```

```
    CreatedTime: '2021-04-18T20:38:56.915000+00:00'
    FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge
    LastModifiedTime: '2023-11-19T20:38:56.915000+00:00'
    Stage: DEVELOPMENT
  Name: MaxAge
  Status: UNPUBLISHED
Location: https://cloudfront.amazonaws.com/2020-05-31/function/
arn:aws:cloudfront:::function/MaxAge
```

La plupart des informations proviennent de la demande. D'autres informations sont ajoutées par CloudFront.

> **Remarques**
>
> - `ETag`— Cette valeur change chaque fois que vous modifiez le magasin de valeurs clés. Vous utilisez cette valeur et le nom de la fonction pour référencer la fonction à l'avenir. Assurez-vous de toujours utiliser le courant`ETag`.
> - `FunctionARN`— L'ARN de votre CloudFront fonction.
> - 111122223333 — Le. Compte AWS
> - `Stage`— Le stade de la fonction (`LIVE`ou`DEVELOPMENT`).
> - `Status`— Le statut de la fonction (`PUBLISHED`ou`UNPUBLISHED`).

Une fois que vous avez créé la fonction, elle est ajoutée à la `DEVELOPMENT` scène. Nous vous recommandons de tester votre fonction avant de la publier. Une fois que vous avez publié votre fonction, celle-ci passe à l'`LIVE`étape.

Fonctions de test

Avant de déployer la fonction sur la scène en direct (production), vous pouvez tester votre fonction pour vérifier qu'elle fonctionne comme prévu. Pour tester une fonction, vous devez spécifier un objet d'événement qui représente une requête ou une réponse HTTP que votre CloudFront distribution pourrait recevoir en production.

CloudFront Functions effectue les opérations suivantes :

1. Exécute la fonction, en utilisant l'objet d'événement fourni comme entrée.

2. Renvoie le résultat de la fonction (l'objet d'évènement modifié) ainsi que les journaux de fonction ou les messages d'erreurs et l'utilisation du calcul de la fonction. Pour plus d'informations sur l'utilisation du calcul, consultez the section called “Comprendre l'utilisation du calcul”.

Table des matières

Configuration de l’objet d’événement

Avant de tester une fonction, vous devez configurer l’objet d’événement avec lequel la tester. Il existe plusieurs options.

Option 1 : configurer un objet d’événement sans l’enregistrer

Vous pouvez configurer un objet d'événement dans l'éditeur visuel de la CloudFront console sans l'enregistrer.

Vous pouvez utiliser cet objet d'événement pour tester la fonction depuis la CloudFront console, même si elle n'est pas enregistrée.

Option 2 : créer un objet d’événement dans l’éditeur visuel

Vous pouvez configurer un objet d'événement dans l'éditeur visuel de la CloudFront console sans l'enregistrer. Vous pouvez créer 10 objets d’événement pour chaque fonction afin de pouvoir, par exemple, tester différentes entrées possibles.

Lorsque vous créez l'objet d'événement de cette manière, vous pouvez l'utiliser pour tester la fonction dans la CloudFront console. Vous ne pouvez pas l'utiliser pour tester la fonction à l'aide d'une AWS API ou d'un SDK.

Option 3 : créer un objet d’événement à l’aide d’un éditeur de texte

Vous pouvez utiliser un éditeur de texte pour créer un objet d’événement au format JSON. Pour en savoir plus sur la structure d’un objet d’événement, consultez Structure d'évènements.

Vous pouvez utiliser cet objet d’événement pour tester la fonction à l’aide de la CLI. Mais vous ne pouvez pas l'utiliser pour tester la fonction dans la CloudFront console.

Pour créer un objet d'événement (option 1 ou 2)

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.

   Choisissez la fonction que vous souhaitez tester.
2. Sur la page de détails de la fonction, choisissez l'onglet Test.
3. Pour Type d'événement, choisissez l'une des options suivantes :

   - Choisissez Demande de l'utilisateur si la fonction modifie une requête HTTP ou génère une réponse basée sur la demande. La section Demande apparaît.
   - Choisissez Viewer response. Les sections Demande et Réponse apparaissent.
4. Complétez les champs à inclure dans l'événement. Vous pouvez choisir Modifier le JSON pour afficher le JSON brut.
5. (Facultatif) Pour enregistrer l'événement, choisissez Enregistrer et dans le champ Enregistrer l'événement de test, entrez un nom, puis sélectionnez Enregistrer.

   Vous pouvez également choisir Modifier le JSON, copier le JSON brut et l'enregistrer dans votre propre fichier, en dehors de CloudFront.

Pour créer un objet d'événement (option 3)

Créez l'objet d'événement à l'aide d'un éditeur de texte. Stockez le fichier dans un répertoire auquel votre ordinateur peut se connecter.

Vérifiez que vous suivez les consignes suivantes :

- Omettez les champs `distributionDomainName`, `distributionId` et `requestId`.
- Les noms des en-têtes, des cookies et des chaînes de requête doivent être en minuscules.

Une option permettant de créer un objet d'événement de cette manière consiste à créer un échantillon à l'aide de l'éditeur visuel. Vous pouvez être sûr que l'échantillon est correctement formaté. Vous pouvez ensuite copier le code JSON brut, le coller dans un éditeur de texte et enregistrer le fichier.

Pour plus d'informations sur la structure d'un événement, consultezStructure d'évènements.

Tester la fonction

Vous pouvez tester une fonction dans la CloudFront console ou avec le AWS Command Line Interface (AWS CLI).

Console

Pour tester la fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez la fonction que vous souhaitez tester.
3. Choisissez l'onglet Test.
4. Assurez-vous que l'événement correct est affiché. Pour passer de l'événement actuellement affiché, choisissez un autre événement dans le champ Sélectionner un événement de test.
5. Choisissez la fonction de test. La console affiche le résultat de la fonction, y compris les journaux des fonctions et l'utilisation du calcul.

CLI

Vous pouvez tester une fonction à l'aide de la aws cloudfront test-function commande.

Pour tester la fonction

1. Ouvrez une fenêtre de ligne de commande.
2. Exécutez la commande suivante à partir du même répertoire que celui qui contient le fichier spécifié.

   Cet exemple utilise la `fileb://` notation pour transmettre le fichier objet de l'événement. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront test-function \
    --name MaxAge \
    --if-match ETVABCEXAMPLE \
    --event-object fileb://event-maxage-test01.json \
    --stage DEVELOPMENT
```

Remarques

- Vous référencez la fonction par son nom et son ETag (dans le paramètre `if-match`). Vous référencez l'objet d'événement par son emplacement dans votre système de fichiers.
- Il peut s'agir de la phase `DEVELOPMENT` ou `LIVE`.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
TestResult:
  ComputeUtilization: '21'
  FunctionErrorMessage: ''
  FunctionExecutionLogs: []
  FunctionOutput: '{"response":{"headers":{"cloudfront-functions":
{"value":"generated-by-CloudFront-Functions"},"location":{"value":"https://
aws.amazon.com/cloudfront/"}},"statusDescription":"Found","cookies":
{},"statusCode":302}}'
  FunctionSummary:
    FunctionConfig:
      Comment: MaxAge function
      Runtime: cloudfront-js-2.0
      KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
    FunctionMetadata:
      CreatedTime: '2021-04-18T20:38:56.915000+00:00'
      FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge
      LastModifiedTime: '2023-17-20T10:38:57.057000+00:00'
      Stage: DEVELOPMENT
    Name: MaxAge
    Status: UNPUBLISHED
```

Remarques

- `FunctionExecutionLogs` contient une liste de lignes de journaux que la fonction a écrites dans les instructions `console.log()` (le cas échéant).

- `ComputeUtilization`contient des informations sur l'exécution de votre fonction. veuillez consulter the section called “Comprendre l'utilisation du calcul”.
- `FunctionOutput` contient l'objet d'évènement renvoyé par la fonction.

Comprendre l'utilisation du calcul

L'utilisation du calcul est la durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé.

Si une fonction dépasse continuellement la durée maximale autorisée CloudFront , elle ralentit. La liste suivante explique la probabilité qu'une fonction soit limitée en fonction de la valeur d'utilisation du calcul.

Valeur d'utilisation du calcul :

- 1 – 50 : la fonction est largement inférieure à la durée maximale autorisée et devrait s'exécuter sans aucune limitation.
- 51 – 70 : la fonction approche de la durée maximale autorisée. Envisagez d'optimiser le code de fonction.
- 71 — 100 — La fonction est très proche de la durée maximale autorisée ou la dépasse. CloudFront est susceptible de limiter cette fonction si vous l'associez à une distribution.

Fonctions de mise à jour

Vous pouvez mettre à jour une fonction à tout moment. Les modifications sont apportées uniquement à la version de la fonction qui figure dans la phase `DEVELOPMENT`. Pour copier les mises à jour de la `DEVELOPMENT` scène vers`LIVE`, vous devez publier la fonction.

Vous pouvez mettre à jour le code d'une fonction dans la CloudFront console ou avec le AWS Command Line Interface (AWS CLI).

Console

Pour mettre à jour le code de fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.

Sélectionnez la fonction à mettre à jour.

2. Choisissez Modifier et apportez les modifications suivantes :

   - Mettez à jour tous les champs de la section Détails.

   - Modifiez ou supprimez le magasin de valeurs-clés associé. Pour plus d'informations sur les magasins de clés-valeurs, consultez the section called "En utilisant CloudFront KeyValueStore".

   - Modifiez le code de fonction. Cliquez sur l'onglet Créer, apportez des modifications, puis sélectionnez Enregistrer les modifications pour enregistrer les modifications apportées au code.

CLI

Mettre à jour le code de la fonction.

1. Ouvrez une fenêtre de ligne de commande.
2. Exécutez la commande suivante.

   Cet exemple utilise la `fileb://` notation pour transmettre le fichier. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront update-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
[{"KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"}]}}' \
    --function-code fileb://function-max-age-v1.js \
    --if-match ETVABCEXAMPLE
```

> **Remarques**
>
> - Vous identifiez la fonction à la fois par son nom et par son ETag (dans le paramètre `if-match`). Assurez-vous d'utiliser l'ETag actuel. Vous pouvez l'obtenir à l'aide d'une opération de description.

- Vous devez inclure l'élément `function-code`, même si vous ne voulez pas le modifier.
- Soyez prudent avec l'élément `function-config`. Vous devez transmettre tout ce que vous voulez conserver dans la configuration. En particulier, gérez le magasin de clés-valeurs comme suit :
  - Pour conserver l'association de magasins clé-valeur existante (le cas échéant), spécifiez le nom du magasin existant.
  - Pour modifier l'association, spécifiez le nom du nouveau magasin de valeurs clés.
  - Pour supprimer l'association, omettez le `KeyValueStoreAssociations` paramètre.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
ETag: ETVXYZEXAMPLE
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years \
    Runtime: cloudfront-js-2.0 \
    KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
  FunctionMetadata: \
    CreatedTime: '2021-04-18T20:38:56.915000+00:00' \
    FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge \
    LastModifiedTime: '2023-12-19T23:41:15.389000+00:00' \
    Stage: DEVELOPMENT \
  Name: MaxAge \
  Status: UNPUBLISHED
```

La plupart des informations proviennent de la demande. D'autres informations sont ajoutées par CloudFront.

Remarques

- `ETag`— Cette valeur change chaque fois que vous modifiez le magasin de valeurs clés.
- `FunctionARN`— L'ARN de votre CloudFront fonction.
- `Stage`— L'étape de la fonction (`LIVE`ou`DEVELOPMENT`).
- `Status`— Le statut de la fonction (`PUBLISHED`ou`UNPUBLISHED`).

Fonctions de publication

Lorsque vous publiez votre fonction, celle-ci est copiée d'une `DEVELOPMENT` scène à l'`LIVE`autre.

Si aucun comportement de cache n'est associé à la fonction, sa publication vous permet de l'associer à un comportement de cache. Vous pouvez uniquement associer des comportements de cache à des fonctions qui sont à l'étape `LIVE`.

Important

- Avant de publier, nous vous recommandons de tester la fonction.
- Une fois que vous avez publié la fonction, tous les comportements de cache associés à cette fonction commencent automatiquement à utiliser la copie récemment publiée, dès que le déploiement des distributions est terminé.

Vous pouvez publier une fonction dans la CloudFront console ou à l'aide du AWS CLI.

Console

Pour publier une fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Sélectionnez la fonction à mettre à jour.
3. Cliquez sur l'onglet Publier, puis sur Publier. Si votre fonction est déjà associée à un ou plusieurs comportements de cache, choisissez Publier et mettre à jour.

4. (Facultatif) Pour voir les distributions associées à la fonction, choisissez CloudFront Distributions associées pour développer cette section.

En cas de succès, une bannière apparaît en haut de la page indiquant que le ***nom de la fonction*** a été publié avec succès. Vous pouvez également choisir l'onglet Générer, puis Live pour afficher la version live du code de fonction.

CLI

Pour publier une fonction

1. Ouvrez une fenêtre de ligne de commande.
2. Exécutez la commande suivante aws cloudfront publish-function. Dans l'exemple, des sauts de ligne sont fournis pour rendre l'exemple plus lisible.

```
aws cloudfront publish-function \
    --name MaxAge \
    --if-match ETVXYZEXAMPLE
```

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years
    Runtime: cloudfront-js-2.0
  FunctionMetadata:
    CreatedTime: '2021-04-18T21:24:21.314000+00:00'
    FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
    LastModifiedTime: '2023-12-19T23:41:15.389000+00:00'
    Stage: LIVE
  Name: MaxAge
  Status: UNASSOCIATED
```

Associer des fonctions à des distributions

Pour utiliser une fonction dans CloudFront Functions avec une distribution, vous devez associer la fonction à un ou plusieurs comportements de cache dans la distribution. Vous pouvez associer une fonction à plusieurs comportements de cache dans plusieurs distributions..

Lorsque vous associez une fonction à un comportement de cache, vous devez choisir un type d'évènement. Le type d'événement détermine le moment où CloudFront Functions exécute la fonction. Vous pouvez choisir les types d'événements suivants :

- Demande du visualiseur — La fonction s'exécute lorsqu'elle CloudFront reçoit une demande d'un visualiseur.
- Réponse du visualiseur — La fonction s'exécute avant de CloudFront renvoyer une réponse au visualiseur.

Vous ne pouvez pas utiliser de types d'événements liés à l'origine (demande d'origine et réponse d'origine) avec CloudFront Functions. Vous pouvez plutôt utiliser Lambda @Edge. Pour plus d'informations, consultez CloudFront événements pouvant déclencher une fonction Lambda @Edge.

> **Note**
>
> Avant d'associer une fonction, vous devez la publier à l'étape `LIVE`.

Vous pouvez associer une fonction à une distribution dans la CloudFront console ou à AWS Command Line Interface (AWS CLI).

Console

Vous pouvez utiliser la CloudFront console pour associer une fonction à un comportement de cache existant dans une CloudFront distribution existante. Pour plus d'informations sur la création d'une distribution, reportez-vous à the section called “Créer une distribution”.

Pour associer une fonction à un comportement de cache existant

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez la fonction que vous souhaitez associer.
3. Sur la page Fonction, choisissez l'onglet Publier.
4. Choisissez la fonction Publier.
5. Choisissez Ajouter une association. Dans la boîte de dialogue qui apparaît, choisissez une distribution, un type d'événement et/ou un comportement de cache.

Pour le type d'événement, choisissez le moment où vous souhaitez que cette fonction s'exécute :

- Requête du visualiseur : exécutez la fonction chaque fois CloudFront que vous recevez une demande.
- Réponse du spectateur : exécutez la fonction chaque fois qu'une réponse est CloudFront renvoyée.

6. Pour enregistrer la configuration, choisissez Ajouter une association.

CloudFront associe la distribution à la fonction. Attendez quelques minutes pour que la distribution associée termine son déploiement. Vous pouvez choisir Afficher la distribution sur la page des détails de la fonction pour vérifier la progression.

CLI

Vous pouvez associer une fonction avec l'un des éléments suivants :

- Un comportement de cache existant
- Nouveau comportement du cache dans une distribution existante
- Nouveau comportement du cache dans une nouvelle distribution

La procédure suivante montre comment associer une fonction à un comportement de cache existant.

Pour associer une fonction à un comportement de cache existant

1. Ouvrez une fenêtre de ligne de commande.
2. Entrez la commande suivante pour enregistrer la configuration de distribution pour la distribution dont vous souhaitez associer le comportement de cache à une fonction. Cette commande enregistre la configuration de distribution dans un fichier nommé `dist-config.yaml`. Pour utiliser cette commande, procédez comme suit :
   - Remplacez *`DistributionID`* par l'ID de la distribution.
   - Exécutez la commande sur une ligne. Dans l'exemple, des sauts de ligne sont fournis pour rendre l'exemple plus lisible.

```
aws cloudfront get-distribution-config \
    --id DistributionID \
    --output yaml > dist-config.yaml
```

Lorsque la commande est réussie, aucune sortie n'est renvoyée. AWS CLI

3. Ouvrez le fichier nommé `dist-config.yaml` que vous avez créé. Apportez les modifications suivantes au fichier.

   a. Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   b. Dans le comportement du cache, recherchez l'objet nommé `FunctionAssociations`. Mettez à jour cet objet pour ajouter une association de fonctions. La syntaxe YAML pour une association de fonctions ressemble à l'exemple ci-dessous.

      - L'exemple suivant montre un objet d'évènement de requête utilisateur (déclenchement). Pour utiliser le type d'évènement Réponse utilisateur, remplacez `viewer-request` par `viewer-response`.
      - Remplacez *arn:aws:cloudfront::111122223333:function/ExampleFunction* par l'Amazon Resource Name (ARN) de la fonction que vous associez à ce comportement de cache. Pour obtenir l'ARN de la fonction, vous pouvez utiliser la commande aws cloudfront list-functions.

```
FunctionAssociations:
  Items:
    - EventType: viewer-request
      FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
  Quantity: 1
```

   c. Après avoir effectué ces modifications, enregistrez le fichier.

4. Utilisez la commande suivante pour mettre à jour la distribution, en ajoutant l'association de fonctions. Pour utiliser cette commande, procédez comme suit :

   - Remplacez *DistributionID* par l'ID de la distribution.
   - Exécutez la commande sur une ligne. Dans l’exemple, des sauts de ligne sont fournis pour rendre l’exemple plus lisible.

```
aws cloudfront update-distribution \
    --id DistributionID \
    --cli-input-yaml file://dist-config.yaml
```

Lorsque la commande réussit, vous voyez une sortie similaire à la suivante, qui décrit la distribution qui vient d'être mise à jour avec l'association de fonctions. L'exemple de sortie suivant est tronqué pour plus de lisibilité.

```
Distribution:
  ARN: arn:aws:cloudfront::111122223333:distribution/EBEDLT3BGRBBW
  ... truncated ...
  DistributionConfig:
    ... truncated ...
    DefaultCacheBehavior:
      ... truncated ...
      FunctionAssociations:
        Items:
        - EventType: viewer-request
          FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
        Quantity: 1
      ... truncated ...
  DomainName: d111111abcdef8.cloudfront.net
  Id: EDFDVBD6EXAMPLE
  LastModifiedTime: '2021-04-19T22:39:09.158000+00:00'
  Status: InProgress
ETag: E2VJGGQEG1JT8S
```

Le `Status` de la distribution passe à `InProgress` pendant le redéploiement de la distribution. Dès que la nouvelle configuration de distribution atteint un emplacement CloudFront périphérique, celui-ci commence à utiliser la fonction associée. Lorsque la distribution est entièrement déployée, elle `Status` redevient`Deployed`, ce qui indique que la CloudFront fonction associée est active dans tous les sites CloudFront périphériques du monde entier. Cela prend généralement quelques minutes.

Amazon CloudFront KeyValueStore

CloudFront KeyValueStore est une banque de données de valeurs clés sécurisée, globale et à faible latence qui permet un accès en lecture depuis CloudFront Functions, permettant ainsi une logique personnalisable avancée aux emplacements CloudFront périphériques.

Vous pouvez ainsi mettre à jour le code de fonction et les données associées à une fonction indépendamment les unes des autres. CloudFront KeyValueStore Cette séparation simplifie le code des fonctions et facilite la mise à jour des données sans qu'il soit nécessaire de déployer des modifications de code.

> **Note**
>
> Pour être utilisée CloudFront KeyValueStore, votre CloudFront fonction doit utiliser le JavaScript runtime 2.0.

La procédure générale d'utilisation des paires clé-valeur est la suivante :

- Créez des magasins de valeurs clés et remplissez-les d'un ensemble de paires clé-valeur. Vous pouvez ajouter vos boutiques à valeur clé à un compartiment Amazon S3 ou les saisir manuellement.
- Associez les magasins de valeurs clés à votre CloudFront fonction.
- Dans votre code de fonction, utilisez le nom de la clé pour extraire la valeur associée à la clé ou pour évaluer si une clé existe. Pour plus d'informations sur l'utilisation de paires clé-valeur dans le code de fonction, et pour plus d'informations sur les méthodes d'assistance, consultez. the section called “Méthodes d’aide pour les magasins de clés-valeurs”

Pour plus d'informations sur la mise en route CloudFront KeyValueStore, consultez le billet de CloudFront KeyValueStore AWS blog « Présentation d'Amazon ».

Vous pouvez utiliser la CloudFront console, l' CloudFront API ou un AWS SDK compatible. Pour commencer CloudFront KeyValueStore, consultez les rubriques suivantes.

Rubriques

- Cas d’utilisation
- Formats de valeurs pris en charge
- Sécurité
- Travaillez avec Key Value Store
- Utilisation de données clé-valeur

Cas d’utilisation

Les cas d'utilisation typiques des paires clé-valeur sont les suivants :

- Réécritures ou redirections d’URL. La paire clé-valeur peut contenir les URL réécrites ou les URL de redirection.
- Tests A/B et indicateurs de fonctionnalités. Vous pouvez créer une fonction pour effectuer des tests en attribuant un pourcentage de trafic à une version spécifique de votre site Web.
- Autorisation d’accès. Vous pouvez mettre en œuvre un contrôle d'accès pour autoriser ou refuser les demandes en fonction de critères que vous avez définis et des données stockées dans un magasin de valeurs clés.

Formats de valeurs pris en charge

La valeur d'une paire clé-valeur peut être stockée dans l'un des formats suivants :

- Une chaîne
- Une chaîne codée en octets
- JSON

Sécurité

La CloudFront fonction et toutes ses valeurs clés stockent les données sont traitées de manière sécurisée, comme suit :

- CloudFront chiffre chaque valeur clé stockée au repos et pendant le transit (lors de la lecture ou de l'écriture dans les magasins de valeurs clés) lorsque vous appelez les opérations de l'CloudFront KeyValueStoreAPI.
- Lorsque la fonction est exécutée, CloudFront déchiffre chaque paire clé-valeur en mémoire aux emplacements périphériques. CloudFront

Travaillez avec Key Value Store

Vous devez créer un magasin clé-valeur pour contenir les paires clé-valeur que vous souhaitez utiliser dans CloudFront Functions.

Après avoir créé les magasins de valeurs clés et les paires clé-valeur ajoutées, vous pouvez utiliser les valeurs clés dans votre code de CloudFront fonction. Le JavaScript runtime 2.0 inclut des méthodes d'assistance pour travailler avec des valeurs clés dans le code de fonction. Pour plus d'informations, consultez the section called “Méthodes d’aide pour les magasins de clés-valeurs”.

Rubriques

Créez un magasin de valeur clé

Vous pouvez créer un magasin clé-valeur vide, puis ajouter des paires clé-valeur ultérieurement. Vous pouvez également créer un magasin clé-valeur et ses paires clé-valeur en même temps.

> **Note**
>
> Si vous spécifiez votre source de données à partir d'un compartiment Amazon S3, vous devez disposer des `s3:GetBucketLocation` autorisations `s3:GetObject` et pour accéder à ce compartiment. Si vous ne disposez pas de ces autorisations, vous ne CloudFront pourrez pas créer correctement votre magasin de valeurs clés.

Console

Pour créer des magasins de valeurs clés (console)

1. Décidez si vous souhaitez ajouter des paires clé-valeur en même temps que vous créez les magasins clé-valeur. Cette fonctionnalité d'importation est prise en charge à la fois sur la CloudFront console et avec les CloudFront API et AWS les SDK. Toutefois, il n'est pris en charge que lorsque vous créez initialement les magasins de valeurs clés.

   Si vous souhaitez utiliser un fichier, créez-le maintenant.

2. Connectez-vous à la page Fonctions AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
3. Cliquez sur l'onglet KeyValueStores. Choisissez Create KeyValueStore.
4. Entrez un nom et une description facultative pour les magasins de valeurs clés.
5. Complétez URI S3 :

   - Si vous avez préparé un fichier de paires clé-valeur, entrez le chemin d'accès au compartiment Amazon S3 dans lequel vous avez stocké le fichier.
   - Laissez ce champ vide si vous prévoyez d’entrer manuellement les paires clé-valeur.
6. Choisissez Créer. Le magasin de valeurs clés existe désormais.

   La page de détails des nouvelles banques de valeurs clés apparaît. Les informations figurant sur cette page incluent l’ID et l’ARN du magasin de clés-valeurs.

   - L'identifiant est une chaîne de caractères aléatoire unique dans votre AWS compte.
   - La syntaxe de l’ARN est la suivante :

     Compte AWS:key-value-store/la valeur clé stocke l'ID
7. Examinez la section Paires clé-valeur. Si vous avez importé un fichier, cette section présente quelques paires. Sinon, elle est vide. Vous pouvez effectuer les actions suivantes :

   - Si vous n'avez pas importé de fichier depuis un compartiment Amazon S3, et si vous souhaitez ajouter des paires clé-valeur dès maintenant, vous pouvez compléter cette section.
   - Si vous avez importé un fichier, vous pouvez également ajouter d’autres valeurs manuellement.
   - Vous pouvez laisser cette section vide et ajouter les paires ultérieurement en modifiant les magasins de valeurs clés.

   Pour ajouter les paires dès maintenant :

   - Cliquez sur le bouton Ajouter des paires clé-valeur.
   - Choisissez Ajouter une paire et entrez un nom et une valeur.
   - Choisissez à nouveau le bouton Ajouter une paire pour ajouter des paires supplémentaires.

Lorsque vous avez terminé, choisissez Enregistrer les modifications pour enregistrer toutes les paires dans le magasin de clés-valeurs. Dans la boîte de dialogue de confirmation qui apparaît, choisissez Terminé.

8. Complétez la section Fonctions associées si vous souhaitez associer les magasins de valeurs clés à une fonction dès maintenant. Vous pouvez également créer cette association ultérieurement, soit à partir de la page de détails de cette clé stocke les valeurs, soit à partir de la page de détails des fonctions.

   Pour créer l'association dès maintenant, choisissez le bouton Accéder aux fonctions. Pour plus d'informations, consultez ??? ou ???.

Programmatically

Pour créer des boutiques à valeur ajoutée

1. Décidez si vous souhaitez ajouter des paires clé-valeur en même temps que vous créez les magasins clé-valeur. (Vous pouvez également ajouter une paire clé-valeur ultérieurement.) Cette fonctionnalité d'importation est prise en charge à la fois sur la CloudFront console et avec CloudFront les API et les SDK. Mais il n'est pris en charge que lorsque vous créez initialement les magasins de valeurs clés.

   Si vous souhaitez utiliser un fichier, créez-le maintenant.
2. Utilisez l'opération de création de l' CloudFront API ou de votre AWS SDK préféré. Par exemple, pour l'API REST, utilisez CloudFront. CreateKeyValueStore. L'opération prend plusieurs paramètres :
   - Un nom
   - Un paramètre `configuration` qui inclut un commentaire.
   - `import-source`Paramètre qui vous permet d'importer des paires clé-valeur à partir d'un fichier stocké dans un compartiment Amazon S3. Notez que vous ne pouvez effectuer d'importation à partir d'un fichier que lors de la création initiale des magasins de valeurs clés. Pour obtenir des informations sur le format de ce fichier, consultez the section called "Création d'un fichier de paires clé-valeur".

La réponse de l'opération inclut les informations suivantes :

- Les valeurs transmises dans la demande, y compris le nom que vous avez attribué.

- Des données telles que l'heure de création.
- Un ETag (par exemple, ETVABCEXAMPLE2), l'ARN qui inclut le nom des stockages de valeurs clés (par exemple,). `arn:aws:cloudfront::111122223333:key-value-store/MaxAge`

  Vous utiliserez une combinaison de l'ETag, de l'ARN et du nom pour travailler avec les valeurs clés stockées par programmation.

Statuts des magasins de valeur clés

Lorsque vous créez un magasin de valeurs clés, le magasin de données peut avoir les valeurs d'état suivantes.

Valeur	Description
Approvisionnement	Le magasin de valeurs clés a été créé et CloudFront traite la source de données que vous avez spécifiée.
Prêt	Le magasin de valeurs clés a été créé et a traité CloudFront avec succès la source de données que vous avez spécifiée.
Échec de l'importation	CloudFront n'a pas pu traiter la source de données que vous avez spécifiée . Ce statut peut apparaître si le format de votre fichier n'est pas valide ou s'il dépasse la limite de taille. Pour plus d'informations, consultez Création d'un fichier de paires clé-valeur.

Associer un magasin de valeurs clés à une fonction

Vous associez un magasin de clés-valeurs à une fonction en travaillant dans la fonction. Vous devez effectuer cette association afin d'utiliser les paires clé-valeur de ce magasin dans cette fonction. Les règles suivantes s'appliquent :

- Une fonction peut avoir un seul magasin de clés-valeurs.
- Un magasin de clés-valeurs peut être associé à plusieurs fonctions.

Vous pouvez utiliser une association des façons suivantes.

- Vous pouvez créer une association entre une fonction et un magasin de clés-valeurs :

- Sur la CloudFront console, consultez la page de détails des stockages de valeurs clés et cliquez sur le bouton Accéder aux fonctions. La page appropriée apparaît : la liste Fonctions (s'il n'y a actuellement aucune fonction associée) ou la page de détails des fonctions (s'il existe actuellement une association). Pour plus d'informations, consultez the section called "Associer un magasin de valeurs clés à une fonction".
- Par programmation, utilisez l'opération de mise à jour des fonctions de votre CloudFront API ou SDK préféré.

Après avoir créé l'association (ou si vous modifiez l'association), vous devez tester la fonction et vous devez republier la fonction.

- Si vous modifiez un magasin de valeurs clés sans modifier les paires clé-valeur, vous n'avez pas besoin de renouveler l'association (ce qui signifie que vous n'avez pas besoin de publier à nouveau). Mais vous devriez tester la fonction.
- Si vous modifiez les paires clé-valeur dans les magasins clé-valeur, vous n'avez pas besoin de renouveler l'association (ce qui signifie que vous n'avez pas besoin de publier à nouveau). Mais vous devez tester la fonction pour vérifier qu'elle fonctionne avec les modifications apportées aux paires clé-valeur.
- Vous pouvez afficher toutes les fonctions qui utilisent des stockages de valeurs-clés spécifiques. Sur la CloudFront console, consultez la page de détails des stockages de valeurs clés.

Modifier un magasin de valeurs clés

Vous pouvez travailler avec les paires clé-valeur et modifier l'association entre les magasins de valeurs clés et la fonction.

Console

Pour modifier un magasin de valeurs clés

1. Connectez-vous à la page Fonctions AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Cliquez sur l'onglet KeyValueStores. Sélectionnez le magasin de clés-valeurs que vous souhaitez modifier. La page de détails s'affiche.

- Pour travailler avec les paires clé-valeur, cliquez sur le bouton Modifier dans la section Paires clé-valeur. Vous pouvez ajouter d'autres paires clé-valeur, supprimer n'importe quelle paire clé-valeur et modifier la valeur d'une paire clé-valeur existante. Lorsque vous avez terminé, choisissez Enregistrer les modifications.
- Pour travailler avec l'association pour ces stockages de valeurs clés, cliquez sur le bouton Accéder aux fonctions. La page appropriée apparaît : la liste Fonctions (s'il n'y a actuellement aucune fonction associée) ou la page de détails des fonctions (s'il existe actuellement une association). Pour plus d'informations, consultez the section called "Associer un magasin de valeurs clés à une fonction".

Programmatically

Vous pouvez utiliser les magasins de valeurs clés de différentes manières.

Modifier les paires clé-valeur

Vous pouvez ajouter d'autres paires clé-valeur, supprimer une ou plusieurs paires clé-valeur et modifier la valeur d'une paire clé-valeur existante. Pour plus d'informations, consultez the section called "Utilisation de paires clé-valeur par programmation".

Modifier l'association de fonctions pour les magasins de valeurs clés

Pour travailler avec l'association chargée de ces magasins à valeur clé, voirthe section called "Fonctions de mise à jour". Vous aurez besoin de l'ARN des magasins de valeurs clés. Pour plus d'informations, consultez the section called "Obtenir une référence à un magasin de valeurs clés".

Supprimer un magasin de valeurs clés

Vous pouvez supprimer votre banque de valeurs clés à l'aide de la CloudFront console ou de l'API.

Console

Pour supprimer un magasin de valeurs clés

1. Connectez-vous à la page Fonctions AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Vérifiez si la valeur clé stockée est associée à une fonction. S'il l'est, supprimez l'association. Pour plus d'informations sur ces étapes, consultez ???.

3. Cliquez sur l'onglet KeyValueStores. Sélectionnez le magasin de valeurs clés que vous souhaitez modifier, puis choisissez Supprimer.

Programmatically

Pour supprimer un magasin de valeurs clés

1. Obtenez l'ETag et le nom des magasins de valeurs clés. Pour plus d'informations, consultez the section called "Obtenir une référence à un magasin de valeurs clés".
2. Vérifiez si la valeur clé stockée est associée à une fonction. S'il l'est, supprimez l'association. Pour plus d'informations sur ces étapes, consultez ???.
3. Pour supprimer les stockages de valeurs clés, utilisez l'opération de suppression de votre CloudFront API ou SDK préféré. Par exemple, pour l'API REST, utilisez CloudFront.DeleteKeyValueStore.

Obtenir une référence à un magasin de valeurs clés

Pour travailler avec les magasins de valeurs clés de manière programmatique, vous avez besoin de l'ETag et du nom du magasin de valeurs clés. Pour obtenir ces données, utilisez l' CloudFront API ou le AWS SDK de votre choix et procédez comme suit :

1. Utilisez l'opération CloudFront.ListKeyValueStoresAPI pour renvoyer une liste de magasins de valeurs clés. Recherchez le nom de la banque de valeurs clés que vous souhaitez modifier.
2. Utilisez l'opération CloudFront.DescribeKeyValueStoreAPI et spécifiez le nom du magasin de valeurs clés que vous avez renvoyé à l'étape précédente.

La réponse inclut un UUID, l'ARN des magasins de valeurs clés et l'ETag des magasins de valeurs clés.

- L'UUID est de 128 bits. Par exemple, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`
- L'ARN inclut le Compte AWS nombre, la constante `key-value-store` et l'UUID. Par exemple :

  `arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`
- Un ETag se présente comme suit : `ETVABCEXAMPLE2`

Pour plus d'informations sur l'`DescribeKeyValueStore`opération, consultezthe section called “À propos CloudFront KeyValueStore”.

Création d'un fichier de paires clé-valeur

Lorsque vous créez un fichier codé en UTF-8, utilisez le format JSON suivant :

```
{
  "data":[
    {
      "key":"key1",
      "value":"value"
    },
    {
      "key":"key2",
      "value":"value"
    }
  ]
}
```

Votre fichier ne peut pas contenir de clés dupliquées. Si vous avez spécifié un fichier non valide dans votre compartiment Amazon S3, vous pouvez le mettre à jour pour supprimer les doublons, puis réessayer de créer votre magasin de valeurs clés.

Pour plus d’informations, consultez Créez un magasin de valeur clé.

> **Note**
>
> Le fichier de votre source de données et ses paires clé-valeur présentent les limites suivantes :
>
> - Taille du fichier : 5 Mo
> - Taille de la clé : 512 caractères
> - Taille de la valeur : 1024 caractères

Utilisation de données clé-valeur

Vous pouvez utiliser des paires clé-valeur dans un magasin clé-valeur existant de la manière suivante :

- À l'aide de la CloudFront console Amazon.
- À l'aide de CloudFront KeyValueStore l'API ou de votre AWS SDK préféré.

Cette section décrit comment ajouter des paires clé-valeur à un magasin clé-valeur existant. Pour inclure des paires clé-valeur lors de la création initiale des magasins clé-valeur, voir. the section called “Créez un magasin de valeur clé”

Rubriques

Utilisation de paires clé-valeur à l'aide de la console CloudFront

Vous pouvez utiliser la CloudFront console pour travailler avec vos paires clé-valeur.

Pour travailler avec des paires clé-valeur

1. Connectez-vous à la page Fonctions AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Cliquez sur l'onglet KeyValueStores. Sélectionnez le magasin de clés-valeurs que vous souhaitez modifier. La page de détails s’affiche.
3. Dans la section Paires de valeurs clés, choisissez Modifier.
4. Vous pouvez ajouter une paire clé-valeur, supprimer une paire clé-valeur ou modifier la valeur d'une paire clé-valeur existante.
5. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Utilisation de paires clé-valeur par programmation

> **Note**
>
> L'CloudFront KeyValueStoreAPI possède un espace de noms différent de celui de l'CloudFront API.

Rubriques

Obtention d’une référence à un magasin de clés-valeurs

Lorsque vous entrez une opération d'écriture à l'aide de CloudFront KeyValueStore, vous devez transmettre l'ARN et l'ETag des magasins de valeurs clés. Pour obtenir ces données, procédez comme suit :

1. Utilisez l'opération de liste de vos CloudFront API ou SDK préférés. Par exemple, pour l’API REST, utilisez CloudFront.ListKeyValueStores. La réponse inclut une liste de magasins de clés-valeurs. Recherchez le nom du magasin de clés-valeurs que vous souhaitez modifier.
2. Utilisez l'opération de description de votre CloudFront KeyValueStore API ou SDK préféré. Par exemple, pour l’API REST, utilisez CloudFrontKeyValueStore.DescribeKeyValueStore. Transmettez le nom que vous avez obtenu à l’étape précédente.

   > **Note**
   >
   > Utilisez l'opération depuis l' CloudFront KeyValueStore API, et non depuis l' CloudFront API. Pour plus d’informations, consultez the section called “À propos CloudFront KeyValueStore”.

   La réponse inclut l'ARN et l'ETag des magasins de valeurs clés.

   - L'ARN inclut le Compte AWS nombre, la constante `key-value-store` et l'UUID. Par exemple :

     ```
     arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
     ```

   - Un ETag se présente comme suit : `ETVABCEXAMPLE2`

Modification des paires clé-valeur dans un magasin clé-valeur

Vous pouvez utiliser les paires clé-valeur à l'aide des opérations suivantes de votre CloudFront KeyValueStore API ou SDK préféré. Toutes ces opérations fonctionnent sur un magasin de valeurs clés spécifié :

- `CloudFrontKeyValueStore.DeleteKey` : supprimez une clé. Consultez DeleteKey.
- `CloudFrontKeyValueStore.GetKey` : obtenez une clé. Consultez GetKey.

- `CloudFrontKeyValueStore.ListKeys` : répertoriez les clés. Consultez ListKeys.

- `CloudFrontKeyValueStore.PutKey` : vous pouvez effectuer deux actions :
  - Créez une nouvelle paire clé-valeur dans un magasin de valeurs clés : dans ce cas, transmettez un nouveau nom et une nouvelle valeur de clé.
  - Définissez une valeur différente dans une paire clé-valeur existante : dans ce cas, transmettez un nom de clé existant et une nouvelle valeur de clé.

  Consultez PutKey.
- `CloudFrontKeyValueStore.UpdateKeys`: vous pouvez effectuer une ou plusieurs des actions suivantes en une seule all-or-nothing opération :
  - Supprimez une ou plusieurs paires clé-valeur.
  - Créez une ou plusieurs nouvelles paires clé-valeur.
  - Définir une valeur différente dans une ou plusieurs paires clé-valeur existantes.

  Consultez UpdateKeys.

À propos CloudFront KeyValueStore

Pour utiliser des paires clé-valeur par programmation dans un magasin clé-valeur existant, vous utilisez le service. CloudFront KeyValueStore

Pour inclure certaines paires clé-valeur dans les magasins de valeurs clés lorsque vous créez initialement les magasins de valeurs clés, vous utilisez le CloudFront service.

Opération de description

L' CloudFront API et l' CloudFront KeyValueStore API disposent toutes deux d'une opération de description qui renvoie des données sur les stockages de valeurs clés :

- L' CloudFront API fournit des données telles que le statut et la date à laquelle le magasin lui-même a été modifié pour la dernière fois.
- L' CloudFront KeyValueStore API fournit des données sur le contenu de la ressource de stockage, à savoir les paires clé-valeur du magasin et la taille du contenu.

Les opérations de description dans les deux API renvoient des données légèrement différentes qui identifient les principales réserves de valeurs :

- L'opération de description dans l' CloudFront API renvoie un ETag, l'UUID et l'ARN des magasins de valeurs clés.

- L'opération de description dans l' CloudFront KeyValueStore API renvoie un ETag et l'ARN des magasins de valeurs clés.

> **Note**
>
> Chaque opération de description renvoie un ETag différent. Les ETags ne sont pas interchangeables.
> Lorsque vous effectuez une opération dans l’une des API, vous devez transmettre l’ETag à partir de l’API appropriée. Par exemple, dans l'opération de suppression CloudFront KeyValueStore, transmettez l'ETag que vous avez obtenu lors de l'opération de description dans CloudFront KeyValueStore.

Exemple de code pour CloudFront KeyValueStore

Example : appel de l'opération **`DescribeKeyValueStore`** API

L'exemple de code suivant vous montre comment appeler l'opération `DescribeKeyValueStore` d'API pour un magasin de valeurs clés.

```
const {
  CloudFrontKeyValueStoreClient,
  DescribeKeyValueStoreCommand,
} = require("@aws-sdk/client-cloudfront-keyvaluestore");

require("@aws-sdk/signature-v4-crt");

(async () => {
  try {
    const client = new CloudFrontKeyValueStoreClient({
      region: "us-east-1"
    });
    const input = {
```

```
      KvsARN: "arn:aws:cloudfront::123456789012:key-value-store/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
    };
    const command = new DescribeKeyValueStoreCommand(input);

    const response = await client.send(command);
  } catch (e) {
    console.log(e);
  }
})();
```

Personnalisez à la périphérie avec Lambda @Edge

Lambda @Edge est une extension de. AWS Lambda Lambda @Edge est un service de calcul qui vous permet d'exécuter des fonctions qui personnalisent le contenu diffusé par Amazon CloudFront . Vous pouvez créer des fonctions Node.js ou Python dans la console Lambda dans l'une d'elles Région AWS, dans l'est des États-Unis (Virginie du Nord).

Vous ajoutez ensuite des déclencheurs dans le Lambda ou dans la CloudFront console pour que les fonctions s'exécutent dans AWS des emplacements plus proches du spectateur, sans provisionner ni gérer de serveurs. Vous pouvez éventuellement utiliser les opérations Lambda et CloudFront API pour configurer vos fonctions et vos déclencheurs par programmation.

Lambda@Edge s'adapte automatiquement, de quelques requêtes par jour jusqu'à des milliers de requêtes par seconde. Le traitement des demandes à AWS des emplacements plus proches de l'utilisateur plutôt que sur les serveurs d'origine réduit considérablement le temps de latence et améliore l'expérience utilisateur.

Rubriques

- Découvrez comment Lambda @Edge gère les demandes et les réponses
- Comment utiliser Lambda @Edge
- Commencez avec les fonctions Lambda @Edge
- Configuration des autorisations et des rôles IAM pour Lambda @Edge
- Écrire et créer une fonction Lambda @Edge
- Ajouter des déclencheurs pour une fonction Lambda @Edge
- Tester et déboguer les fonctions Lambda @Edge
- Supprimer les fonctions et les répliques Lambda @Edge

- Structure d'événement Lambda@Edge
- Travailler avec les demandes et les réponses
- Exemples de fonctions Lambda@Edge

Découvrez comment Lambda @Edge gère les demandes et les réponses

Lorsque vous associez une CloudFront distribution à une fonction Lambda @Edge, elle CloudFront intercepte les demandes et les réponses à CloudFront des emplacements périphériques. Vous pouvez exécuter des fonctions Lambda lorsque les CloudFront événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un téléspectateur (demande du téléspectateur)
- Avant CloudFront de transmettre une demande à l'origine (demande d'origine)
- Quand CloudFront reçoit une réponse de l'origine (réponse d'origine)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)

Si vous l'utilisez AWS WAF, la demande du visualiseur Lambda @Edge est exécutée une fois les AWS WAF règles appliquées.

Pour plus d’informations, consultez Travailler avec les demandes et les réponses et Structure d'événement Lambda@Edge.

Comment utiliser Lambda @Edge

Le traitement Lambda @Edge peut être utilisé à de nombreuses fins dans votre distribution Amazon CloudFront . Par exemple :

- Une fonction Lambda peut inspecter les cookies et réécrire les URL afin que les utilisateurs voient des versions différentes d'un site à des fins de test A/B.
- CloudFront peuvent renvoyer différents objets aux spectateurs en fonction de l'appareil qu'ils utilisent en vérifiant l'`User-Agent`en-tête, qui inclut des informations sur les appareils. Par exemple, ils CloudFront peuvent renvoyer différentes images en fonction de la taille de l'écran de leur appareil. De même, la fonction peut prendre en compte la valeur de l'`Refererer`en-tête et CloudFront renvoyer les images aux robots dont la résolution disponible est la plus faible.
- Ou, vous pouvez vérifier les cookies pour d'autres critères. Par exemple, sur un site Web de vente au détail qui vend des vêtements, si vous utilisez des cookies pour indiquer la couleur choisie par

un utilisateur pour une veste, une fonction Lambda peut modifier la demande afin de CloudFront renvoyer l'image d'une veste dans la couleur sélectionnée.

- Une fonction Lambda peut générer des réponses HTTP lorsque des événements de demande d' CloudFront utilisateur ou de demande d'origine se produisent.
- Une fonction peut inspecter les en-têtes ou les jetons d'autorisation et insérer un en-tête pour contrôler l'accès à votre contenu avant de CloudFront transmettre la demande à votre origine.
- Une fonction Lambda peut également effectuer des appels réseau à des ressources externes pour confirmer les informations d'identification utilisateur, ou récupérer du contenu supplémentaire pour personnaliser une réponse.

Pour plus d'idées, y compris des exemples de code, consultezExemples de fonctions Lambda@Edge.

Pour une procédure expliquant comment configurer Lambda @Edge dans la console, consultez. Tutoriel : Création d'une fonction Lambda @Edge de base

Commencez avec les fonctions Lambda @Edge

Avec Lambda @Edge, vous pouvez utiliser des CloudFront déclencheurs pour appeler une fonction Lambda. Lorsque vous associez une CloudFront distribution à une fonction Lambda, CloudFront intercepte les demandes et les réponses à des emplacements CloudFront périphériques et exécute la fonction. Les fonctions Lambda peuvent améliorer la sécurité ou personnaliser les informations proches de vos spectateurs afin d'améliorer les performances.

La liste suivante fournit un aperçu de base de la création et de l'utilisation de fonctions Lambda avec. CloudFront Pour un step-by-step didacticiel, voirTutoriel : Création d'une fonction Lambda @Edge de base.

1. Dans la AWS Lambda console, créez une fonction Lambda dans la région USA Est (Virginie du Nord). (Vous pouvez également créer la fonction par programmation à l'aide de l'un des AWS SDK.)
2. Enregistrez et publiez une version numérotée de la fonction.

   Si vous souhaitez modifier la fonction, vous devez modifier la version $LATEST de la fonction dans la région USA Est (Virginie du Nord). Ensuite, avant de le configurer pour qu'il fonctionne CloudFront, vous publiez une nouvelle version numérotée.

3. Associez la fonction à une CloudFront distribution et à un comportement de cache. Spécifiez ensuite un ou plusieurs CloudFront événements (déclencheurs) à l'origine de l'exécution de la fonction. Par exemple, vous pouvez créer un déclencheur pour que la fonction s'exécute lorsqu'elle CloudFront reçoit une demande d'un utilisateur.
4. Lorsque vous créez un déclencheur, Lambda crée des répliques de la fonction dans le monde AWS entier.

> **Tip**
>
> Découvrez comment utiliser Lambda @Edge pour vos propres solutions personnalisées. En savoir plus sur la création et la mise à jour de fonctions, la structure des événements et l'ajout de CloudFront déclencheurs. Vous pouvez également trouver d'autres idées et obtenir des exemples de code dans Exemples de fonctions Lambda@Edge.

Rubriques

- Tutoriel : Création d'une fonction Lambda @Edge de base

Tutoriel : Création d'une fonction Lambda @Edge de base

Ce didacticiel explique comment démarrer avec Lambda @Edge en créant et en configurant un exemple de fonction Node.js qui s'exécute dans. CloudFront Cet exemple ajoute des en-têtes de sécurité HTTP à une réponse lors de la CloudFront récupération d'un fichier. (Cela peut améliorer la sécurité et la confidentialité d'un site Web.)

Vous n'avez pas besoin de votre propre site Web pour ce didacticiel. Toutefois, lorsque vous choisissez de créer votre propre solution Lambda @Edge, vous devez suivre des étapes similaires et sélectionner les mêmes options.

Rubriques

- Étape 1 : s'inscrire à un Compte AWS
- Étape 2 : Créer une distribution CloudFront
- Étape 3 : créer votre fonction
- Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction
- Étape 5 : vérifier l’exécution de la fonction

Étape 1 : s'inscrire à un Compte AWS

Si vous ne l'avez pas déjà fait, inscrivez-vous à un Compte AWS. Pour plus d'informations, consultez Inscrivez-vous pour un Compte AWS.

Étape 2 : Créer une distribution CloudFront

Avant de créer l'exemple de fonction Lambda @Edge, vous devez disposer d'un CloudFront environnement de travail incluant une origine à partir de laquelle diffuser le contenu.

Dans cet exemple, vous créez une CloudFront distribution qui utilise un compartiment Amazon S3 comme origine de la distribution. Si vous avez déjà un environnement à utiliser, vous pouvez ignorer cette étape.

Pour créer une CloudFront distribution avec une origine Amazon S3

1. Créez un compartiment Amazon S3 avec un fichier ou deux, par exemple des fichiers image, comme exemples de contenu. Pour obtenir de l'aide, suivez les étapes dans Chargement de votre contenu sur Amazon S3. Assurez-vous de définir des autorisations pour accorder l'accès public en lecture sur les objets de votre compartiment.
2. Créez une CloudFront distribution et ajoutez votre compartiment S3 comme origine, en suivant les étapes décrites dans Créer une distribution CloudFront Web. Si vous avez déjà une distribution, vous pouvez, au lieu de cela, ajouter le compartiment en tant qu'origine pour cette distribution.

> **Tip**
>
> Notez votre ID de distribution. Plus loin dans ce didacticiel, lorsque vous ajoutez un CloudFront déclencheur pour votre fonction, vous devez choisir l'ID de votre distribution dans une liste déroulante, par exemple,. `E653W22221KDDL`

Étape 3 : créer votre fonction

Au cours de cette étape, vous allez créer une fonction Lambda à partir d'un modèle de plan dans la console Lambda. La fonction ajoute du code pour mettre à jour les en-têtes de sécurité de votre CloudFront distribution.

Pour créer une fonction Lambda

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/lambda/.

   > **Important**
   >
   > Assurez-vous que vous êtes dans le US-east-1 (Virginie du Nord) (Région AWS us-east-1). Vous devez être dans cette région pour créer des fonctions Lambda@Edge.

2. Choisissez Créer une fonction.
3. Sur la page Créer une fonction, choisissez Utiliser un plan, puis filtrez les CloudFront plans en les saisissant **`cloudfront`** dans le champ de recherche.

   > **Note**
   >
   > CloudFront les plans ne sont disponibles que dans la région US-east-1 (Virginie du Nord) (us-east-1).

4. Choisissez le plan d'en-tête de réponse HTTP Modify comme modèle pour votre fonction.
5. Entrez les informations suivantes sur votre fonction :

   Nom de la fonction

   Entrez un nom pour votre fonction.

   Rôle d'exécution

   Choisissez la façon de définir les autorisations pour votre fonction. Pour utiliser le modèle de politique d'autorisation de base recommandé par Lambda @Edge, choisissez Create a new role from AWS policy templates.

   Nom du rôle

   Entrez un nom pour le rôle créé par le modèle de stratégie.

Modèles de politique

Lambda ajoute automatiquement le modèle de politique Basic Lambda @Edge permissions parce que vous avez choisi un CloudFront plan comme base pour votre fonction. Ce modèle de politique ajoute des autorisations de rôle d'exécution qui CloudFront permettent d'exécuter votre fonction Lambda pour vous dans le CloudFront monde entier. Pour plus d'informations, consultez Configuration des autorisations et des rôles IAM pour Lambda @Edge.

6. Choisissez Créer une fonction.
7. Dans le volet Deploy to Lambda @Edge qui apparaît, choisissez Annuler. (Pour ce didacticiel, vous devez modifier le code de la fonction avant de déployer la fonction sur Lambda @Edge.)
8. Faites défiler la page jusqu'à la section Source du code.
9. Remplacez le code de modèle par une fonction qui modifie les en-têtes de sécurité renvoyés par votre origine. Par exemple, vous pouvez utiliser du code tel que :

```
'use strict';
exports.handler = (event, context, callback) => {

    //Get contents of response
    const response = event.Records[0].cf.request;
    const headers = response.headers;

    //Set new headers
    headers['strict-transport-security'] = [{key: 'Strict-Transport-Security',
 value: 'max-age= 63072000; includeSubdomains; preload'}];
    headers['content-security-policy'] = [{key: 'Content-Security-Policy', value:
 "default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; object-
src 'none'"}];
    headers['x-content-type-options'] = [{key: 'X-Content-Type-Options', value:
 'nosniff'}];
    headers['x-frame-options'] = [{key: 'X-Frame-Options', value: 'DENY'}];
    headers['x-xss-protection'] = [{key: 'X-XSS-Protection', value: '1;
 mode=block'}];
    headers['referrer-policy'] = [{key: 'Referrer-Policy', value: 'same-origin'}];

    //Return modified response
    callback(null, response);
};
```

10. Choisissez Fichier, puis Enregistrer pour enregistrer votre code mis à jour.

Passez à la section suivante pour ajouter un CloudFront déclencheur permettant d'exécuter la fonction.

Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction

Maintenant que vous disposez d'une fonction Lambda pour mettre à jour les en-têtes de sécurité, configurez le CloudFront déclencheur pour exécuter votre fonction afin d'ajouter les en-têtes dans toute réponse CloudFront reçue de l'origine de votre distribution.

Pour configurer le CloudFront déclencheur de votre fonction

1. Dans la console Lambda, sur la page d'aperçu des fonctions de votre fonction, choisissez Ajouter un déclencheur.
2. Pour la configuration du déclencheur, choisissez CloudFront.
3. Choisissez Deploy to Lambda @Edge.
4. Dans le volet Deploy to Lambda @Edge, sous Configurer le CloudFront déclencheur, entrez les informations suivantes :

   Distribution

   L'ID CloudFront de distribution à associer à votre fonction. Dans la liste déroulante, choisissez l'ID de distribution.

   Comportement de cache

   Comportement de cache à utiliser avec le déclencheur. Pour cet exemple, laissez la valeur définie sur *, qui correspond au comportement de cache par défaut de votre distribution. Pour plus d’informations, consultez Paramètres de comportement du cache dans la rubrique Référence des paramètres de distribution.

   CloudFront événement

   Déclencheur qui spécifie le moment où votre fonction s'exécute. Nous voulons que la fonction d'en-têtes de sécurité s'exécute chaque fois que CloudFront renvoie une réponse depuis l'origine. Donc, dans la liste déroulante, choisissez Origin response. Pour plus d’informations, consultez Ajouter des déclencheurs pour une fonction Lambda @Edge.
5. Cochez la case Confirmer le déploiement vers Lambda @Edge.
6. Choisissez Deploy (Déployer) pour ajouter le déclencheur et répliquer la fonction dans les emplacements AWS à travers le monde.

7. Attendez que la réplication de la fonction soit terminée. Cela prend généralement plusieurs minutes.

   Vous pouvez vérifier si la réplication est terminée en accédant à la CloudFront console et en consultant votre distribution. Attendez que l'état de distribution passe de Déploiement à une date et à une heure, ce qui signifie que votre fonction a été répliquée. Pour vérifier que la fonction s'exécute correctement, suivez les étapes de la section suivante.

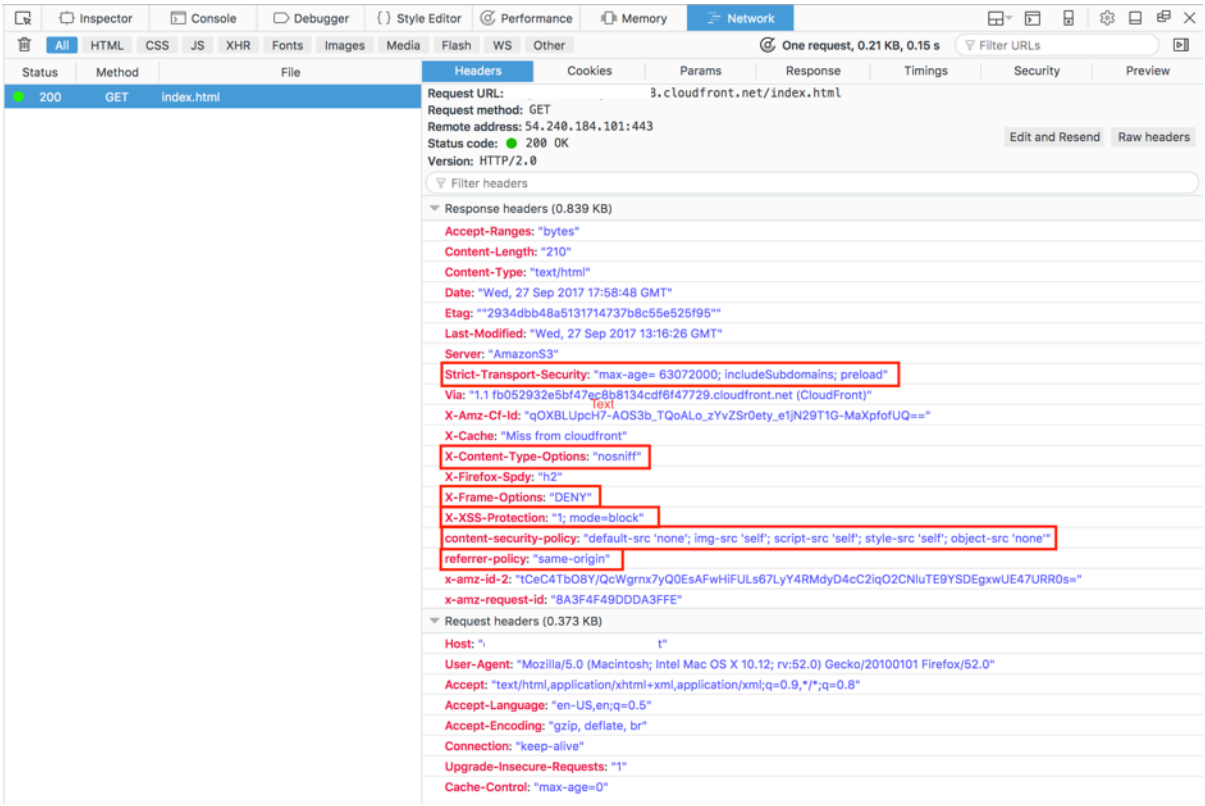
Étape 5 : vérifier l’exécution de la fonction

Maintenant que vous avez créé votre fonction Lambda et configuré un déclencheur pour l'exécuter pour une CloudFront distribution, assurez-vous que la fonction répond à vos attentes. Dans cet exemple, nous vérifions les en-têtes HTTP CloudFront renvoyés pour nous assurer que les en-têtes de sécurité ont été ajoutés.

Pour vérifier que votre fonction Lambda@Edge ajoute des en-têtes de sécurité

1. Dans un navigateur, entrez l'URL d'un fichier dans votre compartiment S3. Par exemple, vous pouvez utiliser une URL similaire à `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Pour plus d'informations sur le nom de CloudFront domaine à utiliser dans l'URL du fichier, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.
2. Ouvrez la barre d'outils Web Developer de votre navigateur. Par exemple, dans votre fenêtre de navigateur Chrome, ouvrez le menu contextuel (clic droit), puis choisissez Inspecter.
3. Choisissez l'onglet Network (Réseau).
4. Rechargez la page pour afficher votre image, puis choisissez une demande HTTP dans le volet de gauche. Vous voyez les en-têtes HTTP s'afficher dans un volet distinct.
5. Parcourez la liste des en-têtes HTTP pour vérifier que les en-têtes de sécurité attendus sont inclus dans la liste. Par exemple, vous pourrez peut-être voir des en-têtes similaires à ceux affichés dans la capture d'écran suivante.



Si les en-têtes de sécurité sont inclus dans votre liste d'en-têtes, cela signifie que vous avez créé avec succès votre première fonction Lambda@Edge. En cas d'erreur de CloudFront retour ou d'autres problèmes, passez à l'étape suivante pour résoudre les problèmes.

Étape 6 : résoudre les problèmes

Si elle CloudFront renvoie des erreurs ou n'ajoute pas les en-têtes de sécurité comme prévu, vous pouvez étudier l'exécution de votre fonction en consultant CloudWatch Logs. Veillez à utiliser les journaux stockés à l' AWS emplacement le plus proche de l'endroit où la fonction est exécutée.

Par exemple, si vous consultez le fichier depuis Londres, essayez de remplacer la région dans la CloudWatch console par Europe (Londres).

Pour examiner les CloudWatch journaux de votre fonction Lambda @Edge

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Modifiez Région en spécifiant l'emplacement qui est montré lorsque vous affichez le fichier dans votre navigateur. C'est là que la fonction s'exécute.

3. Dans le volet de gauche, choisissez Logs (Journaux) pour afficher les journaux de votre distribution.

Pour plus d'informations, consultez Surveillance CloudFront des métriques avec Amazon CloudWatch.

Étape 7 : nettoyer votre exemple de ressources

Si vous avez créé un compartiment et une CloudFront distribution Amazon S3 uniquement pour ce didacticiel, supprimez les AWS ressources que vous avez allouées afin de ne plus payer de frais. Une fois que vous avez supprimé vos AWS ressources, le contenu que vous avez ajouté n'est plus disponible.

Tâches

- Supprimer le compartiment S3
- Supprimer la fonction Lambda
- Supprimer la CloudFront distribution

Supprimer le compartiment S3

Avant de supprimer votre compartiment Amazon S3, assurez-vous que la journalisation est désactivée pour le compartiment. Dans le cas contraire, AWS continue d'écrire des journaux dans votre compartiment lorsque vous le supprimez.

Pour désactiver la journalisation pour un compartiment

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Sélectionnez le compartiment, puis choisissez Properties (Propriétés).
3. Dans Properties (Propriétés), choisissez Logging (Journalisation).
4. Désactivez la case à cocher Activé.
5. Choisissez Enregistrer.

Vous pouvez maintenant supprimer votre compartiment. Pour plus d'informations, consultez la section Suppression d'un compartiment du Guide de l'utilisateur de la console Amazon Simple Storage Service.

Supprimer la fonction Lambda

Pour obtenir des instructions sur la suppression de l'association de fonctions Lambda et éventuellement de la fonction elle-même, reportez-vous à. Supprimer les fonctions et les répliques Lambda @Edge

Supprimer la CloudFront distribution

Avant de supprimer une CloudFront distribution, vous devez la désactiver. Une distribution désactivée n'est plus fonctionnelle et n'accumule pas de frais. Vous pouvez activer une distribution désactivée à tout moment. Une fois que vous avez supprimé une distribution désactivée, celle-ci n'est plus disponible.

Pour désactiver et supprimer une distribution CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution que vous souhaitez désactiver, puis choisissez Désactiver).
3. Lorsque vous serez invité à confirmer l'opération, choisissez Oui, désactiver.
4. Sélectionnez la distribution désactivée, puis choisissez Supprimer.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Oui, supprimer.

Ressources pour en savoir plus

Maintenant que vous avez une idée générale de la manière dont les fonctions Lambda@Edge s'exécutent, lisez les documents suivants pour en savoir plus :

- Exemples de fonctions Lambda@Edge
- Bonnes pratiques de conception Lambda @Edge
- Réduction de la latence et transfert du calcul vers la périphérie avec Lambda @Edge

Configuration des autorisations et des rôles IAM pour Lambda @Edge

Pour configurer Lambda @Edge, vous devez disposer des autorisations et rôles IAM suivants pour Lambda :

- Autorisations IAM : ces autorisations vous permettent de créer votre AWS Lambda fonction et de l'associer à votre CloudFront distribution.

- Un rôle d'exécution de fonction Lambda (rôle IAM) — Les responsables du service Lambda assument ce rôle pour exécuter votre fonction.
- Rôles liés à un service pour Lambda @Edge — Les rôles liés à un service permettent à des utilisateurs spécifiques de Services AWS répliquer des fonctions Lambda dans des fichiers journaux et de les utiliser. Régions AWS CloudWatch CloudFront

Autorisations IAM requises pour associer les fonctions Lambda @Edge aux distributions CloudFront

Outre les autorisations IAM dont vous avez besoin pour Lambda, vous avez besoin des autorisations suivantes pour associer les fonctions Lambda aux distributions : CloudFront

- `lambda:GetFunction`— Accorde l'autorisation d'obtenir des informations de configuration pour votre fonction Lambda et une URL présignée pour télécharger un `.zip` fichier contenant la fonction.
- `lambda:EnableReplication*`— Accorde l'autorisation à la politique de ressources afin que le service de réplication Lambda puisse obtenir le code de fonction et la configuration.
- `lambda:DisableReplication*`— Accorde l'autorisation à la politique de ressources afin que le service de réplication Lambda puisse supprimer la fonction.

> **Important**
>
> Vous devez ajouter l'astérisque (`*`) à la fin des `lambda:DisableReplication*` actions `lambda:EnableReplication*` et.

- Pour la ressource, spécifiez l'ARN de la version de fonction que vous souhaitez exécuter lorsqu'un CloudFront événement se produit, comme dans l'exemple suivant :

  `arn:aws:lambda:us-east-1:123456789012:function:`*`TestFunction`*`:2`
- `iam:CreateServiceLinkedRole`— Accorde l'autorisation de créer un rôle lié à un service que Lambda @Edge utilise pour répliquer les fonctions Lambda. CloudFront Après avoir configuré Lambda @Edge pour la première fois, le rôle lié au service est automatiquement créé pour vous. Il n'est pas nécessaire d'ajouter cette autorisation aux autres distributions qui utilisent Lambda @Edge.
- `cloudfront:UpdateDistribution`ou `cloudfront:CreateDistribution` — Autorise la mise à jour ou la création d'une distribution.

Pour plus d'informations, consultez les rubriques suivantes :

- Identity and Access Management pour Amazon CloudFront
- Autorisations d'accès aux ressources Lambda dans le guide du développeur AWS Lambda

Rôle d'exécution de fonction pour les principaux de service

Vous devez créer un rôle IAM que les responsables `lambda.amazonaws.com` et les responsables du `edgelambda.amazonaws.com` service peuvent assumer lorsqu'ils exécutent votre fonction.

> **Tip**
>
> Lorsque vous créez votre fonction dans la console Lambda, vous pouvez choisir de créer un nouveau rôle d'exécution à l'aide d'un modèle de AWS politique. Cette étape ajoute automatiquement les autorisations Lambda @Edge requises pour exécuter votre fonction. Consultez l'étape 5 du didacticiel : Création d'une fonction Lambda @Edge simple.

Pour plus d'informations sur la création manuelle d'un rôle IAM, consultez la section Création de rôles et attachement de politiques (console) dans le guide de l'utilisateur IAM.

Example Exemple : politique de confiance dans les rôles

Vous pouvez ajouter ce rôle sous l'onglet Trust Relationship de la console IAM. N'ajoutez pas cette politique sous l'onglet Autorisations.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "lambda.amazonaws.com",
               "edgelambda.amazonaws.com"
            ]
         },
         "Action": "sts:AssumeRole"
      }
   ]
```

```
}
```

Pour plus d'informations sur les autorisations que vous devez accorder au rôle d'exécution, consultez la section Autorisations d'accès aux ressources Lambda dans le Guide du AWS Lambda développeur.

Remarques

- Par défaut, chaque fois qu'un CloudFront événement déclenche une fonction Lambda, les données sont écrites dans Logs. CloudWatch Si vous souhaitez utiliser ces journaux, le rôle d'exécution doit être autorisé à écrire des données dans les CloudWatch journaux. Vous pouvez utiliser les paramètres prédéfinis AWSLambdaBasicExecutionRole pour accorder l'autorisation au rôle d'exécution.

  Pour plus d'informations sur CloudWatch les journaux, consultezthe section called "Journaux des fonctions Edge".
- Si votre code de fonction Lambda accède à d'autres AWS ressources, telles que la lecture d'un objet depuis un compartiment S3, le rôle d'exécution doit être autorisé pour effectuer cette action.

Rôles liés à un service pour Lambda@Edge

Lambda @Edge utilise des rôles liés à un service IAM. Un rôle lié à un service est un type unique de rôle IAM lié directement à un service. Les rôles liés à un service sont prédéfinis par le service et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Lambda @Edge utilise les rôles liés aux services IAM suivants :

- AWSServiceRoleForLambdaReplicator – Lambda@Edge utilise ce rôle pour autoriser Lambda@Edge à répliquer des fonctions vers Régions AWS.

  Lorsque vous ajoutez un déclencheur Lambda @Edge pour la première fois CloudFront, un rôle nommé AWSServiceRoleForLambdaReplicator est créé automatiquement pour permettre à Lambda @Edge de répliquer des fonctions sur. Régions AWS Ce rôle est requis pour utiliser les fonctions Lambda @Edge. L'ARN du AWSServiceRoleForLambdaReplicator rôle ressemble à l'exemple suivant :

```
arn:aws:iam::123456789012:role/aws-service-role/
replicator.lambda.amazonaws.com/AWSServiceRoleForLambdaReplicator
```

- AWSServiceRoleForCloudFrontLogger— CloudFront utilise ce rôle pour transférer les fichiers journaux dans CloudWatch. Vous pouvez utiliser des fichiers journaux pour corriger les erreurs de validation Lambda @Edge.

  Le AWSServiceRoleForCloudFrontLogger rôle est créé automatiquement lorsque vous ajoutez une association de fonctions Lambda @Edge pour permettre de transférer les fichiers CloudFront journaux d'erreurs Lambda @Edge vers. CloudWatch L'ARN pour le rôle AWSServiceRoleForCloudFrontLogger prend la forme suivante :

  ```
  arn:aws:iam::account_number:role/aws-service-role/
  logger.cloudfront.amazonaws.com/AWSServiceRoleForCloudFrontLogger
  ```

Un rôle lié à un service simplifie la configuration et l'utilisation de Lambda@Edge, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Lambda@Edge définit les autorisations de ses rôles liés un service et seul Lambda@Edge peut endosser ces rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Vous ne pouvez pas attacher la politique d'autorisations à une autre entité IAM.

Vous devez supprimer toutes les ressources associées CloudFront ou Lambda @Edge avant de pouvoir supprimer un rôle lié à un service. Cela permet de protéger vos ressources Lambda @Edge afin de ne pas supprimer un rôle lié à un service qui est toujours nécessaire pour accéder aux ressources actives.

Pour plus d'informations sur les rôles liés à un service, consultez Rôles liés à un service pour CloudFront.

Autorisations du rôle lié à un service pour Lambda@Edge

Lambda@Edge utilise deux rôles liés à un service nommé AWSServiceRoleForLambdaReplicator et AWSServiceRoleForCloudFrontLogger. Les sections suivantes décrivent comment gérer les autorisations pour chacun de ces rôles.

Table des matières

Autorisations du rôle lié à un service pour Lambda Replicator

Ce rôle lié à un service permet à Lambda de répliquer les fonctions Lambda@Edge vers Régions AWS.

Le rôle lié à un service AWSServiceRoleForLambdaReplicator fait confiance au service `replicator.lambda.amazonaws.com` pour endosser le rôle.

La politique d'autorisations du rôle permet à Lambda@Edge de réaliser les actions suivantes sur les ressources spécifiées :

- `lambda:CreateFunction` sur `arn:aws:lambda:*:*:function:*`
- `lambda:DeleteFunction` sur `arn:aws:lambda:*:*:function:*`
- `lambda:DisableReplication` sur `arn:aws:lambda:*:*:function:*`
- `iam:PassRole` sur `all AWS resources`
- `cloudfront:ListDistributionsByLambdaFunction` sur `all AWS resources`

Autorisations de rôle liées au service pour l'enregistreur CloudFront

Ce rôle lié à un service permet de CloudFront transférer des fichiers journaux CloudWatch afin que vous puissiez corriger les erreurs de validation Lambda @Edge.

Le rôle lié à un service AWSServiceRoleForCloudFrontLogger fait confiance au service `logger.cloudfront.amazonaws.com` pour endosser le rôle.

La politique d'autorisation des rôles permet à Lambda @Edge d'effectuer les actions suivantes sur la ressource spécifiée `arn:aws:logs:*:*:log-group:/aws/cloudfront/*` :

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de supprimer les rôles liés à un service Lambda@Edge. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création de rôles liés à un service pour Lambda@Edge

Vous n'avez généralement pas besoin de créer manuellement les rôles liés à un service pour Lambda@Edge. Le service crée les rôles automatiquement pour vous dans les scénarios suivants :

- Lorsque vous créez un déclencheur pour la première fois, le service crée le AWSServiceRoleForLambdaReplicator rôle (s'il n'existe pas déjà). Ce rôle permet à Lambda de répliquer les fonctions Lambda @Edge sur. Régions AWS

  Si vous supprimez le rôle lié à un service, le rôle sera à nouveau créé lorsque vous ajouterez un nouveau déclencheur pour Lambda@Edge dans une distribution.
- Lorsque vous mettez à jour ou créez une CloudFront distribution associée à Lambda @Edge, le service crée le AWSServiceRoleForCloudFrontLogger rôle (si le rôle n'existe pas déjà). Ce rôle permet CloudFront de transférer vos fichiers journaux vers CloudWatch.

  Si vous supprimez le rôle lié à un service, le rôle sera créé à nouveau lorsque vous mettrez à jour ou créerez une CloudFront distribution associée à Lambda @Edge.

Pour créer manuellement ces rôles liés à un service, vous pouvez exécuter les commandes suivantes AWS Command Line Interface (AWS CLI) :

Pour créer le rôle AWSServiceRoleForLambdaReplicator

- Exécutez la commande suivante.

```
aws iam create-service-linked-role --aws-service-name
 replicator.lambda.amazonaws.com
```

Pour créer le rôle AWSServiceRoleForCloudFrontLogger

- Exécutez la commande suivante.

```
aws iam create-service-linked-role --aws-service-name
 logger.cloudfront.amazonaws.com
```

Modification des rôles liés à un service Lambda@Edge.

Lambda @Edge ne vous permet pas de modifier les rôles AWSServiceRoleForLambdaReplicator ou les rôles liés à un AWSServiceRoleForCloudFrontLogger service. Une fois que le service a créé un rôle lié au service, vous ne pouvez pas modifier le nom du rôle car différentes entités peuvent y faire référence. Néanmoins, vous pouvez utiliser IAM pour modifier la description du rôle. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Pris en charge Régions AWS pour les CloudFront rôles liés à un service

CloudFront prend en charge l'utilisation de rôles liés à un service pour Lambda @Edge dans les domaines suivants : Régions AWS

- US East (N. Virginia) – `us-east-1`
- US East (Ohio) – `us-east-2`
- US West (N. California) – `us-west-1`
- US West (Oregon) – `us-west-2`
- Asia Pacific (Mumbai) – `ap-south-1`
- Asie-Pacifique (Séoul) – `ap-northeast-2`
- Asia Pacific (Singapore) – `ap-southeast-1`
- Asie-Pacifique (Sydney) – `ap-southeast-2`
- Asie-Pacifique (Tokyo) – `ap-northeast-1`
- Europe (Frankfurt) – `eu-central-1`
- Europe (Ireland) – `eu-west-1`
- Europe (London) – `eu-west-2`
- South America (São Paulo) – `sa-east-1`

Écrire et créer une fonction Lambda @Edge

Pour utiliser Lambda @Edge, vous devez écrire le code de votre AWS Lambda fonction. Ensuite, vous configurez Lambda pour exécuter la fonction en fonction d' CloudFrontévénements spécifiques, appelés déclencheurs.

Vous pouvez utiliser le AWS Management Console pour utiliser les fonctions et les CloudFront déclencheurs Lambda, ou vous pouvez utiliser Lambda @Edge par programmation à l'aide de l'API.

Rubriques

Écrivez votre fonction Lambda @Edge

Pour vous aider à écrire des fonctions Lambda @Edge, consultez les ressources suivantes :

- Structure d'événement Lambda@Edge— Comprenez la structure d'événements à utiliser avec Lambda @Edge.
- Exemples de fonctions Lambda@Edge— Exemples de fonctions, telles que les tests A/B et la génération d'une redirection HTTP.

Le modèle de programmation pour utiliser Node.js ou Python avec Lambda @Edge est le même que pour utiliser Lambda dans un. Région AWSPour plus d'informations, voir Création de fonctions Lambda avec Node.js ou Création de fonctions Lambda avec Python dans le Guide du développeur.AWS Lambda

Dans votre fonction Lambda @Edge, incluez le `callback` paramètre et renvoyez l'objet applicable pour les événements de demande ou de réponse :

- Événements de demande – Incluez l'objet `cf.request` dans la réponse.

  Si vous générez une réponse, incluez l'objet `cf.response` dans la réponse. Pour plus d'informations, consultez Générer des réponses HTTP dans les déclencheurs de requêtes.
- Événements de réponse – Incluez l'objet `cf.response` dans la réponse.

Création d'une fonction Lambda @Edge

AWS Lambda Pour configurer l'exécution de fonctions Lambda basées sur des CloudFront événements, suivez cette procédure.

Pour créer une fonction Lambda @Edge (console)

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

2. Si vous avez déjà une ou plusieurs fonctions Lambda, choisissez Create function (Créer fonction).

   Si vous n'avez aucune fonction, choisissez Mise en route.

3. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).

4. Créez une fonction à l'aide de votre propre code ou créez une fonction à partir d'un CloudFront plan.

   - Pour créer une fonction à l'aide de votre propre code, choisissez Créer à partir de zéro.
   - Pour afficher une liste de plans pour CloudFront, tapez cloudfront dans le champ de filtre, puis choisissez Enter.

     Si vous trouvez un plan que vous souhaitez utiliser, choisissez le nom de ce plan.

5. Dans la section Informations de base, spécifiez les valeurs suivantes :

   a. Nom — Entrez le nom de votre fonction.

   b. Rôle : pour démarrer rapidement, choisissez Créer un nouveau rôle à partir de modèles. Vous pouvez également choisir Choisir un rôle existant ou Créer un rôle personnalisé, puis suivre les instructions pour compléter les informations de cette section.

   c. Nom du rôle — Entrez le nom du rôle.

   d. Modèles de politiques — Choisissez les autorisations Lambda de base pour Edge.

6. Si vous avez choisi Créer à partir de zéro à l'étape 4, passez directement à l'étape 7.

   Si vous avez choisi un plan à l'étape 4, la section cloudfront vous permet de créer un déclencheur, qui associe cette fonction à un cache dans une CloudFront distribution et à un événement. CloudFront Pour l'instant, nous vous recommandons de choisir Supprimer, afin qu'il n'y ait pas de déclencheur pour la fonction lorsqu'elle sera créée. Vous pourrez ajouter des déclencheurs par la suite.

   > **Tip**
   >
   > Nous vous recommandons de tester et de déboguer la fonction avant d'ajouter des déclencheurs. Si vous ajoutez un déclencheur maintenant, la fonction s'exécutera dès que vous la créerez, qu'elle aura fini de se répliquer AWS dans le monde entier et que la distribution correspondante sera déployée.

7. Choisissez Créer une fonction.

   Lambda crée deux versions de votre fonction : $LATEST et Version 1. Vous pouvez modifier uniquement la version $LATEST, mais la console affiche initialement la version 1.

8. Pour modifier la fonction, choisissez Version 1 en haut de la page, sous l'ARN de la fonction. Puis, dans l'onglet Versions, choisissez $LATEST. (Si vous avez quitté la fonction, puis êtes revenu à celle-ci, le bouton est appelé Qualificateurs.)
9. Dans l'onglet Configuration, choisissez le Type d'entrée de code applicable. Ensuite, suivez les instructions pour modifier ou charger votre code.
10. Pour Exécution, choisissez la valeur en fonction du code de votre fonction.
11. Dans la section Balises, ajoutez les éventuelles balises applicables.
12. Choisissez Actions, puis Publier une nouvelle version.
13. Saisissez la description de la nouvelle version de la fonction.
14. Choisissez Publish.
15. Testez et déboguez la fonction. Pour plus d'informations sur les tests dans la console Lambda, consultez la section Appel de la fonction Lambda et vérification des résultats, des journaux et des métriques de Créer une fonction Lambda avec la console dans le Guide du développeur AWS Lambda .
16. Lorsque vous êtes prêt à exécuter la fonction pour des CloudFront événements, publiez une autre version et modifiez la fonction pour ajouter des déclencheurs. Pour plus d’informations, consultez Ajouter des déclencheurs pour une fonction Lambda @Edge.

Utiliser l'API ou AWS CLI travailler avec Lambda @Edge

Vous pouvez également utiliser les opérations Lambda et CloudFront API pour configurer les fonctions et les déclencheurs Lambda @Edge par programmation. CloudFront Pour plus d’informations, consultez les rubriques suivantes :

- AWS Lambda API Reference
- Référence CloudFront d'API Amazon
- Vous pouvez également utiliser les commandes AWS Command Line Interface (AWS CLI) suivantes :
  - Fonction de création Lambda
  - CloudFront créer-distribuer

- CloudFront create-distribution-with-tags
- CloudFront distribution des mises à jour
- AWS SDK (voir la section SDK et boîtes à outils.)
- AWS Tools for PowerShell Référence de l'applet de commande

Modifiez votre fonction Lambda

Après avoir créé une fonction Lambda @Edge, vous pouvez utiliser la console Lambda pour la modifier.

> **Remarques**
>
> - La version d'origine est étiquetée $LATEST.
> - Vous ne pouvez modifier que la version $LATEST.
> - Chaque fois que vous modifiez la version $LATEST, vous devez publier une nouvelle version numérotée.
> - Vous ne pouvez pas créer de déclencheurs pour $LATEST.
> - Lorsque vous publiez une nouvelle version d'une fonction, Lambda ne copie pas automatiquement les déclencheurs à partir de la version précédente vers la nouvelle version. Vous devez reproduire les déclencheurs pour la nouvelle version.
> - Lorsque vous ajoutez un déclencheur pour un CloudFront événement à une fonction, s'il existe déjà un déclencheur pour la même distribution, le même comportement de cache et le même événement pour une version antérieure de la même fonction, Lambda supprime le déclencheur de la version précédente.
> - Après avoir mis à jour une CloudFront distribution, par exemple en ajoutant des déclencheurs, vous devez attendre que les modifications se propagent aux emplacements périphériques pour que les fonctions que vous avez spécifiées dans les déclencheurs fonctionnent.

Pour modifier une fonction Lambda (console)

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

2. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Dans la liste des fonctions, choisissez le nom de la fonction.

   Par défaut, la console affiche la version $LATEST. Vous pouvez consulter les versions précédentes (choisissez Qualificateurs), mais vous ne pouvez modifier que $ LATEST.
4. Dans l'onglet Code, pour Code entry type (Type d'entrée de code), choisissez de modifier le code dans le navigateur, de charger un fichier .zip ou de charger un fichier depuis Amazon S3.
5. Choisissez Enregistrer ou Enregistrer et tester.
6. Choisissez Actions, puis Publish new version (Publier nouvelle version).
7. Dans la boîte de dialogue Publier la nouvelle version à partir de $LATEST, indiquez une description de la nouvelle version. Cette description s'affiche dans la liste des versions, accompagnée d'un numéro de version généré automatiquement.
8. Choisissez Publish.

   La nouvelle version devient automatiquement la version la plus récente. Le numéro de version apparaît sur la version dans le coin supérieur gauche de la page.
9. Choisissez l'onglet Triggers (Déclencheurs).
10. Choisissez Add trigger (Ajouter déclencheur).
11. Dans la boîte de dialogue Ajouter un déclencheur, choisissez la zone en pointillés, puis choisissez CloudFront.

    > **Note**
    >
    > Si vous avez déjà créé un ou plusieurs déclencheurs pour une fonction, CloudFront c'est le service par défaut.

12. Spécifiez les valeurs suivantes pour indiquer le moment où vous voulez que la fonction Lambda s'exécute.

    a. ID de distribution — Choisissez l'ID de la distribution à laquelle vous souhaitez ajouter le déclencheur.

    b. Comportement du cache : choisissez le comportement du cache qui spécifie les objets sur lesquels vous souhaitez exécuter la fonction.

    c. CloudFront event — Choisissez l' CloudFront événement à l'origine de l'exécution de la fonction.

d. Activer le déclencheur et la réplication : cochez cette case pour que Lambda réplique la fonction de manière globale. Régions AWS

13. Sélectionnez Envoyer.
14. Pour ajouter d'autres déclencheurs pour cette fonction, répétez les étapes 10 à 13.

Ajouter des déclencheurs pour une fonction Lambda @Edge

Un déclencheur Lambda @Edge est une combinaison d'une CloudFront distribution, d'un comportement de cache et d'un événement qui entraîne l'exécution d'une fonction. Vous pouvez spécifier un ou plusieurs CloudFront déclencheurs qui déclenchent l'exécution de la fonction. Par exemple, vous pouvez créer un déclencheur qui entraîne l'exécution de la fonction lorsqu'un utilisateur CloudFront reçoit une demande concernant un comportement de cache spécifique que vous avez configuré pour votre distribution.

> **Tip**
>
> Lorsque vous créez une CloudFront distribution, vous spécifiez des paramètres qui indiquent CloudFront comment répondre lorsqu'elle reçoit différentes demandes. Les paramètres par défaut sont appelés comportement de cache par défaut pour la distribution. Vous pouvez configurer des comportements de cache supplémentaires qui définissent la manière dont il CloudFront répond dans des circonstances spécifiques, par exemple lorsqu'il reçoit une demande pour un type de fichier spécifique. Pour de plus amples informations, veuillez consulter Paramètres de comportement du cache.

Lorsque vous créez une fonction Lambda, vous ne pouvez spécifier qu'un seul déclencheur. Vous pouvez ajouter d'autres déclencheurs à la même fonction ultérieurement en utilisant la console Lambda ou en modifiant la distribution dans la CloudFront console.

- La console Lambda fonctionne bien si vous souhaitez ajouter d'autres déclencheurs à une fonction pour la même CloudFront distribution.
- La CloudFront console peut être meilleure si vous souhaitez ajouter des déclencheurs pour plusieurs distributions, car il est plus facile de trouver la distribution que vous souhaitez mettre à jour. Vous pouvez également mettre à jour d'autres CloudFront paramètres en même temps.

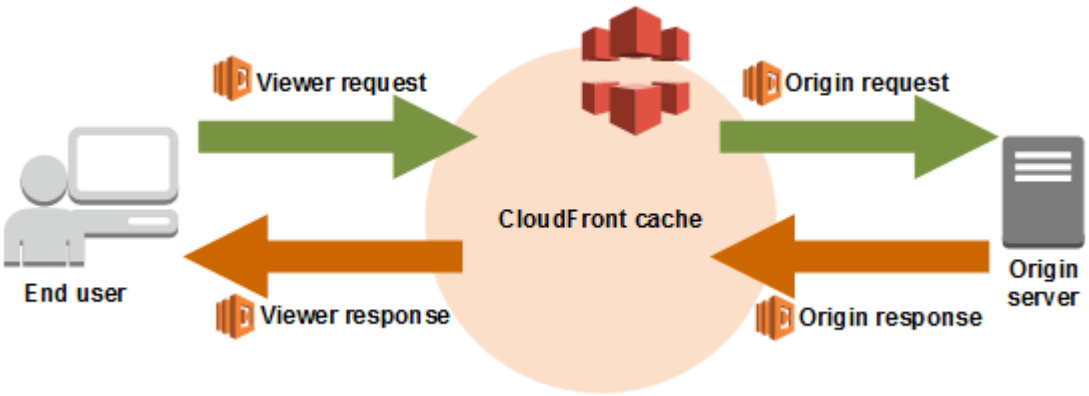
> **Note**
>
> Pour utiliser Lambda @Edge par programmation, voir. Utiliser l'API ou AWS CLI travailler avec Lambda @Edge

Rubriques

- CloudFront événements pouvant déclencher une fonction Lambda @Edge
- Décidez quel CloudFront événement utiliser pour déclencher une fonction Lambda @Edge
- Ajouter des déclencheurs à une fonction Lambda @Edge

CloudFront événements pouvant déclencher une fonction Lambda @Edge

Pour chaque comportement de cache dans une CloudFront distribution Amazon, vous pouvez ajouter jusqu'à quatre déclencheurs (associations) qui déclenchent l'exécution d'une fonction Lambda lorsque des CloudFront événements spécifiques se produisent. CloudFront les déclencheurs peuvent être basés sur l'un des quatre CloudFront événements suivants, comme le montre le schéma suivant.



Les CloudFront événements qui peuvent être utilisés pour déclencher les fonctions Lambda @Edge sont les suivants :

Demande utilisateur

La fonction s'exécute lorsqu'elle CloudFront reçoit une demande d'un visualiseur, avant de vérifier si l'objet demandé se trouve dans le CloudFront cache.

Demande de l’origine

La fonction s'exécute uniquement lorsque CloudFront vous transmettez une demande à votre origine. Lorsque l'objet demandé est dans le CloudFront cache, la fonction ne s'exécute pas.

Réponse de l’origine

La fonction s'exécute après avoir CloudFront reçu une réponse de l'origine et avant de mettre en cache l'objet dans la réponse. Notez que la fonction s'exécute même si une erreur est renvoyée de l'origine.

La fonction ne s’exécute pas dans les cas suivants :

- Lorsque le fichier demandé est dans le CloudFront cache et n'a pas expiré.
- Lorsque la réponse est générée à partir d'une fonction qui a été déclenchée par un événement de demande à l'origine.

Réponse utilisateur

La fonction s'exécute avant de renvoyer le fichier demandé à l'utilisateur. Notez que la fonction s'exécute indépendamment du fait que le fichier soit déjà dans le CloudFront cache ou non.

La fonction ne s’exécute pas dans les cas suivants :

- Lorsque l'origine renvoie un code de statut HTTP égal ou supérieur à 400.
- Lorsqu'une page d'erreur personnalisée est renvoyée.
- Lorsque la réponse est générée à partir d'une fonction qui a été déclenchée par un événement de demande utilisateur.
- Lorsque redirige CloudFront automatiquement une requête HTTP vers HTTPS (lorsque la valeur de Viewer Protocol Policy est Rediriger HTTP vers HTTPS).

Lorsque vous ajoutez plusieurs déclencheurs au même comportement de cache, vous pouvez les utiliser pour exécuter la même fonction ou des fonctions différentes pour chaque déclencheur. Vous pouvez associer la même fonction à plusieurs distributions.

> **Note**
>
> Lorsqu'un CloudFront événement déclenche l'exécution d'une fonction Lambda, celle-ci doit se terminer avant de CloudFront pouvoir continuer. Par exemple, si une fonction Lambda est déclenchée par un événement de demande d'affichage, elle CloudFront ne renverra pas de réponse au CloudFront visualiseur ni ne transmettra la demande à l'origine tant que la fonction Lambda n'aura pas fini de s'exécuter. Cela signifie que chaque demande qui déclenche une fonction Lambda augmente sa latence. Vous souhaitez ainsi que la fonction s'exécute le plus vite possible.

Décidez quel CloudFront événement utiliser pour déclencher une fonction Lambda @Edge

Lorsque vous décidez quel CloudFront événement vous souhaitez utiliser pour déclencher une fonction Lambda, tenez compte des points suivants :

Voulez-vous CloudFront mettre en cache des objets modifiés par une fonction Lambda ?

Si vous souhaitez CloudFront mettre en cache un objet qui a été modifié par une fonction Lambda afin de CloudFront pouvoir le servir depuis l'emplacement périphérique lors de sa prochaine demande, utilisez l'événement de demande d'origine ou de réponse d'origine. Cela réduit la charge sur l'origine, réduit la latence pour les demandes suivantes et réduit le coût de l'appel de Lambda@Edge sur les demandes suivantes.

Par exemple, si vous souhaitez ajouter, supprimer ou modifier les en-têtes des objets renvoyés par l'origine et que vous souhaitez CloudFront mettre le résultat en cache, utilisez l'événement de réponse d'origine.

Voulez-vous que la fonction s'exécute pour chaque demande ?

Si vous souhaitez que la fonction s'exécute pour chaque demande CloudFront reçue pour la distribution, utilisez les événements de demande ou de réponse de l'utilisateur. Les événements de demande d'origine et de réponse d'origine se produisent uniquement lorsqu'un objet demandé n'est pas mis en cache dans un emplacement périphérique et CloudFront transmet une demande à l'origine.

La fonction modifie-t-elle la clé de cache ?

Si vous voulez que la fonction modifie une valeur que vous utilisez comme base pour la mise en cache, utilisez l'événement de demande utilisateur. Par exemple, si une fonction modifie l'URL pour inclure une abréviation de langue dans le chemin d'accès (par exemple, parce que l'utilisateur a choisi sa langue dans une liste déroulante), utilisez l'événement de demande utilisateur :

- URL dans la demande utilisateur – https://example.com/en/index.html
- URL lorsque la demande provient d'une adresse IP en Allemagne — https://example.com/de/index.html

Vous utilisez également l'événement de demande utilisateur si vous mettez en cache en fonction des cookies ou des en-têtes de demande.

> **Note**
>
> Si la fonction modifie les cookies ou les en-têtes, configurez CloudFront pour transmettre la partie applicable de la demande à l'origine. Pour plus d'informations, consultez les rubriques suivantes :
>
> - Contenu du cache basé sur les cookies
> - Contenu du cache basé sur les en-têtes des demandes

La fonction affecte-t-elle la réponse provenant de l'origine ?

Si vous voulez que la fonction modifie la demande d'une manière qui affecte la réponse provenant de l'origine, utilisez l'événement de demande à l'origine. Généralement, la plupart des événements de demande du spectateur ne sont pas transmis à l'origine ; ils CloudFront répondent à une demande avec un objet déjà présent dans le cache périphérique. Si la fonction modifie la demande en fonction d'un événement de demande d'origine, met en CloudFront cache la réponse à la demande d'origine modifiée.

Ajouter des déclencheurs à une fonction Lambda @Edge

Vous pouvez utiliser la AWS Lambda console ou la CloudFront console Amazon pour ajouter un déclencheur à votre fonction Lambda @Edge.

> **Important**
>
> Vous ne pouvez créer des déclencheurs que pour les versions numérotées de votre fonction (et non pour le $LATEST).

Lambda console

Pour ajouter des déclencheurs à une fonction Lambda @Edge

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).

3. Sur la page Fonctions, choisissez le nom de la fonction pour laquelle vous souhaitez ajouter des déclencheurs.
4. Sur la page d'aperçu des fonctions, choisissez l'onglet Versions.
5. Choisissez la version à laquelle vous souhaitez ajouter des déclencheurs.

   Une fois que vous avez choisi une version, le texte du bouton est remplacé par Version: $LATEST ou Version: numéro de version.
6. Choisissez l'onglet Triggers (Déclencheurs).
7. Choisissez Add trigger (Ajouter déclencheur).
8. Pour la configuration du déclencheur, choisissez Sélectionner une source**`cloudfront`**, entrez, puis choisissez CloudFront.

   > **Note**
   >
   > Si vous avez déjà créé un ou plusieurs déclencheurs, CloudFront c'est le service par défaut.

9. Spécifiez les valeurs suivantes pour indiquer le moment où vous voulez que la fonction Lambda s'exécute.

   a. Distribution : choisissez la distribution à laquelle vous souhaitez ajouter le déclencheur.

   b. Comportement du cache : choisissez le comportement du cache qui spécifie les objets sur lesquels vous souhaitez exécuter la fonction.

      > **Note**
      >
      > Si vous spécifiez * pour le comportement de cache, la fonction Lambda se déploie sur le comportement de cache par défaut.

   c. CloudFront event — Choisissez l'CloudFront événement à l'origine de l'exécution de la fonction.

   d. Inclure le corps : cochez cette case si vous souhaitez accéder au corps de la demande dans votre fonction.

   e. Confirmez le déploiement sur Lambda @Edge : cochez cette case pour AWS Lambda répliquer la fonction de manière globale. Régions AWS
10. Choisissez Ajouter.

La fonction commence à traiter les demandes relatives aux CloudFront événements spécifiés lorsque la CloudFront distribution mise à jour est déployée. Pour déterminer si une distribution a été déployée, choisissez Distributions dans le panneau de navigation. Lorsqu'une distribution est déployée, la valeur de la colonne État de la distribution passe de Déploiement à la date et à l'heure du déploiement.

CloudFront console

Pour ajouter des déclencheurs d' CloudFront événements à une fonction Lambda

1. Obtenez le nom ARN de la fonction Lambda pour laquelle vous voulez ajouter des déclencheurs :

   a. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

   b. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).

   c. Dans la liste des fonctions, choisissez le nom de la fonction à laquelle vous voulez ajouter des déclencheurs.

   d. Sur la page d'aperçu des fonctions, cliquez sur l'onglet Versions, puis choisissez la version numérotée à laquelle vous souhaitez ajouter des déclencheurs.

   e. Cliquez sur le bouton Copier l'ARN pour copier l'ARN dans votre presse-papiers. L'ARN de la fonction Lambda ressemble à ceci :

      ```
      arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2
      ```

      Le numéro à la fin (2 dans cet exemple) est le numéro de version de la fonction.

2. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
3. Dans la liste des distributions, choisissez l'ID de la distribution à laquelle vous voulez ajouter des déclencheurs.
4. Choisissez l'onglet Comportements.
5. Sélectionnez le comportement du cache auquel vous souhaitez ajouter des déclencheurs, puis choisissez Modifier.

6. Pour les associations de fonctions, dans la liste des types de fonctions, choisissez Lambda @Edge lorsque vous souhaitez que la fonction s'exécute : pour les demandes du lecteur, les réponses du lecteur, les demandes d'origine ou les réponses d'origine.

   Pour plus d'informations, consultez Décidez quel CloudFront événement utiliser pour déclencher une fonction Lambda @Edge.
7. Dans la zone de texte Function ARN/Name, collez l'ARN de la fonction Lambda que vous souhaitez exécuter lorsque l'événement choisi se produit. Il s'agit de la valeur que vous avez copiée depuis la console Lambda.
8. Sélectionnez Inclure le corps si vous souhaitez accéder au corps de la demande dans votre fonction.

   Si vous souhaitez simplement remplacer le corps de la demande, vous n'avez pas besoin de sélectionner cette option.
9. Pour exécuter la même fonction pour d'autres types d'événements, répétez les étapes 6 et 7.
10. Sélectionnez Enregistrer les modifications.
11. Pour ajouter des déclencheurs à d'autres comportements de cache pour cette distribution, répétez les étapes 5 à 10.

    La fonction commence à traiter les demandes relatives aux CloudFront événements spécifiés lorsque la CloudFront distribution mise à jour est déployée. Pour déterminer si une distribution a été déployée, choisissez Distributions dans le panneau de navigation. Lorsqu'une distribution est déployée, la valeur de la colonne État de la distribution passe de Déploiement à l'heure et à la date du déploiement.

Tester et déboguer les fonctions Lambda @Edge

Cette rubrique inclut des rubriques qui décrivent les stratégies de test et de débogage des fonctions Lambda@Edge. Il est important de tester votre code de fonction Lambda @Edge de manière autonome, pour vous assurer qu'il exécute la tâche prévue, et de réaliser des tests d'intégration pour vous assurer que la fonction fonctionne correctement avec. CloudFront

Pendant les tests d'intégration ou après le déploiement de votre fonction, vous devrez peut-être déboguer CloudFront des erreurs, telles que des erreurs HTTP 5xx. Les erreurs peuvent être de différents types : une réponse non valide renvoyée par la fonction Lambda, des erreurs d'exécution lorsque la fonction est déclenchée, ou encore des erreurs en raison de la limitation d'exécution par

le service Lambda. Les sections de cette rubrique donnent des stratégies pour déterminer le type de défaillance qui est à l'origine du problème, puis les étapes à suivre afin de résoudre le problème.

> **Note**
>
> Lorsque vous consultez des fichiers CloudWatch journaux ou des indicateurs pour résoudre des erreurs, sachez qu'ils sont affichés ou stockés à l'emplacement le Région AWS plus proche de l'endroit où la fonction s'est exécutée. Ainsi, si vous avez un site Web ou une application Web dont les utilisateurs se trouvent au Royaume-Uni et qu'une fonction Lambda est associée à votre distribution, par exemple, vous devez modifier la région pour afficher les CloudWatch métriques ou les fichiers journaux de Londres. Région AWS Pour plus d'informations, consultez the section called “ Déterminer la région Lambda @Edge”.

Rubriques

Testez vos fonctions Lambda @Edge

Il existe deux étapes pour tester votre fonction Lambda : le test autonome et le test d'intégration.

Test de la fonctionnalité autonome

Avant d'ajouter votre fonction Lambda à CloudFront, assurez-vous de la tester d'abord en utilisant les fonctionnalités de test de la console Lambda ou en utilisant d'autres méthodes. Pour plus d'informations sur les tests dans la console Lambda, consultez la section Appel de la fonction Lambda et vérification des résultats, des journaux et des métriques de Créer une fonction Lambda avec la console dans le Guide du développeur AWS Lambda .

Testez le fonctionnement de votre fonction dans CloudFront

Il est important de réaliser des tests d'intégration, dans lesquels votre fonction est associée à une distribution et s'exécute en fonction d'un CloudFront événement. Assurez-vous que la fonction est déclenchée pour le bon événement et renvoie une réponse valide et correcte pour CloudFront. Par exemple, assurez-vous que la structure de l'événement est correcte, que seuls les en-têtes valides sont inclus, etc.

Au fur et à mesure que vous testez l'intégration de votre fonction dans la console Lambda, reportez-vous aux étapes du didacticiel Lambda @Edge pour modifier votre code ou CloudFront le déclencheur qui appelle votre fonction. Par exemple, vérifiez que vous travaillez avec une version numérotée de votre fonction, comme le décrit cette étape du tutoriel : Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction.

Lorsque vous apportez des modifications et que vous les déployez, sachez qu'il faudra plusieurs minutes pour que votre fonction et vos CloudFront déclencheurs mis à jour soient répliqués dans toutes les régions. Cela prend généralement quelques minutes, mais peut durer jusqu'à 15 minutes.

Vous pouvez vérifier si la réplication est terminée en accédant à la CloudFront console et en consultant votre distribution.

Pour vérifier si le déploiement de votre réplication est terminé

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez le nom de la distribution.
3. Vérifiez que le statut de distribution passe de En cours à Déployé, ce qui signifie que votre fonction a été répliquée. Suivez les étapes de la section suivante afin de vérifier que la fonction s'exécute correctement.

Sachez que les tests effectués dans la console valident uniquement la logique de votre fonction et n'appliquent pas de quotas (auparavant appelés limites) de service spécifiques à Lambda@Edge.

Identifiez les erreurs de fonction Lambda @Edge dans CloudFront

Une fois que vous avez vérifié que la logique de votre fonction fonctionne correctement, des erreurs HTTP 5xx peuvent encore s'afficher lors de l'exécution de votre fonction. CloudFront Les erreurs

HTTP 5xx peuvent être renvoyées pour diverses raisons, notamment des erreurs liées à la fonction Lambda ou d'autres problèmes. CloudFront

- Si vous utilisez les fonctions Lambda @Edge, vous pouvez utiliser les graphiques de la CloudFront console pour identifier la cause de l'erreur, puis essayer de la corriger. Par exemple, vous pouvez voir si les erreurs HTTP 5xx sont causées par CloudFront ou par des fonctions Lambda, puis, pour des fonctions spécifiques, vous pouvez consulter les fichiers journaux associés afin d'étudier le problème.
- Pour résoudre les erreurs HTTP en général dans CloudFront, consultez les étapes de résolution des problèmes décrites dans la rubrique suivante :Résolution des réponses d’erreur de votre origine.

Quelles sont les causes des erreurs de fonction Lambda @Edge dans CloudFront

Il existe plusieurs raisons pour lesquelles une fonction Lambda peut entraîner une erreur HTTP 5xx. Les étapes de résolution à suivre dépendent du type d'erreur. Les erreurs peuvent être classées comme suit :

Une erreur d'exécution de la fonction Lambda

> Une erreur d'exécution se produit lorsque Lambda CloudFront ne reçoit pas de réponse en raison d'exceptions non gérées dans la fonction ou d'une erreur dans le code. Par exemple, si le code comprend le rappel (Error). Pour plus d'informations, consultez la section Erreurs de fonction Lambda dans le manuel du AWS Lambda développeur.

Une réponse de fonction Lambda non valide est renvoyée à CloudFront

> Une fois la fonction exécutée, CloudFront reçoit une réponse de Lambda. Une erreur est renvoyée si la structure d'objet de la réponse n'est pas conforme à Structure d'événement Lambda@Edge ou si la réponse contient des en-têtes ou d'autres champs non valides.

L'exécution dans CloudFront est limitée en raison des quotas de service Lambda (anciennement appelés limites)

> Le service Lambda limite les exécutions dans chaque région, et renvoie une erreur si vous dépassez le quota.

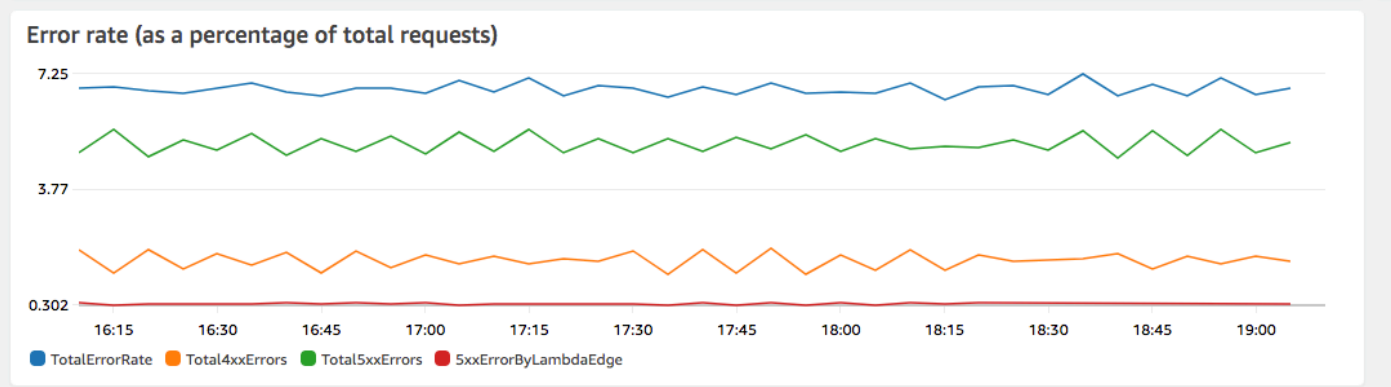
Comment déterminer le type d'échec

Pour vous aider à déterminer sur quoi vous concentrer lorsque vous débugez et que vous vous efforcez de résoudre les erreurs renvoyées CloudFront, il est utile de déterminer pourquoi une erreur HTTP CloudFront est renvoyée. Pour commencer, vous pouvez utiliser les graphiques fournis dans la section Surveillance de la CloudFront console sur le AWS Management Console. Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezSurveillance CloudFront des métriques avec Amazon CloudWatch.

Les graphiques suivants peuvent être particulièrement utiles lorsque vous souhaitez retracer si des erreurs sont renvoyées par les origines ou par une fonction Lambda, et pour réduire le type de problème lorsqu'il s'agit d'une erreur provenant d'une fonction Lambda.

Graphique des taux d'erreurs

L'un des graphiques que vous pouvez afficher dans l'onglet Présentation pour chacune de vos distributions est un graphique de taux d'erreurs. Ce graphique affiche le taux d'erreurs sous forme de pourcentage du nombre total de demandes adressées à votre distribution. Ce graphique montre le taux d'erreurs total, le total des erreurs 4xx, le total des erreurs 5xx et le total des erreurs 5xx provenant des fonctions Lambda. Selon le type d'erreur et le volume, vous pouvez prendre des mesures pour étudier et résoudre le problème initial.



- Si vous voyez des erreurs Lambda, vous pouvez poursuivre vos investigations en examinant les types d'erreurs spécifiques que la fonction renvoie. L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut des graphiques qui classent les erreurs de fonction par type pour vous aider à identifier le problème pour une fonction spécifique.
- Si vous CloudFront constatez des erreurs, vous pouvez les résoudre et vous efforcer de corriger les erreurs d'origine ou de modifier votre CloudFront configuration. Pour plus d'informations, consultez Résolution des réponses d'erreur de votre origine.

Graphiques des erreurs d'exécution et des réponses de fonction non valide

L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut des graphiques permettant de classer les erreurs Lambda@Edge pour une distribution spécifique, par type. Par exemple, un graphique montre toutes les erreurs d'exécution par Région AWS.

Pour faciliter la résolution des problèmes, vous pouvez rechercher des problèmes spécifiques en ouvrant et en examinant les fichiers journaux pour des fonctions spécifiques par région.

Pour afficher les fichiers journaux d'une fonction spécifique par région

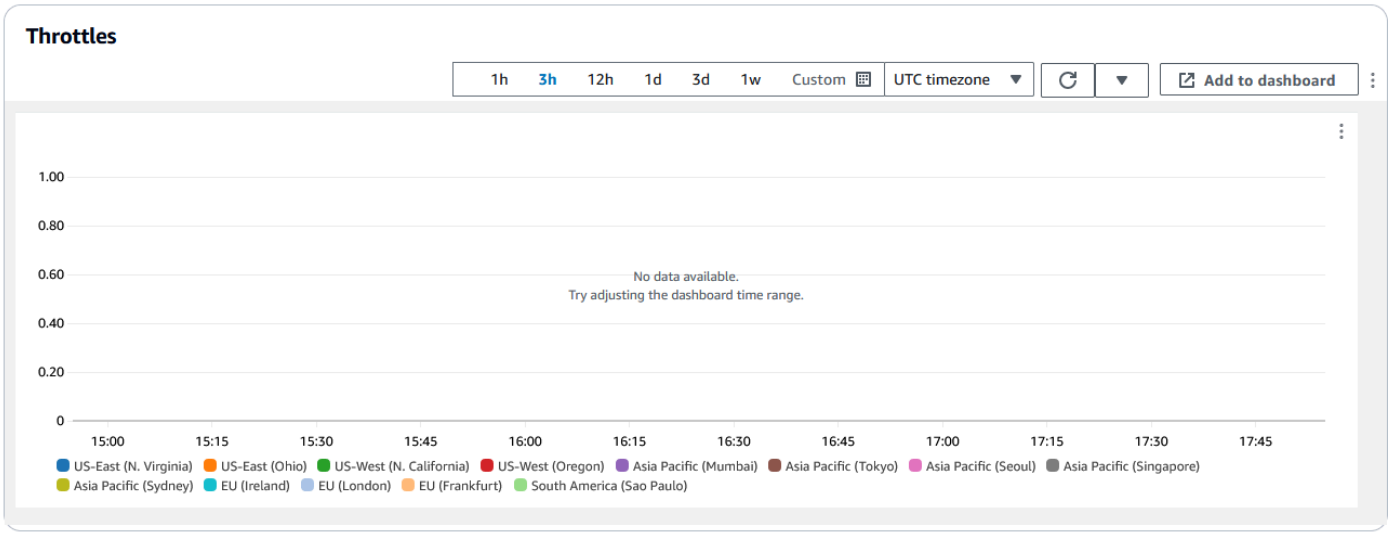
1. Dans l'onglet Erreurs Lambda @Edge, sous Fonctions Lambda @Edge associées, choisissez le nom de la fonction, puis choisissez Afficher les métriques.
2. Ensuite, sur la page portant le nom de votre fonction, dans le coin supérieur droit, choisissez Afficher les journaux des fonctions, puis choisissez une région.

   Par exemple, si vous voyez des problèmes dans le graphique des erreurs pour la région USA Ouest (Oregon), sélectionnez cette région dans la liste déroulante. Cela ouvre la CloudWatch console Amazon.
3. Dans la CloudWatch console de cette région, sous Log streams, choisissez un log stream pour afficher les événements liés à la fonction.

De plus, lisez les sections suivantes de ce chapitre pour plus de recommandations sur le dépannage et la correction des erreurs.

Graphique des limitations

L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut également un graphique Throttles (Limitations). Occasionnellement, le service Lambda limite vos appels de fonction par région si vous atteignez le quota (auparavant appelé limite) de simultanéité régionale. Si vous voyez une erreur de dépassement de limite, cela signifie que votre fonction a atteint un quota que le service Lambda impose sur les exécutions dans une région. Pour obtenir plus d'informations sur ces limites et découvrir comment demander une augmentation du quota, veuillez consulter Quotas sur Lambda@Edge.



Pour obtenir un exemple sur la façon d'utiliser ces informations pour résoudre des erreurs HTTP, consultez le billet de blog Four steps for debugging your content delivery on AWS.

Résoudre les problèmes liés aux réponses non valides à la fonction Lambda @Edge (erreurs de validation)

Si vous identifiez que votre problème est dû à une erreur de validation Lambda, cela signifie que votre fonction Lambda renvoie une réponse non valide à. CloudFront Suivez les instructions de cette section pour prendre les mesures nécessaires pour revoir votre fonction et vous assurer que votre réponse est conforme aux CloudFront exigences.

CloudFront valide la réponse d'une fonction Lambda de deux manières :

- La réponse Lambda doit se conformer à la structure d'objet requise. Voici des exemples de mauvaise structure d'objet : impossible d'analyser JSON, champs obligatoires manquants et la réponse contient un objet non valide. Pour plus d'informations, consultez le Structure d'événement Lambda@Edge.
- La réponse doit inclure uniquement les valeurs d'objet valides. Une erreur se produit si la réponse inclut un objet valide mais dont les valeurs ne sont pas prises en charge. Les exemples incluent les éléments suivants : ajout ou mise à jour d'en-têtes non autorisés ou en lecture seule (voir Restrictions sur les fonctions périphériques), dépassement des limitations de taille du corps (voir Limites sur la taille de la réponse générée dans la rubrique Lambda@Edge Erreurs) et les caractères ou les valeurs non valables (voir Structure d'événement Lambda@Edge).

Lorsque Lambda renvoie une réponse non valide à CloudFront, des messages d'erreur sont écrits CloudWatch dans des fichiers journaux qui sont CloudFront redirigés vers la région où la fonction Lambda a été exécutée. C'est le comportement par défaut auquel envoyer les fichiers journaux en CloudWatch cas de réponse non valide. Toutefois, si vous avez associé une fonction Lambda à une fonction Lambda CloudFront avant son lancement, il est possible qu'elle ne soit pas activée pour votre fonction. Pour plus d'informations, consultez la section Déterminer si votre compte transmet les journaux CloudWatch plus loin dans cette rubrique.

CloudFront envoie les fichiers journaux vers la région correspondant à l'endroit où votre fonction a été exécutée, dans le groupe de journaux associé à votre distribution. Les groupes de journaux ont le format suivant :`/aws/cloudfront/LambdaEdge/`*`DistributionId`*, où *`DistributionId`*est l'ID de votre distribution. Pour déterminer la région dans laquelle se trouvent les fichiers CloudWatch journaux, consultez la section Détermination de la région Lambda @Edge plus loin dans cette rubrique.

Si l'erreur est reproductible, vous pouvez créer une nouvelle demande qui entraîne l'erreur, puis rechercher l'identifiant de la demande dans une CloudFront réponse ayant échoué (`X-Amz-Cf-Id`en-tête) afin de localiser un seul échec dans les fichiers journaux. L'entrée du fichier journal inclut des informations susceptibles de vous aider à identifier les raisons pour lesquelles l'erreur est renvoyée, et affiche aussi l'ID de demande Lambda correspondant, ce qui vous permet d'analyser la cause première dans le cadre d'une seule demande.

Si une erreur est intermittente, vous pouvez utiliser les journaux d' CloudFront accès pour trouver l'identifiant d'une demande qui a échoué, puis rechercher dans CloudWatch les journaux les messages d'erreur correspondants. Pour plus d'informations, consultez la section précédente, Détermination du type d'échec.

Résoudre les erreurs d'exécution de la fonction Lambda @Edge

Si le problème provient d'une erreur d'exécution Lambda, il peut être utile de créer des instructions de journalisation pour les fonctions Lambda, d'écrire des messages dans des fichiers CloudWatch journaux qui surveillent l'exécution de votre fonction CloudFront et déterminent si elle fonctionne comme prévu. Vous pouvez ensuite rechercher ces instructions dans les fichiers CloudWatch journaux pour vérifier que votre fonction fonctionne.

> **Note**
>
> Même si vous n'avez pas modifié votre fonction Lambda@Edge, les mises à jour de l'environnement d'exécution de la fonction Lambda peuvent l'affecter et renvoyer une erreur

d'exécution. Pour plus d'informations sur les tests et la migration vers une version ultérieure, consultez Prochaines mises à jour de l'environnement d'exécution AWS Lambda et AWS Lambda @Edge.

Déterminer la région Lambda @Edge

Pour connaître les régions dans lesquelles votre fonction Lambda @Edge reçoit du trafic, consultez les métriques de la fonction sur la CloudFront console du. AWS Management Console Les statistiques sont affichées pour chaque AWS région. Sur la même page, vous pouvez choisir une région et afficher les fichiers journaux pour cette région afin de pouvoir rechercher des problèmes. Vous devez consulter les fichiers CloudWatch journaux dans la AWS région appropriée pour voir les fichiers journaux créés lors de l' CloudFront exécution de votre fonction Lambda.

Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezSurveillance CloudFront des métriques avec Amazon CloudWatch.

Déterminez si votre compte envoie les journaux vers CloudWatch

Par défaut, CloudFront active la journalisation des réponses de fonction Lambda non valides et envoie les fichiers journaux vers CloudWatch . Rôles liés à un service pour Lambda@Edge Si vous avez ajouté des fonctions Lambda @Edge CloudFront avant la publication de la fonctionnalité de journal des réponses des fonctions Lambda non valide, la journalisation est activée lors de la prochaine mise à jour de votre configuration Lambda @Edge, par exemple en ajoutant un déclencheur. CloudFront

Vous pouvez vérifier que le transfert des fichiers journaux vers CloudWatch est activé pour votre compte en procédant comme suit :

- Vérifiez si les journaux apparaissent dans CloudWatch. Assurez-vous de vérifier les fichiers journaux dans la région où la fonction Lambda@Edge est exécutée. Pour plus d'informations, consultez Déterminer la région Lambda @Edge.
- Définissez si le rôle lié à un service existe dans votre compte dans IAM. Pour ce faire, ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/, puis choisissez Roles (Rôles) pour afficher la liste des rôles liés à un service de votre compte. Recherchez le rôle suivant : `AWSServiceRoleForCloudFrontLogger`.

Supprimer les fonctions et les répliques Lambda @Edge

Vous ne pouvez supprimer une fonction Lambda @Edge que lorsque les répliques de la fonction ont été supprimées par. CloudFront Les réplicas d'une fonction Lambda sont automatiquement supprimés dans les cas suivants :

- Après avoir supprimé la dernière association pour la fonction dans toutes vos CloudFront distributions. Si plusieurs distributions utilisent une fonction, les réplicas ne sont supprimés qu'après avoir supprimé l'association de fonctions de la dernière distribution.
- Après avoir supprimé la dernière distribution à laquelle une fonction était associée.

Ils sont généralement supprimés en quelques heures. Vous ne pouvez pas supprimer manuellement des réplicas de fonction Lambda @Edge. Cela permet d'éviter la suppression d'un réplica en cours d'utilisation, ce qui entraînerait une erreur.

> **Warning**
>
> Ne créez pas d'applications qui utilisent des répliques de fonctions Lambda @Edge en dehors de. CloudFront Ces réplicas sont supprimés lorsque leurs associations avec des distributions sont supprimées, ou lorsque les distributions elles-mêmes sont supprimées. Le réplica dont dépend une application externe pourrait être supprimé sans avertissement, ce qui entraînerait un échec.

Pour supprimer une association de fonctions Lambda @Edge d'une CloudFront distribution (console)

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution avec l'association de fonctions Lambda @Edge que vous souhaitez supprimer.
3. Choisissez l’onglet Comportements.
4. Sélectionnez le comportement de cache associé à la fonction Lambda @Edge que vous souhaitez supprimer, puis choisissez Modifier.
5. Sous Associations de fonctions, Type de fonction, choisissez Aucune association pour supprimer l'association de fonctions Lambda @Edge.
6. Sélectionnez Enregistrer les modifications.

Après avoir supprimé une association de fonctions Lambda @Edge d'une CloudFront distribution, vous pouvez éventuellement supprimer la fonction Lambda ou sa version de. AWS Lambda Attendez quelques heures après avoir supprimé l'association de fonctions afin que les répliques de fonctions Lambda @Edge puissent être nettoyées. Ensuite, vous pourrez supprimer la fonction à l'aide de la console Lambda, de l'API AWS CLI Lambda ou d'un SDK. AWS

Vous pouvez également supprimer une version spécifique d'une fonction Lambda si aucune CloudFront distribution n'est associée à cette version. Après avoir supprimé toutes les associations pour une version de fonction Lambda, attendez quelques heures. Vous pourrez ensuite supprimer la version de la fonction.

Structure d'événement Lambda@Edge

Les rubriques suivantes décrivent les objets d'événements de demande et de réponse CloudFront transmis à une fonction Lambda @Edge lorsqu'elle est déclenchée.

Rubriques

Sélection de l'origine dynamique

Vous pouvez utiliser le modèle de chemin dans un comportement de cache pour router les demandes vers une origine, en fonction du chemin et du nom de l'objet demandé, tels que `images/*.jpg`. En utilisant Lambda@Edge, vous pouvez également acheminer des demandes vers une origine en fonction d'autres caractéristiques, comme les valeurs contenues dans les en-têtes de la demande.

Cette sélection d'origine dynamique peut être utile de diverses façons. Par exemple, vous pouvez répartir les demandes entre des origines de différentes zones géographiques pour vous aider à réaliser un équilibrage de charge international. Ou vous pouvez acheminer de façon sélective des demandes vers différentes origines servant chacune une fonction donnée : gestion du robot, optimisation de la stratégie SEO, authentification, etc. Pour obtenir des exemples de code qui expliquent comment utiliser cette fonction, veuillez consulter Sélection d'origine dynamique basée sur le contenu – exemples.

Dans l'événement de demande CloudFront d'origine, l'`origin`objet de la structure d'événement contient des informations sur l'origine vers laquelle la demande serait acheminée, en fonction

du modèle de chemin. Vous pouvez mettre à jour les valeurs de l'objet `origin` pour router une demande vers une autre origine. Quand vous mettez à jour l'objet `origin`, vous n'avez pas besoin de définir l'origine dans la distribution. Vous pouvez également remplacer un objet d'origine Amazon S3 par un objet d'origine personnalisée, et vice versa. Toutefois, vous ne pouvez spécifier qu'une seule origine par demande ; une origine personnalisée ou une origine Amazon S3, mais pas les deux.

Événements de demande

Les rubriques suivantes présentent la structure de l'objet qui est transmis à CloudFront une fonction Lambda pour les événements de demande d'affichage et d'origine. Ces exemples montrent une demande `GET` sans corps. Après les exemples, vous trouverez la liste de tous les champs possibles dans les événements de demande d'utilisateur et d'origine.

Rubriques

- Exemple de demande d'utilisateur
- Exemple de demande de l'origine
- Champs d'événement de demande

Exemple de demande d'utilisateur

L'exemple suivant montre un objet d'événement de demande d'utilisateur.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "viewer-request",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "host": [
              {
                "key": "Host",
                "value": "d111111abcdef8.cloudfront.net"
```

```
            }
          ],
          "user-agent": [
            {
              "key": "User-Agent",
              "value": "curl/7.66.0"
            }
          ],
          "accept": [
            {
              "key": "accept",
              "value": "*/*"
            }
          ]
        },
        "method": "GET",
        "querystring": "",
        "uri": "/"
      }
    }
  ]
}
```

Exemple de demande de l'origine

L'exemple suivant montre un objet d'événement de demande d'origine.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-request",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
```

```
              "value": "203.0.113.178"
            }
          ],
          "user-agent": [
            {
              "key": "User-Agent",
              "value": "Amazon CloudFront"
            }
          ],
          "via": [
            {
              "key": "Via",
              "value": "2.0 2afae0d44e2540f472c0635ab62c232b.cloudfront.net
(CloudFront)"
            }
          ],
          "host": [
            {
              "key": "Host",
              "value": "example.org"
            }
          ],
          "cache-control": [
            {
              "key": "Cache-Control",
              "value": "no-cache"
            }
          ]
        },
        "method": "GET",
        "origin": {
          "custom": {
            "customHeaders": {},
            "domainName": "example.org",
            "keepaliveTimeout": 5,
            "path": "",
            "port": 443,
            "protocol": "https",
            "readTimeout": 30,
            "sslProtocols": [
              "TLSv1",
              "TLSv1.1",
              "TLSv1.2"
            ]
```

```
            }
          },
          "querystring": "",
          "uri": "/"
        }
      }
    }
  ]
}
```

Champs d'événement de demande

Les données d'objet d'événement de demande sont contenues dans deux sous-objets : `config` (`Records.cf.config`) et `request` (`Records.cf.request`). Les listes suivantes décrivent les champs de chaque sous-objet.

Champs de l’objet config

La liste suivante décrit les champs figurant dans l’objet `config` (`Records.cf.config`).

`distributionDomainName` (lecture seule)

Nom de domaine de la distribution qui est associée à la demande.

`distributionID` (lecture seule)

ID de la distribution qui est associée à la demande.

`eventType` (lecture seule)

Type de déclencheur associé à la demande : `viewer-request` ou `origin-request`.

`requestId` (lecture seule)

Chaîne cryptée qui identifie de manière unique le visiteur à la demande. CloudFront La `requestId` valeur apparaît également dans les journaux CloudFront d'accès sous la forme`x-edge-request-id`. Pour plus d’informations, consultez Configuration et utilisation des journaux standard (journaux d’accès) et Champs d’un fichier journal standard.

Champs de l'objet de demande

La liste suivante décrit les champs figurant dans l’objet `request` (`Records.cf.request`).

`clientIp` (lecture seule)

Adresse IP de l'utilisateur qui a émis la requête. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur correspond à l'adresse IP du proxy ou de l'équilibreur de charge.

en-têtes (lecture/écriture)

En-têtes de la requête. Remarques :

- Les clés figurant dans l'objet `headers` sont les versions en minuscules des noms d'en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.
- Chaque objet d'en-tête (par exemple, `headers["accept"]` ou `headers["host"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur dans la demande.
- `key` contient le nom sensible à la casse de l'en-tête tel qu'il apparaissait dans la requête HTTP ; par exemple, `Host`, `User-Agent`, `X-Forwarded-For`, etc.
- `value` contient la valeur d'en-tête telle qu'elle apparaissait dans la requête HTTP.
- Lorsque votre fonction Lambda ajoute ou modifie des en-têtes de demande et que vous n'incluez pas le champ `key` d'en-tête, Lambda@Edge insère automatiquement une clé (`key`) d'en-tête en utilisant le nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée automatiquement est formatée avec une majuscule initiale pour chaque partie, séparée par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme le suivant, sans clé (`key`) d'en-tête :

  ```
  "user-agent": [
    {
      "value": "ExampleCustomUserAgent/1.X.0"
    }
  ]
  ```

  Dans cet exemple, Lambda@Edge insère automatiquement `"key": "User-Agent"`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`method` (lecture seule)

Méthode HTTP de la demande.

`querystring` (lecture/écriture)

Chaîne de requête, le cas échéant, dans la demande. Si la demande n'inclut pas de chaîne de requête, l'objet d'événement inclut quand-même `querystring` avec une valeur vide. Pour plus d'informations sur les chaînes de requête, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

`uri` (lecture/écriture)

Chemin d'accès relatif de l'objet demandé. Si votre fonction Lambda modifie la valeur `uri`, notez ce qui suit :

- La nouvelle valeur `uri` doit commencer par une barre oblique (/).
- Lorsqu'une fonction modifie la valeur `uri`, cela change l'objet que l'utilisateur demande.
- Lorsqu'une fonction modifie la valeur `uri`, cela ne modifie pas le comportement de cache pour la demande ou l'origine vers laquelle la demande est envoyée.

`body` (lecture/écriture)

Corps de la requête HTTP. La structure `body` peut contenir les champs suivants :

`inputTruncated` (lecture seule)

Indicateur booléen qui indique si le corps a été tronqué par Lambda@Edge. Pour plus d'informations, consultez Restrictions relatives au corps de la requête avec l'option Inclure le corps.

`action` (lecture/écriture)

L'action que vous avez l'intention de prendre avec le corps. Les options pour l'`action`sont les suivantes :

- `read-only:` Il s'agit de l'option par défaut. Au moment de renvoyer la réponse à partir de la fonction Lambda, si `action` est en lecture seule, Lambda@Edge ignore les modifications apportée à `encoding` ou à `data`.
- `replace:` À préciser lorsque vous souhaitez remplacer le corps envoyé à l'origine.

`encoding` (lecture/écriture)

L'encodage pour le corps. Lorsque Lambda@Edge expose le corps à la fonction Lambda, il convertit d'abord le corps en base64-encoding. Si vous choisissez `replace` comme `action` pour remplacer le corps, vous pouvez choisir d'utiliser l'encodage `base64` (option par défaut) ou `text`. Si vous spécifiez `encoding` comme `base64` mais que le corps n'est pas validebase64, CloudFront renvoie une erreur.

`data` (lecture/écriture)

Le contenu du corps de requête.

`origin` (lecture/écriture) (événements d'origine uniquement)

Origine vers laquelle envoyer la demande. La structure `origin` doit contenir une et une seule origine, qui peut être une origine personnalisée ou une origine Amazon S3. La structure d'origine peut contenir les champs suivants :

`customHeaders` (lecture/écriture) (origines personnalisées et Amazon S3)

Vous pouvez inclure des en-têtes personnalisés dans la requête en spécifiant un nom et une valeur d'en-tête pour chacun d'eux. Vous ne pouvez pas ajouter des en-têtes non autorisés et un en-tête portant le même nom ne peut pas être présent dans `Records.cf.request.headers`. Les notes sur les en-têtes de demande s'appliquent également aux en-têtes personnalisés. Pour plus d'informations, consultez En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine et Restrictions sur les fonctions périphériques.

`domainName` (lecture/écriture) (origines personnalisées et Amazon S3)

Nom de domaine de l'origine. Le nom de domaine ne peut pas être vide.

- Pour les origines personnalisées – Spécifiez un nom de domaine DNS, tel que `www.example.com`. Le nom de domaine ne peut pas inclure un signe deux-points (:) et ne peut pas être une adresse IP. Le nom du domaine peut contenir jusqu'à 253 caractères.
- Pour les origines Amazon S3 – Spécifiez le nom de domaine DNS du compartiment Amazon S3, tel que `awsexamplebucket.s3.eu-west-1.amazonaws.com`. Il peut comporter jusqu'à 128 caractères, qui doivent tous être en minuscules.

`path` (lecture/écriture) (origines personnalisées et Amazon S3)

Chemin de répertoire à l'origine où la demande doit localiser le contenu. Ce chemin doit commencer par une barre oblique (/) mais ne doit pas se terminer par une barre oblique (par exemple, il ne doit pas se terminer par `example-path/`). Pour les origines personnalisées uniquement, le chemin doit être codé par URL et avoir une longueur maximale de 255 caractères.

`keepaliveTimeout` (lecture/écriture) (origines personnalisées uniquement)

Combien de temps, en secondes, cela CloudFront devrait essayer de maintenir la connexion à l'origine après avoir reçu le dernier paquet de réponse. La valeur doit être un nombre compris entre 1 et 60, bornes incluses.

`port` (lecture/écriture) (origines personnalisées uniquement)

Le port auquel vous CloudFront devez vous connecter à votre point d'origine personnalisé. Il doit s'agir du port 80, du port 443 ou d'un port compris entre 1 024 et 65 535.

`protocol` (lecture/écriture) (origines personnalisées uniquement)

Le protocole de connexion à utiliser CloudFront lors de la connexion à votre point d'origine. La valeur peut être `http` ou `https`.

`readTimeout` (lecture/écriture) (origines personnalisées uniquement)

Combien de temps, en secondes, CloudFront doit attendre une réponse après avoir envoyé une demande à votre origine. Cela indique également le temps CloudFront d'attente après réception d'un paquet de réponse avant de recevoir le paquet suivant. La valeur doit être un nombre compris entre 4 et 60, bornes incluses.

Si votre cas d'utilisation prend plus de 60 secondes, vous pouvez demander un quota plus élevé pour`Response timeout per origin`. Pour plus d'informations, consultez Quotas généraux sur les distributions.

`sslProtocols` (lecture/écriture) (origines personnalisées uniquement)

Protocole SSL/TLS minimal CloudFront pouvant être utilisé lors de l'établissement d'une connexion HTTPS avec votre origine. Il peut s'agir des valeurs suivantes : `TLSv1.2`, `TLSv1.1`, `TLSv1` ou `SSLv3`.

`authMethod` (lecture/écriture) (origines Amazon S3 uniquement)

Si vous utilisez une identité d'accès à l'origine (OAI), définissez ce champ sur `origin-access-identity`. Si vous n'utilisez pas d'OAI, configurez-le sur `none`. Si vous définissez `authMethod` sur `origin-access-identity`, il existe plusieurs exigences :

- Vous devez spécifier le paramètre `region` (voir le champ suivant).
- Vous devez utiliser la même identité d'accès à l'origine lorsque vous changez l'origine Amazon S3 de la demande.
- Vous ne pouvez pas utiliser d'identité d'accès à l'origine lorsque vous remplacez l'origine personnalisée de la demande par une origine Amazon S3.

> **Note**
>
> Ce champ ne prend pas en charge le contrôle d'accès à l'origine (OAC).

`region` (lecture/écriture) (origines Amazon S3 uniquement)

La AWS région de votre compartiment Amazon S3. Cette option n'est requise que lorsque vous définissez `authMethod` sur `origin-access-identity`.

Événements de réponse

Les rubriques suivantes présentent la structure de l'objet qui est CloudFront transmis à une fonction Lambda pour les événements de réponse du visualiseur et de l'origine. Après les exemples, vous trouverez la liste de tous les champs possibles dans les événements de réponse d'utilisateur et d'origine.

Rubriques

- Exemple de réponse de l'origine
- Exemple de réponse de l'utilisateur
- Champs d'événement de réponse

Exemple de réponse de l'origine

L'exemple suivant montre un objet d'événement de réponse de l'origine.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-response",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
                "value": "203.0.113.178"
              }
            ],
```

```
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "Amazon CloudFront"
              }
            ],
            "via": [
              {
                "key": "Via",
                "value": "2.0 8f22423015641505b8c857a37450d6c0.cloudfront.net
(CloudFront)"
              }
            ],
            "host": [
              {
                "key": "Host",
                "value": "example.org"
              }
            ],
            "cache-control": [
              {
                "key": "Cache-Control",
                "value": "no-cache"
              }
            ]
          },
          "method": "GET",
          "origin": {
            "custom": {
              "customHeaders": {},
              "domainName": "example.org",
              "keepaliveTimeout": 5,
              "path": "",
              "port": 443,
              "protocol": "https",
              "readTimeout": 30,
              "sslProtocols": [
                "TLSv1",
                "TLSv1.1",
                "TLSv1.2"
              ]
            }
          },
          "querystring": "",
```

```
          "uri": "/"
        },
        "response": {
          "headers": {
            "access-control-allow-credentials": [
              {
                "key": "Access-Control-Allow-Credentials",
                "value": "true"
              }
            ],
            "access-control-allow-origin": [
              {
                "key": "Access-Control-Allow-Origin",
                "value": "*"
              }
            ],
            "date": [
              {
                "key": "Date",
                "value": "Mon, 13 Jan 2020 20:12:38 GMT"
              }
            ],
            "referrer-policy": [
              {
                "key": "Referrer-Policy",
                "value": "no-referrer-when-downgrade"
              }
            ],
            "server": [
              {
                "key": "Server",
                "value": "ExampleCustomOriginServer"
              }
            ],
            "x-content-type-options": [
              {
                "key": "X-Content-Type-Options",
                "value": "nosniff"
              }
            ],
            "x-frame-options": [
              {
                "key": "X-Frame-Options",
                "value": "DENY"
```

```
            }
          ],
          "x-xss-protection": [
            {
              "key": "X-XSS-Protection",
              "value": "1; mode=block"
            }
          ],
          "content-type": [
            {
              "key": "Content-Type",
              "value": "text/html; charset=utf-8"
            }
          ],
          "content-length": [
            {
              "key": "Content-Length",
              "value": "9593"
            }
          ]
        },
        "status": "200",
        "statusDescription": "OK"
      }
    }
  }
 ]
}
```

Exemple de réponse de l'utilisateur

L'exemple suivant montre un objet d'événement de réponse de l'utilisateur.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "viewer-response",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
```

```
          "clientIp": "203.0.113.178",
          "headers": {
            "host": [
              {
                "key": "Host",
                "value": "d111111abcdef8.cloudfront.net"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "curl/7.66.0"
              }
            ],
            "accept": [
              {
                "key": "accept",
                "value": "*/*"
              }
            ]
          },
          "method": "GET",
          "querystring": "",
          "uri": "/"
        },
        "response": {
          "headers": {
            "access-control-allow-credentials": [
              {
                "key": "Access-Control-Allow-Credentials",
                "value": "true"
              }
            ],
            "access-control-allow-origin": [
              {
                "key": "Access-Control-Allow-Origin",
                "value": "*"
              }
            ],
            "date": [
              {
                "key": "Date",
                "value": "Mon, 13 Jan 2020 20:14:56 GMT"
              }
```

```
            ],
            "referrer-policy": [
              {
                "key": "Referrer-Policy",
                "value": "no-referrer-when-downgrade"
              }
            ],
            "server": [
              {
                "key": "Server",
                "value": "ExampleCustomOriginServer"
              }
            ],
            "x-content-type-options": [
              {
                "key": "X-Content-Type-Options",
                "value": "nosniff"
              }
            ],
            "x-frame-options": [
              {
                "key": "X-Frame-Options",
                "value": "DENY"
              }
            ],
            "x-xss-protection": [
              {
                "key": "X-XSS-Protection",
                "value": "1; mode=block"
              }
            ],
            "age": [
              {
                "key": "Age",
                "value": "2402"
              }
            ],
            "content-type": [
              {
                "key": "Content-Type",
                "value": "text/html; charset=utf-8"
              }
            ],
            "content-length": [
```

```
              {
                "key": "Content-Length",
                "value": "9593"
              }
            ]
          },
          "status": "200",
          "statusDescription": "OK"
        }
      }
    }
  ]
}
```

Champs d'événement de réponse

Les données d'objet d'événement de réponse sont contenues dans trois sous-objets : `config` (`Records.cf.config`), `request` (`Records.cf.request`) et `response` (`Records.cf.response`). Pour de plus amples informations sur les champs de l'objet de demande, veuillez consulter Champs de l'objet de demande. Les listes suivantes décrivent les champs figurant dans les sous-objets `config` et `response`.

Champs de l’objet config

La liste suivante décrit les champs figurant dans l’objet `config` (`Records.cf.config`).

`distributionDomainName` (lecture seule)

Nom de domaine de la distribution qui est associée à la réponse.

`distributionID` (lecture seule)

ID de la distribution qui est associée à la réponse.

`eventType` (lecture seule)

Type de déclencheur associé à la réponse : `origin-response` ou `viewer-response`.

`requestId` (lecture seule)

Chaîne cryptée qui identifie de manière unique le téléspectateur à qui CloudFront cette réponse est associée. La `requestId` valeur apparaît également dans les journaux CloudFront d'accès sous la forme`x-edge-request-id`. Pour plus d’informations, consultez Configuration et utilisation des journaux standard (journaux d’accès) et Champs d’un fichier journal standard.

Champs de l'objet de réponse

La liste suivante décrit les champs figurant dans l'objet `response` (`Records.cf.response`). Pour obtenir des informations sur l'utilisation d'une fonction Lambda@Edge pour générer une réponse HTTP, veuillez consulter Générer des réponses HTTP dans les déclencheurs de requêtes.

`headers` (lecture/écriture)

En-têtes de la réponse. Remarques :

- Les clés figurant dans l'objet `headers` sont les versions en minuscules des noms d'en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.
- Chaque objet d'en-tête (par exemple, `headers["content-type"]` ou `headers["content-length"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur de la réponse.
- `key`contient le nom de l'en-tête distinguant majuscules et minuscules tel qu'il apparaît dans la réponse HTTP ; par exemple `Content-Type` `Content-LengthCookie`,,, etc.
- `value` contient la valeur d'en-tête telle qu'elle apparaît dans la réponse HTTP.
- Lorsque votre fonction Lambda ajoute ou modifie des en-têtes de réponse et que vous n'incluez pas le champ `key` d'en-tête, Lambda@Edge insère automatiquement une clé (`key`) d'en-tête en utilisant le nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée automatiquement est formatée avec une majuscule initiale pour chaque partie, séparée par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme le suivant, sans clé (`key`) d'en-tête :

  ```
  "content-type": [
    {
      "value": "text/html;charset=UTF-8"
    }
  ]
  ```

  Dans cet exemple, Lambda@Edge insère automatiquement `"key": "Content-Type"`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`status`

Code de statut HTTP de la réponse.

`statusDescription`

Description de l'état HTTP de la réponse.

Travailler avec les demandes et les réponses

Les rubriques de cette section expliquent plusieurs manières d'utiliser les demandes et réponses Lambda@Edge.

Rubriques

- Utiliser les fonctions Lambda @Edge avec le basculement d'origine
- Générer des réponses HTTP dans les déclencheurs de requêtes
- Mettre à jour les réponses HTTP dans les déclencheurs de réponse d'origine
- Accédez au corps de la demande en choisissant l'option Inclure le corps

Utiliser les fonctions Lambda @Edge avec le basculement d'origine

Vous pouvez utiliser les fonctions Lambda @Edge avec des CloudFront distributions que vous avez configurées avec des groupes d'origine, par exemple, pour le basculement d'origine que vous configurez afin de garantir une haute disponibilité. Pour utiliser une fonction Lambda avec un groupe d'origine, spécifiez la fonction dans une requête d'origine ou un déclencheur de réponse de l'origine pour un groupe d'origine lorsque vous créez le comportement de cache.

Pour plus d'informations, consultez les ressources suivantes :

- Créez des groupes d'origine : Création d'un groupe d'origine
- Comment fonctionne le basculement d'origine avec Lambda@Edge: Utilisation du basculement d'origine avec les fonctions Lambda@Edge

Générer des réponses HTTP dans les déclencheurs de requêtes

Lorsque CloudFront vous recevez une demande, vous pouvez utiliser une fonction Lambda pour générer une réponse HTTP qui est CloudFront renvoyée directement au visualiseur sans transmettre

la réponse à l'origine. La génération de réponses HTTP réduit la charge sur le serveur d'origine, et aussi généralement la latence pour l'utilisateur.

Les scénarios courants pour générer des réponses HTTP sont les suivants :

- Renvoi d'une petite page web à l'utilisateur
- Renvoi d'un code de statut HTTP 301 ou 302 pour rediriger l'utilisateur vers une autre page web
- Renvoi d'un code de statut HTTP 401 lorsque l'utilisateur ne s'est pas authentifié

Une fonction Lambda @Edge peut générer une réponse HTTP lorsque les CloudFront événements suivants se produisent :

Événements de demande utilisateur

Lorsqu'une fonction est déclenchée par un événement de demande du spectateur, CloudFront renvoie la réponse au visualiseur sans la mettre en cache.

Événements de demande à l'origine

Lorsqu'une fonction est déclenchée par un événement de demande d' CloudFront origine, recherche dans le cache périphérique une réponse précédemment générée par la fonction.

- Si la réponse se trouve dans le cache, la fonction n'est pas exécutée et CloudFront renvoie la réponse mise en cache au visualiseur.
- Si la réponse ne se trouve pas dans le cache, la fonction est exécutée, CloudFront renvoie la réponse au visualiseur et la met également en cache.

Pour voir un exemple de code permettant de générer des réponses HTTP, consultez Exemples de fonctions Lambda@Edge. Vous pouvez également remplacer les réponses HTTP dans les déclencheurs de réponse. Pour plus d’informations, consultez Mettre à jour les réponses HTTP dans les déclencheurs de réponse d'origine.

Modèle de programmation

Cette section décrit le modèle de programmation permettant d'utiliser Lambda@Edge pour générer des réponses HTTP.

Rubriques

- Objet Réponse
- Erreurs

- Champs obligatoires

Objet Réponse

La réponse que vous renvoyez en tant que paramètre `result` de la méthode `callback` doit avoir la structure suivante (notez que seul le champ `status` est requis).

```
const response = {
    body: 'content',
    bodyEncoding: 'text' | 'base64',
    headers: {
        'header name in lowercase': [{
           key: 'header name in standard case',
           value: 'header value'
         }],
         ...
    },
    status: 'HTTP status code (string)',
    statusDescription: 'status description'
};
```

L'objet de réponse peut inclure les valeurs suivantes :

`body`

Le corps, le cas échéant, que vous CloudFront souhaitez renvoyer dans la réponse générée.

`bodyEncoding`

Encodage de la valeur que vous avez spécifiée dans `body`. Les seuls encodages valides sont `text` et `base64`. Si vous incluez `body` dans l'`response`objet mais que vous l'omettez`bodyEncoding`, CloudFront traite le corps comme du texte.

Si vous spécifiez `bodyEncoding` as `base64` mais que le corps n'est pas valide en base64, CloudFront renvoie une erreur.

`headers`

En-têtes que vous CloudFront souhaitez renvoyer dans la réponse générée. Notez ce qui suit :

- Les clés figurant dans l'objet `headers` sont les versions en minuscules des noms d'en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.

- Chaque en-tête (par exemple, `headers["accept"]` ou `headers["host"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur de la réponse générée.
- `key` (facultatif) est le nom de l'en-tête sensible à la casse tel qu'il s'affiche dans une demande HTTP, par exemple, `accept` ou `host`.
- Indiquez `value` comme valeur d'en-tête.
- Si vous n'incluez pas la partie clé d'en-tête de la paire clé-valeur, Lambda@Edge insère automatiquement une clé d'en-tête à l'aide du nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée est formatée automatiquement avec une majuscule initiale pour les différentes parties séparées par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme suit, sans clé d'en-tête : `'content-type': [{ value: 'text/html;charset=UTF-8' }]`

  Dans cet exemple, Lambda@Edge crée la clé d'en-tête suivante : `Content-Type`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`status`

Le code d'état HTTP . Fournissez le code d'état sous forme de chaîne. CloudFront utilise le code d'état fourni pour les opérations suivantes :

- Renvoi dans la réponse
- Cache dans le cache CloudFront périphérique, lorsque la réponse a été générée par une fonction déclenchée par un événement de demande d'origine
- Connectez-vous CloudFront Configuration et utilisation des journaux standard (journaux d'accès)

Si la `status` valeur n'est pas comprise entre 200 et 599, CloudFront renvoie une erreur au visualiseur.

`statusDescription`

Description que vous souhaitez CloudFront renvoyer dans la réponse, pour accompagner le code d'état HTTP. Vous n'avez pas besoin d'utiliser de descriptions standard, telles que `OK` pour un code de statut HTTP 200.

Erreurs

Voici des erreurs possibles pour les réponses HTTP générées.

La réponse contient un corps et un code de statut HTTP 204 (Pas de contenu)

Lorsqu'une fonction est déclenchée par une demande d'affichage, CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) au visualiseur lorsque les deux conditions suivantes sont vraies :

- La valeur du code `status` est 204 (Pas de contenu)
- La réponse inclut une valeur pour `body`

Cela vient du fait que Lambda@Edge impose la restriction facultative incluse dans la RFC 2616, qui stipule qu'une réponse `HTTP 204` n'a pas besoin d'inclure de corps de message.

Restrictions concernant la taille de la réponse générée

La taille maximale d'une réponse générée par une fonction Lambda dépend de l'événement qui a déclenché la fonction :

- Événements de demande utilisateur – 40 Ko
- Événements de demande à l'origine – 1 Mo

Si la réponse est supérieure à la taille autorisée, CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) au visualiseur.

Champs obligatoires

Le champ `status` est obligatoire.

Tous les autres champs sont facultatifs.

Mettre à jour les réponses HTTP dans les déclencheurs de réponse d'origine

Lorsque CloudFront vous recevez une réponse HTTP du serveur d'origine, si un déclencheur de réponse d'origine est associé au comportement du cache, vous pouvez modifier la réponse HTTP pour remplacer ce qui a été renvoyé par l'origine.

Les scénarios courants pour mettre à jour des réponses HTTP sont les suivants :

- Modification du statut sur HTTP 200 et création d'un contenu de corps statique à renvoyer à l'utilisateur lorsqu'une origine renvoie un code de statut d'erreur (4xx ou 5xx). Pour un exemple de

code, consultez Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 200.

- Modification du statut pour définir un code de statut HTTP 301 ou HTTP 302, afin de rediriger l'utilisateur vers un autre site web lorsqu'une origine renvoie un code de statut d'erreur (4xx ou 5xx). Pour un exemple de code, consultez Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 302.

> **Note**
>
> La fonction doit renvoyer une valeur d'état comprise entre `200` et `599` (inclus), sinon elle CloudFront renvoie une erreur au visualiseur.

Vous pouvez également remplacer les réponses HTTP dans les événements de requête utilisateur et à l'origine. Pour plus d'informations, consultez Générer des réponses HTTP dans les déclencheurs de requêtes.

Lorsque vous utilisez la réponse HTTP, Lambda@Edge n'expose pas le corps renvoyé par le serveur d'origine au déclencheur de réponse de l'origine. Vous pouvez générer un corps de contenu statique en lui attribuant la valeur souhaitée, ou supprimer le corps à l'intérieur de la fonction en définissant une valeur vide. Si vous n'actualisez pas le champ du corps dans votre fonction, le corps d'origine renvoyé par le serveur d'origine est renvoyé à l'utilisateur.

Accédez au corps de la demande en choisissant l'option Inclure le corps

Vous pouvez décider que Lambda@Edge expose le corps dans une demande pour des méthodes HTTP accessibles en écriture (POST, PUT, DELETE, etc.) afin que vous puissiez y accéder dans vos fonctions Lambda. Vous pouvez choisir un accès en lecture seule ou vous pouvez préciser que vous remplacerez le corps.

Pour activer cette option, choisissez Include Body lorsque vous créez un CloudFront déclencheur pour votre fonction destiné à une demande d'utilisateur ou à un événement de demande d'origine. Pour de plus amples informations, veuillez consulter Ajouter des déclencheurs pour une fonction Lambda @Edge, ou pour en savoir plus sur l'utilisation de Include Body (Inclure le corps) avec votre fonction, veuillez consulter Structure d'événement Lambda@Edge.

Les scénarios lorsque vous êtes susceptibles de vouloir utiliser cette fonction incluent les éléments suivants :

- Traitement des formulaires Web, comme « Contactez-nous », sans renvoyer les données saisies par le client aux serveurs d'origine.
- Collecte des données de balise web envoyées par les navigateurs des utilisateurs et traitement de ces données en périphérie.

Pour un exemple de code, consultez Exemples de fonctions Lambda@Edge.

> **Note**
>
> Si le corps de la demande est grand, Lambda@Edge le tronque. Pour plus d'informations sur la taille maximale et la troncature, veuillez consulter Restrictions relatives au corps de la requête avec l'option Inclure le corps.

Exemples de fonctions Lambda@Edge

Consultez les sections suivantes pour des exemples d'utilisation des fonctions Lambda avec Amazon. CloudFront

> **Note**
>
> Si vous choisissez d'exécuter Node.js 18 ou une version ultérieure pour votre fonction Lambda @Edge, un `index.mjs` fichier est créé automatiquement pour vous. Pour utiliser les exemples de code suivants, renommez `index.js` plutôt le `index.mjs` fichier en.

Rubriques

- Exemples généraux
- Générer des réponses - exemples
- Chaînes de requête - exemples
- Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples
- Sélection d'origine dynamique basée sur le contenu – exemples
- Mettre à jour les statuts d'erreur - exemples
- Accéder au corps de la demande - exemples

Exemples généraux

Les exemples présentés dans cette section illustrent certaines manières courantes d'utiliser Lambda @Edge dans. CloudFront

Rubriques

- Exemple : test A/B
- Exemple : remplacer un en-tête de réponse

Exemple : test A/B

Vous pouvez utiliser l'exemple suivant pour tester deux versions différentes d'une image sans créer de redirections ni modifier l'URL. Cet exemple lit les cookies dans la demande de l'utilisateur et modifie l'URL de la demande en conséquence. Si l'utilisateur n'envoie pas de cookie avec l'une des valeurs attendues, l'exemple affecte de façon aléatoire l'utilisateur à l'une des URL.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    if (request.uri !== '/experiment-pixel.jpg') {
        // do not process if this is not an A-B test request
        callback(null, request);
        return;
    }

    const cookieExperimentA = 'X-Experiment-Name=A';
    const cookieExperimentB = 'X-Experiment-Name=B';
    const pathExperimentA = '/experiment-group/control-pixel.jpg';
    const pathExperimentB = '/experiment-group/treatment-pixel.jpg';

    /*
     * Lambda at the Edge headers are array objects.
     *
     * Client may send multiple Cookie headers, i.e.:
     * > GET /viewerRes/test HTTP/1.1
```

```
     * > User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1
 OpenSSL/1.0.1u zlib/1.2.3
     * > Cookie: First=1; Second=2
     * > Cookie: ClientCode=abc
     * > Host: example.com
     *
     * You can access the first Cookie header at headers["cookie"][0].value
     * and the second at headers["cookie"][1].value.
     *
     * Header values are not parsed. In the example above,
     * headers["cookie"][0].value is equal to "First=1; Second=2"
     */
    let experimentUri;
    if (headers.cookie) {
        for (let i = 0; i < headers.cookie.length; i++) {
            if (headers.cookie[i].value.indexOf(cookieExperimentA) >= 0) {
                console.log('Experiment A cookie found');
                experimentUri = pathExperimentA;
                break;
            } else if (headers.cookie[i].value.indexOf(cookieExperimentB) >= 0) {
                console.log('Experiment B cookie found');
                experimentUri = pathExperimentB;
                break;
            }
        }
    }

    if (!experimentUri) {
        console.log('Experiment cookie has not been found. Throwing dice...');
        if (Math.random() < 0.75) {
            experimentUri = pathExperimentA;
        } else {
            experimentUri = pathExperimentB;
        }
    }

    request.uri = experimentUri;
    console.log(`Request uri set to "${request.uri}"`);
    callback(null, request);
};
```

Python

```
import json
import random

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    if request['uri'] != '/experiment-pixel.jpg':
        # Not an A/B Test
        return request

    cookieExperimentA, cookieExperimentB = 'X-Experiment-Name=A', 'X-Experiment-
Name=B'
    pathExperimentA, pathExperimentB = '/experiment-group/control-pixel.jpg', '/
experiment-group/treatment-pixel.jpg'

    '''
    Lambda at the Edge headers are array objects.

    Client may send multiple cookie headers. For example:
    > GET /viewerRes/test HTTP/1.1
    > User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1
 OpenSSL/1.0.1u zlib/1.2.3
    > Cookie: First=1; Second=2
    > Cookie: ClientCode=abc
    > Host: example.com

    You can access the first Cookie header at headers["cookie"][0].value
    and the second at headers["cookie"][1].value.

    Header values are not parsed. In the example above,
    headers["cookie"][0].value is equal to "First=1; Second=2"
    '''

    experimentUri = ""

    for cookie in headers.get('cookie', []):
        if cookieExperimentA in cookie['value']:
            print("Experiment A cookie found")
            experimentUri = pathExperimentA
            break
        elif cookieExperimentB in cookie['value']:
```

```
            print("Experiment B cookie found")
            experimentUri = pathExperimentB
            break

    if not experimentUri:
        print("Experiment cookie has not been found. Throwing dice...")
        if random.random() < 0.75:
            experimentUri = pathExperimentA
        else:
            experimentUri = pathExperimentB

    request['uri'] = experimentUri
    print(f"Request uri set to {experimentUri}")
    return request
```

Exemple : remplacer un en-tête de réponse

L'exemple suivant montre comment changer la valeur d'un en-tête de réponse en fonction de la valeur d'un autre en-tête.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
   const response = event.Records[0].cf.response;
   const headers = response.headers;

   const headerNameSrc = 'X-Amz-Meta-Last-Modified';
   const headerNameDst = 'Last-Modified';

   if (headers[headerNameSrc.toLowerCase()]) {
      headers[headerNameDst.toLowerCase()] = [
         headers[headerNameSrc.toLowerCase()][0],
      ];
      console.log(`Response header "${headerNameDst}" was set to ` +
               `"${headers[headerNameDst.toLowerCase()][0].value}"`);
   }

   callback(null, response);
};
```

Python

```
import json

def lambda_handler(event, context):
    response = event["Records"][0]["cf"]["response"]
    headers = response["headers"]

    headerNameSrc = "X-Amz-Meta-Last-Modified"
    headerNameDst = "Last-Modified"

    if headers.get(headerNameSrc.lower(), None):
        headers[headerNameDst.lower()] = [headers[headerNameSrc.lower()][0]]
        print(f"Response header {headerNameDst.lower()} was set to
 {headers[headerNameSrc.lower()][0]}")

    return response
```

Générer des réponses - exemples

Les exemples de cette section illustrent l'utilisation de Lambda@Edge pour générer des réponses.

Rubriques

- Exemple : diffuser du contenu statique (réponse générée)
- Exemple : générer une redirection HTTP (réponse générée)

Exemple : diffuser du contenu statique (réponse générée)

L'exemple suivant montre comment utiliser une fonction Lambda pour traiter le contenu statique d'un site web, ce qui réduit la charge sur le serveur d'origine et réduit la latence globale.

> **Note**
>
> Vous pouvez générer des réponses HTTP pour les événements de requête utilisateur ou de requête à l'origine. Pour plus d'informations, consultez the section called “Générer des réponses HTTP dans les déclencheurs de requêtes”.

Vous pouvez également remplacer ou supprimer le corps de la réponse HTTP dans les événements de réponse de l'origine. Pour plus d'informations, consultez the section called "Mettre à jour les réponses HTTP dans les déclencheurs de réponse d'origine".

Node.js

```
'use strict';

const content = `
<\!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Simple Lambda@Edge Static Content Response</title>
  </head>
  <body>
    <p>Hello from Lambda@Edge!</p>
  </body>
</html>
`;

exports.handler = (event, context, callback) => {
    /*
     * Generate HTTP OK response using 200 status code with HTML body.
     */
    const response = {
        status: '200',
        statusDescription: 'OK',
        headers: {
            'cache-control': [{
                key: 'Cache-Control',
                value: 'max-age=100'
            }],
            'content-type': [{
                key: 'Content-Type',
                value: 'text/html'
            }]
        },
        body: content,
    };
    callback(null, response);
```

```
};
```

Python

```
import json

CONTENT = """
<\!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Simple Lambda@Edge Static Content Response</title>
</head>
<body>
    <p>Hello from Lambda@Edge!</p>
</body>
</html>
"""

def lambda_handler(event, context):
    # Generate HTTP OK response using 200 status code with HTML body.
    response = {
        'status': '200',
        'statusDescription': 'OK',
        'headers': {
            'cache-control': [
                {
                    'key': 'Cache-Control',
                    'value': 'max-age=100'
                }
            ],
            "content-type": [
                {
                    'key': 'Content-Type',
                    'value': 'text/html'
                }
            ]
        },
        'body': CONTENT
    }
    return response
```

Exemple : générer une redirection HTTP (réponse générée)

L'exemple suivant montre comment générer une redirection HTTP.

> **Note**
>
> Vous pouvez générer des réponses HTTP pour les événements de requête utilisateur ou de requête à l'origine. Pour plus d'informations, consultez Générer des réponses HTTP dans les déclencheurs de requêtes.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    /*
     * Generate HTTP redirect response with 302 status code and Location header.
     */
    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: 'https://docs.aws.amazon.com/lambda/latest/dg/lambda-
edge.html',
            }],
        },
    };
    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):

    # Generate HTTP redirect response with 302 status code and Location header.

    response = {
        'status': '302',
        'statusDescription': 'Found',
```

```
        'headers': {
            'location': [{
                'key': 'Location',
                'value': 'https://docs.aws.amazon.com/lambda/latest/dg/lambda-
edge.html'
            }]
        }
    }

    return response
```

Chaînes de requête - exemples

Les exemples de cette section illustrent plusieurs méthodes d'utilisation de Lambda@Edge avec des chaînes de requête.

Rubriques

- Exemple : ajout d'un en-tête basé sur un paramètre de chaîne de requête
- Exemple : normalisation des paramètres de chaîne de requête pour améliorer le taux de réussite du cache
- Exemple : rediriger les utilisateurs non authentifiés vers une page de connexion

Exemple : ajout d'un en-tête basé sur un paramètre de chaîne de requête

L'exemple suivant montre comment obtenir la paire clé-valeur d'un paramètre de chaîne de requête, puis ajouter un en-tête en fonction de ces valeurs.

Node.js

```
'use strict';

const querystring = require('querystring');
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    /* When a request contains a query string key-value pair but the origin server
     * expects the value in a header, you can use this Lambda function to
     * convert the key-value pair to a header. Here's what the function does:
     * 1. Parses the query string and gets the key-value pair.
```

```
     * 2. Adds a header to the request using the key-value pair that the function
 got in step 1.
     */

    /* Parse request querystring to get javascript object */
    const params = querystring.parse(request.querystring);

    /* Move auth param from querystring to headers */
    const headerName = 'Auth-Header';
    request.headers[headerName.toLowerCase()] = [{ key: headerName, value:
 params.auth }];
    delete params.auth;

    /* Update request querystring */
    request.querystring = querystring.stringify(params);

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    When a request contains a query string key-value pair but the origin server
    expects the value in a header, you can use this Lambda function to
    convert the key-value pair to a header. Here's what the function does:
        1. Parses the query string and gets the key-value pair.
        2. Adds a header to the request using the key-value pair that the function
 got in step 1.
    '''

    # Parse request querystring to get dictionary/json
    params = {k : v[0] for k, v in parse_qs(request['querystring']).items()}

    # Move auth param from querystring to headers
    headerName = 'Auth-Header'
    request['headers'][headerName.lower()] = [{'key': headerName, 'value':
 params['auth']}]
    del params['auth']
```

```
    # Update request querystring
    request['querystring'] = urlencode(params)

    return request
```

Exemple : normalisation des paramètres de chaîne de requête pour améliorer le taux de réussite du cache

L'exemple suivant montre comment améliorer le taux de réussite de votre cache en apportant les modifications suivantes aux chaînes de requête avant de CloudFront transférer les demandes à votre origine :

- Classez par ordre alphabétique les paires clé-valeur selon le nom du paramètre.
- Modifiez la casse des paires clé-valeur en minuscules.

Pour plus d'informations, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

Node.js

```
'use strict';

const querystring = require('querystring');

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    /* When you configure a distribution to forward query strings to the origin and
     * to cache based on an allowlist of query string parameters, we recommend
     * the following to improve the cache-hit ratio:
     * - Always list parameters in the same order.
     * - Use the same case for parameter names and values.
     *
     * This function normalizes query strings so that parameter names and values
     * are lowercase and parameter names are in alphabetical order.
     *
     * For more information, see:
     * https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/
QueryStringParameters.html
     */

    console.log('Query String: ', request.querystring);
```

```
    /* Parse request query string to get javascript object */
    const params = querystring.parse(request.querystring.toLowerCase());
    const sortedParams = {};

    /* Sort param keys */
    Object.keys(params).sort().forEach(key => {
        sortedParams[key] = params[key];
    });

    /* Update request querystring with normalized  */
    request.querystring = querystring.stringify(sortedParams);

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    '''
    When you configure a distribution to forward query strings to the origin and
    to cache based on an allowlist of query string parameters, we recommend
    the following to improve the cache-hit ratio:
    Always list parameters in the same order.
    - Use the same case for parameter names and values.

    This function normalizes query strings so that parameter names and values
    are lowercase and parameter names are in alphabetical order.

    For more information, see:
    https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/
QueryStringParameters.html
    '''
    print("Query string: ", request["querystring"])

    # Parse request query string to get js object
    params = {k : v[0] for k, v in parse_qs(request['querystring'].lower()).items()}

    # Sort param keys
    sortedParams = sorted(params.items(), key=lambda x: x[0])
```

```
    # Update request querystring with normalized
    request['querystring'] = urlencode(sortedParams)

    return request
```

Exemple : rediriger les utilisateurs non authentifiés vers une page de connexion

L'exemple suivant montre comment rediriger des utilisateurs vers une page de connexion s'ils n'ont pas saisi leurs informations d'identification.

Node.js

```
'use strict';

function parseCookies(headers) {
    const parsedCookie = {};
    if (headers.cookie) {
        headers.cookie[0].value.split(';').forEach((cookie) => {
            if (cookie) {
                const parts = cookie.split('=');
                parsedCookie[parts[0].trim()] = parts[1].trim();
            }
        });
    }
    return parsedCookie;
}

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    /* Check for session-id in request cookie in viewer-request event,
     * if session-id is absent, redirect the user to sign in page with original
     * request sent as redirect_url in query params.
     */

    /* Check for session-id in cookie, if present then proceed with request */
    const parsedCookies = parseCookies(headers);
    if (parsedCookies && parsedCookies['session-id']) {
        callback(null, request);
        return;
```

```
    }

    /* URI encode the original request to be sent as redirect_url in query params */
    const encodedRedirectUrl = encodeURIComponent(`https://
${headers.host[0].value}${request.uri}?${request.querystring}`);
    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: `https://www.example.com/signin?redirect_url=
${encodedRedirectUrl}`,
            }],
        },
    };
    callback(null, response);
};
```

Python

```
import urllib

def parseCookies(headers):
    parsedCookie = {}
    if headers.get('cookie'):
        for cookie in headers['cookie'][0]['value'].split(';'):
            if cookie:
                parts = cookie.split('=')
                parsedCookie[parts[0].strip()] = parts[1].strip()
    return parsedCookie

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    '''
    Check for session-id in request cookie in viewer-request event,
    if session-id is absent, redirect the user to sign in page with original
    request sent as redirect_url in query params.
    '''

    # Check for session-id in cookie, if present, then proceed with request
```

```
    parsedCookies = parseCookies(headers)

    if parsedCookies and parsedCookies['session-id']:
        return request

    # URI encode the original request to be sent as redirect_url in query params
    redirectUrl = "https://%s%s?%s" % (headers['host'][0]['value'], request['uri'],
request['querystring'])
    encodedRedirectUrl = urllib.parse.quote_plus(redirectUrl.encode('utf-8'))

    response = {
        'status': '302',
        'statusDescription': 'Found',
        'headers': {
            'location': [{
                'key': 'Location',
                'value': 'https://www.example.com/signin?redirect_url=%s' %
encodedRedirectUrl
            }]
        }
    }
    return response
```

Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples

Les exemples de cette section illustrent une méthode d'utilisation de Lambda@Edge pour personnaliser le comportement en fonction de l'emplacement ou du type d'appareil utilisé par l'utilisateur.

Rubriques

- Exemple : rediriger les demandes des visiteurs vers une URL spécifique à un pays
- Exemple : servir différentes versions d'un objet en fonction de l'appareil

Exemple : rediriger les demandes des visiteurs vers une URL spécifique à un pays

L'exemple suivant montre comment générer une réponse de redirection HTTP avec une URL propre à un pays et renvoyer la réponse à l'utilisateur. Ceci s'avère utile lorsque vous souhaitez fournir des réponses propres à un pays. Exemples :

- Si vous avez des sous-domaines propres à un pays, comme us.example.com et tw.example.com, vous pouvez générer une réponse de redirection lorsqu'un utilisateur demande example.com.
- Si vous diffusez une vidéo, mais que vous ne disposez pas de droits pour diffuser le contenu dans un pays spécifique, vous pouvez rediriger les utilisateurs de ce pays vers une page qui explique pourquoi ils ne peuvent regarder la vidéo.

Remarques :

- Vous devez configurer votre distribution pour être mise en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- CloudFront ajoute l'`CloudFront-Viewer-Country`en-tête après l'événement de demande du spectateur. Pour utiliser cet exemple, vous devez créer un déclencheur pour l'événement de demande à l'origine.

Node.js

```
'use strict';

/* This is an origin request function */
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    /*
     * Based on the value of the CloudFront-Viewer-Country header, generate an
     * HTTP status code 302 (Redirect) response, and return a country-specific
     * URL in the Location header.
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Viewer-Country header. For more information, see
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    let url = 'https://example.com/';
```

```
    if (headers['cloudfront-viewer-country']) {
        const countryCode = headers['cloudfront-viewer-country'][0].value;
        if (countryCode === 'TW') {
            url = 'https://tw.example.com/';
        } else if (countryCode === 'US') {
            url = 'https://us.example.com/';
        }
    }

    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: url,
            }],
        },
    };
    callback(null, response);
};
```

Python

```
# This is an origin request function

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    '''
    Based on the value of the CloudFront-Viewer-Country header, generate an
    HTTP status code 302 (Redirect) response, and return a country-specific
    URL in the Location header.
    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    url = 'https://example.com/'
```

```
    viewerCountry = headers.get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        if countryCode == 'TW':
            url = 'https://tw.example.com/'
        elif countryCode == 'US':
            url = 'https://us.example.com/'

    response = {
        'status': '302',
        'statusDescription': 'Found',
        'headers': {
            'location': [{
                'key': 'Location',
                'value': url
            }]
        }
    }

    return response
```

Exemple : servir différentes versions d'un objet en fonction de l'appareil

L'exemple suivant montre comment servir différentes versions d'un objet en fonction du type d'appareil employé par l'utilisateur, par exemple, un appareil mobile ou une tablette. Remarques :

- Vous devez configurer votre distribution pour être mise en cache en fonction des en-têtes `CloudFront-Is-*-Viewer`. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- CloudFront ajoute les `CloudFront-Is-*-Viewer` en-têtes après l'événement de demande du spectateur. Pour utiliser cet exemple, vous devez créer un déclencheur pour l'événement de demande à l'origine.

Node.js

```
'use strict';

/* This is an origin request function */
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
```

```
    const headers = request.headers;

    /*
     * Serve different versions of an object based on the device type.
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Is-*-Viewer headers. For more information, see
     *          the following documentation:
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-device-type
     *       2. CloudFront adds the CloudFront-Is-*-Viewer headers after the viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    const desktopPath = '/desktop';
    const mobilePath = '/mobile';
    const tabletPath = '/tablet';
    const smarttvPath = '/smarttv';

    if (headers['cloudfront-is-desktop-viewer']
        && headers['cloudfront-is-desktop-viewer'][0].value === 'true') {
        request.uri = desktopPath + request.uri;
    } else if (headers['cloudfront-is-mobile-viewer']
               && headers['cloudfront-is-mobile-viewer'][0].value === 'true') {
        request.uri = mobilePath + request.uri;
    } else if (headers['cloudfront-is-tablet-viewer']
               && headers['cloudfront-is-tablet-viewer'][0].value === 'true') {
        request.uri = tabletPath + request.uri;
    } else if (headers['cloudfront-is-smarttv-viewer']
               && headers['cloudfront-is-smarttv-viewer'][0].value === 'true') {
        request.uri = smarttvPath + request.uri;
    }
    console.log(`Request uri set to "${request.uri}"`);

    callback(null, request);
};
```

Python

```
# This is an origin request function
def lambda_handler(event, context):
```

```
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    '''
    Serve different versions of an object based on the device type.
    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Is-*-Viewer headers. For more information, see
            the following documentation:
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
            https://docs.aws.amazon.com/console/cloudfront/cache-on-device-type
          2. CloudFront adds the CloudFront-Is-*-Viewer headers after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    desktopPath = '/desktop';
    mobilePath = '/mobile';
    tabletPath = '/tablet';
    smarttvPath = '/smarttv';

    if 'cloudfront-is-desktop-viewer' in headers and headers['cloudfront-is-desktop-
viewer'][0]['value'] == 'true':
        request['uri'] = desktopPath + request['uri']
    elif 'cloudfront-is-mobile-viewer' in headers and headers['cloudfront-is-mobile-
viewer'][0]['value'] == 'true':
        request['uri'] = mobilePath + request['uri']
    elif 'cloudfront-is-tablet-viewer' in headers and headers['cloudfront-is-tablet-
viewer'][0]['value'] == 'true':
        request['uri'] = tabletPath + request['uri']
    elif 'cloudfront-is-smarttv-viewer' in headers and headers['cloudfront-is-
smarttv-viewer'][0]['value'] == 'true':
        request['uri'] = smarttvPath + request['uri']

    print("Request uri set to %s" % request['uri'])

    return request
```

Sélection d'origine dynamique basée sur le contenu – exemples

Les exemples de cette section illustrent une méthode d'utilisation de Lambda@Edge pour acheminer vers différentes origines en fonction des informations contenues dans la demande.

Rubriques

Exemple : utiliser un déclencheur de demande d'origine pour passer d'une origine personnalisée à une origine Amazon S3

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour passer d'une origine personnalisée à une origine Amazon S3 à partir de laquelle le contenu est récupéré en fonction des propriétés de la demande.

Node.js

```
'use strict';

 const querystring = require('querystring');

 exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

     /**
      * Reads query string to check if S3 origin should be used, and
      * if true, sets S3 origin properties.
      */

     const params = querystring.parse(request.querystring);

     if (params['useS3Origin']) {
         if (params['useS3Origin'] === 'true') {
             const s3DomainName = 'my-bucket.s3.amazonaws.com';
```

```
            /* Set S3 origin fields */
            request.origin = {
                s3: {
                    domainName: s3DomainName,
                    region: '',
                    authMethod: 'none',
                    path: '',
                    customHeaders: {}
                }
            };
            request.headers['host'] = [{ key: 'host', value: s3DomainName}];
        }
    }

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    '''
    Reads query string to check if S3 origin should be used, and
    if true, sets S3 origin properties
    '''
    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}
    if params.get('useS3Origin') == 'true':
        s3DomainName = 'my-bucket.s3.amazonaws.com'

        # Set S3 origin fields
        request['origin'] = {
            's3': {
                'domainName': s3DomainName,
                'region': '',
                'authMethod': 'none',
                'path': '',
                'customHeaders': {}
            }
        }
        request['headers']['host'] = [{'key': 'host', 'value': s3DomainName}]
    return request
```

Exemple : utiliser un déclencheur de demande d'origine pour modifier la région d'origine d'Amazon S3

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour modifier l'origine Amazon S3 à partir de laquelle le contenu est récupéré en fonction des propriétés de la demande.

Dans cet exemple, nous utilisons la valeur de l'en-tête `CloudFront-Viewer-Country` pour mettre à jour le nom de domaine de compartiment S3 en spécifiant un compartiment dans une région plus proche de l'utilisateur. Cela peut être utile à plusieurs égards :

- Cela réduit la latence lorsque la région spécifiée est plus proche du pays de l'utilisateur.
- Il est possible de contrôler les données en s'assurant qu'elles sont distribuées depuis une origine qui se trouve dans le pays de provenance de la demande.

Pour utiliser cet exemple, vous devez procéder comme suit :

- Vous devez configurer votre distribution à mettre en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- Créez un déclencheur pour cette fonction dans l'événement de demande d'origine. CloudFrontajoute l'`CloudFront-Viewer-Country`en-tête après l'événement de demande du visualiseur. Pour utiliser cet exemple, vous devez vous assurer que la fonction s'exécute pour une demande d'origine.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    /**
     * This blueprint demonstrates how an origin-request trigger can be used to
     * change the origin from which the content is fetched, based on request
 properties.
     * In this example, we use the value of the CloudFront-Viewer-Country header
     * to update the S3 bucket domain name to a bucket in a Region that is closer to
     * the viewer.
```

```
    *
    * This can be useful in several ways:
    *      1) Reduces latencies when the Region specified is nearer to the viewer's
    *         country.
    *      2) Provides data sovereignty by making sure that data is served from an
    *         origin that's in the same country that the request came from.
    *
    * NOTE: 1. You must configure your distribution to cache based on the
    *          CloudFront-Viewer-Country header. For more information, see
    *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
    *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
    *          request event. To use this example, you must create a trigger for
 the
    *          origin request event.
    */

   const countryToRegion = {
       'DE': 'eu-central-1',
       'IE': 'eu-west-1',
       'GB': 'eu-west-2',
       'FR': 'eu-west-3',
       'JP': 'ap-northeast-1',
       'IN': 'ap-south-1'
   };

   if (request.headers['cloudfront-viewer-country']) {
       const countryCode = request.headers['cloudfront-viewer-country'][0].value;
       const region = countryToRegion[countryCode];

       /**
        * If the viewer's country is not in the list you specify, the request
        * goes to the default S3 bucket you've configured.
        */
       if (region) {
           /**
            * If you've set up OAI, the bucket policy in the destination bucket
            * should allow the OAI GetObject operation, as configured by default
            * for an S3 origin with OAI. Another requirement with OAI is to provide
            * the Region so it can be used for the SIGV4 signature. Otherwise, the
            * Region is not required.
            */
           request.origin.s3.region = region;
```

```
            const domainName = `my-bucket-in-${region}.s3.amazonaws.com`;
            request.origin.s3.domainName = domainName;
            request.headers['host'] = [{ key: 'host', value: domainName }];
        }
    }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    This blueprint demonstrates how an origin-request trigger can be used to
    change the origin from which the content is fetched, based on request
 properties.
    In this example, we use the value of the CloudFront-Viewer-Country header
    to update the S3 bucket domain name to a bucket in a Region that is closer to
    the viewer.

    This can be useful in several ways:
        1) Reduces latencies when the Region specified is nearer to the viewer's
            country.
        2) Provides data sovereignty by making sure that data is served from an
            origin that's in the same country that the request came from.

    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
```

```
    }

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        region = countryToRegion.get(countryCode)

        # If the viewer's country in not in the list you specify, the request
        # goes to the default S3 bucket you've configured
        if region:
            '''
            If you've set up OAI, the bucket policy in the destination bucket
            should allow the OAI GetObject operation, as configured by default
            for an S3 origin with OAI. Another requirement with OAI is to provide
            the Region so it can be used for the SIGV4 signature. Otherwise, the
            Region is not required.
            '''
            request['origin']['s3']['region'] = region
            domainName = 'my-bucket-in-%s.s3.amazonaws.com' % region
            request['origin']['s3']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Exemple : utiliser un déclencheur de demande d'origine pour passer d'une origine Amazon S3 à une origine personnalisée

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour modifier l'origine personnalisée à partir de laquelle le contenu est récupéré, en fonction des propriétés de la demande.

Node.js

```
'use strict';

const querystring = require('querystring');

 exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

     /**
      * Reads query string to check if custom origin should be used, and
```

```
     * if true, sets custom origin properties.
     */

    const params = querystring.parse(request.querystring);

    if (params['useCustomOrigin']) {
        if (params['useCustomOrigin'] === 'true') {

            /* Set custom origin fields*/
            request.origin = {
                custom: {
                    domainName: 'www.example.com',
                    port: 443,
                    protocol: 'https',
                    path: '',
                    sslProtocols: ['TLSv1', 'TLSv1.1'],
                    readTimeout: 5,
                    keepaliveTimeout: 5,
                    customHeaders: {}
                }
            };
            request.headers['host'] = [{ key: 'host', value: 'www.example.com'}];
        }
    }
    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    # Reads query string to check if custom origin should be used, and
    # if true, sets custom origin properties

    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}

    if params.get('useCustomOrigin') == 'true':
            # Set custom origin fields
            request['origin'] = {
                'custom': {
```

```
                    'domainName': 'www.example.com',
                    'port': 443,
                    'protocol': 'https',
                    'path': '',
                    'sslProtocols': ['TLSv1', 'TLSv1.1'],
                    'readTimeout': 5,
                    'keepaliveTimeout': 5,
                    'customHeaders': {}
                }
            }
            request['headers']['host'] = [{'key': 'host', 'value':
 'www.example.com'}]

    return request
```

Exemple : utilisez un déclencheur de demande d'origine pour transférer progressivement le trafic d'un compartiment Amazon S3 à un autre

Cette fonction montre comment transférer progressivement le trafic d'un compartiment Amazon S3 à un autre de manière contrôlée.

Node.js

```
'use strict';

    function getRandomInt(min, max) {
        /* Random number is inclusive of min and max*/
        return Math.floor(Math.random() * (max - min + 1)) + min;
 }

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const BLUE_TRAFFIC_PERCENTAGE = 80;

    /**
      * This Lambda function demonstrates how to gradually transfer traffic from
      * one S3 bucket to another in a controlled way.
      * We define a variable BLUE_TRAFFIC_PERCENTAGE which can take values from
      * 1 to 100. If the generated randomNumber less than or equal to
 BLUE_TRAFFIC_PERCENTAGE, traffic
      * is re-directed to blue-bucket. If not, the default bucket that we've
 configured
```

```
      * is used.
      */

    const randomNumber = getRandomInt(1, 100);

if (randomNumber <= BLUE_TRAFFIC_PERCENTAGE) {
         const domainName = 'blue-bucket.s3.amazonaws.com';
         request.origin.s3.domainName = domainName;
         request.headers['host'] = [{ key: 'host', value: domainName}];
     }
    callback(null, request);
};
```

Python

```
import math
import random

def getRandomInt(min, max):
    # Random number is inclusive of min and max
    return math.floor(random.random() * (max - min + 1)) + min

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    BLUE_TRAFFIC_PERCENTAGE = 80

    '''
    This Lambda function demonstrates how to gradually transfer traffic from
    one S3 bucket to another in a controlled way.
    We define a variable BLUE_TRAFFIC_PERCENTAGE which can take values from
    1 to 100. If the generated randomNumber less than or equal to
 BLUE_TRAFFIC_PERCENTAGE, traffic
    is re-directed to blue-bucket. If not, the default bucket that we've configured
    is used.
    '''

    randomNumber = getRandomInt(1, 100)

    if randomNumber <= BLUE_TRAFFIC_PERCENTAGE:
        domainName = 'blue-bucket.s3.amazonaws.com'
        request['origin']['s3']['domainName'] = domainName
        request['headers']['host'] = [{'key': 'host', 'value': domainName}]
```

```
    return request
```

Exemple : utilisez un déclencheur de demande d'origine pour modifier le nom de domaine d'origine en fonction de l'en-tête du pays

Cette fonction explique comment vous pouvez modifier le nom de domaine de l'origine en fonction de l'en-tête `CloudFront-Viewer-Country` afin que le contenu soit transmis depuis une origine plus proche du pays de l'utilisateur.

La mise en œuvre de cette fonctionnalité pour votre distribution peut avoir les avantages suivants :

- Réduction de la latence lorsque la région spécifiée est plus proche du pays de l'utilisateur
- Assurance de la souveraineté des données en veillant à ce que les données soient distribuées depuis une origine qui se trouve dans le pays d'où vient la demande

Notez que pour activer cette fonctionnalité, vous devez configurer votre distribution pour qu'elle soit mise en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d'informations, consultez the section called “Mise en cache basée sur des en-têtes de demande sélectionnés”.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

  if (request.headers['cloudfront-viewer-country']) {
        const countryCode = request.headers['cloudfront-viewer-country'][0].value;
        if (countryCode === 'GB' || countryCode === 'DE' || countryCode === 'IE' )
 {
            const domainName = 'eu.example.com';
            request.origin.custom.domainName = domainName;
            request.headers['host'] = [{key: 'host', value: domainName}];
        }
     }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        if countryCode == 'GB' or countryCode == 'DE' or countryCode == 'IE':
            domainName = 'eu.example.com'
            request['origin']['custom']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]
    return request
```

Mettre à jour les statuts d'erreur - exemples

Les exemples de cette section fournissent des conseils sur l'utilisation de Lambda@Edge pour modifier le statut d'erreur qui est renvoyé aux utilisateurs.

Rubriques

- Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 200
- Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 302

Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 200

Cette fonction explique comment vous pouvez mettre à jour le statut de la réponse sur 200 et générer un contenu de corps statique à renvoyer à l'utilisateur dans le scénario suivant :

- La fonction est déclenchée dans une réponse de l'origine.
- Le statut de la réponse du serveur d'origine est un code de statut d'erreur (4xx ou 5xx).

Node.js

```
'use strict';
```

```
exports.handler = (event, context, callback) => {
    const response = event.Records[0].cf.response;

    /**
     * This function updates the response status to 200 and generates static
     * body content to return to the viewer in the following scenario:
     * 1. The function is triggered in an origin response
     * 2. The response status from the origin server is an error status code (4xx or
 5xx)
     */

    if (response.status >= 400 && response.status <= 599) {
        response.status = 200;
        response.statusDescription = 'OK';
        response.body = 'Body generation example';
    }

    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']

    '''
    This function updates the response status to 200 and generates static
    body content to return to the viewer in the following scenario:
    1. The function is triggered in an origin response
    2. The response status from the origin server is an error status code (4xx or
 5xx)
    '''

    if int(response['status']) >= 400 and int(response['status']) <= 599:
        response['status'] = 200
        response['statusDescription'] = 'OK'
        response['body'] = 'Body generation example'
    return response
```

Exemple : utilisez un déclencheur de réponse d'origine pour mettre à jour le code d'état d'erreur à 302

Cette fonction explique comment vous pouvez mettre à jour le code de statut HTTP sur 302 pour rediriger le trafic vers un autre chemin (comportement de cache) qui possède une autre origine configurée. Remarques :

- La fonction est déclenchée dans une réponse de l'origine.
- Le statut de la réponse du serveur d'origine est un code de statut d'erreur (4xx ou 5xx).

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const response = event.Records[0].cf.response;
    const request = event.Records[0].cf.request;

    /**
     * This function updates the HTTP status code in the response to 302, to
 redirect to another
     * path (cache behavior) that has a different origin configured. Note the
 following:
     * 1. The function is triggered in an origin response
     * 2. The response status from the origin server is an error status code (4xx or
 5xx)
     */

    if (response.status >= 400 && response.status <= 599) {
        const redirect_path = `/plan-b/path?${request.querystring}`;

        response.status = 302;
        response.statusDescription = 'Found';

        /* Drop the body, as it is not required for redirects */
        response.body = '';
        response.headers['location'] = [{ key: 'Location', value: redirect_path }];
    }

    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']
    request = event['Records'][0]['cf']['request']

    '''
    This function updates the HTTP status code in the response to 302, to redirect
 to another
    path (cache behavior) that has a different origin configured. Note the
 following:
    1. The function is triggered in an origin response
    2. The response status from the origin server is an error status code (4xx or
 5xx)
    '''

    if int(response['status']) >= 400 and int(response['status']) <= 599:
        redirect_path = '/plan-b/path?%s' % request['querystring']

        response['status'] = 302
        response['statusDescription'] = 'Found'

        # Drop the body as it is not required for redirects
        response['body'] = ''
        response['headers']['location'] = [{'key': 'Location', 'value':
 redirect_path}]

    return response
```

Accéder au corps de la demande - exemples

Les exemples de cette section illustrent l'utilisation de Lambda@Edge pour utiliser des demandes POST.

> **Note**
>
> Pour utiliser ces exemples, vous devez activer l'option Inclure le corps dans l'association de fonction Lambda de la distribution. Elle n'est pas activée par défaut.
>
> - Pour activer ce paramètre dans la CloudFront console, cochez la case Inclure le corps dans l'association de fonctions Lambda.

- Pour activer ce paramètre dans l' CloudFront API ou avec AWS CloudFormation, définissez le `IncludeBody` champ sur `true` in`LambdaFunctionAssociation`.

Rubriques

- Exemple : utiliser un déclencheur de requête pour lire un formulaire HTML
- Exemple : utilisation d'un déclencheur de demande pour modifier un formulaire HTML

Exemple : utiliser un déclencheur de requête pour lire un formulaire HTML

Cette fonction montre comment vous pouvez traiter le corps d'une requête POST générée par un formulaire HTML (formulaire web), tel que « Contactez-nous ». Par exemple, vous pouvez avoir un formulaire HTML comme le suivant :

```
<html>
  <form action="https://example.com" method="post">
    Param 1: <input type="text" name="name1"><br>
    Param 2: <input type="text" name="name2"><br>
    input type="submit" value="Submit">
  </form>
</html>
```

Pour l'exemple de fonction qui suit, la fonction doit être déclenchée dans une demande de CloudFront visualisation ou une demande d'origine.

Node.js

```
'use strict';

const querystring = require('querystring');

/**
 * This function demonstrates how you can read the body of a POST request
 * generated by an HTML form (web form). The function is triggered in a
 * CloudFront viewer request or origin request event type.
 */

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
```

```
    if (request.method === 'POST') {
        /* HTTP body is always passed as base64-encoded string. Decode it. */
        const body = Buffer.from(request.body.data, 'base64').toString();

        /* HTML forms send the data in query string format. Parse it. */
        const params = querystring.parse(body);

        /* For demonstration purposes, we only log the form fields here.
         * You can put your custom logic here. For example, you can store the
         * fields in a database, such as Amazon DynamoDB, and generate a response
         * right from your Lambda@Edge function.
         */
        for (let param in params) {
            console.log(`For "${param}" user submitted "${params[param]}".\n`);
        }
    }
    return callback(null, request);
};
```

Python

```
import base64
from urllib.parse import parse_qs

'''
Say there is a POST request body generated by an HTML such as:

<html>
<form action="https://example.com" method="post">
    Param 1: <input type="text" name="name1"><br>
    Param 2: <input type="text" name="name2"><br>
    input type="submit" value="Submit">
</form>
</html>

'''

'''
This function demonstrates how you can read the body of a POST request
generated by an HTML form (web form). The function is triggered in a
CloudFront viewer request or origin request event type.
'''
```

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    if request['method'] == 'POST':
        # HTTP body is always passed as base64-encoded string. Decode it
        body = base64.b64decode(request['body']['data'])

        # HTML forms send the data in query string format. Parse it
        params = {k: v[0] for k, v in parse_qs(body).items()}

        '''
        For demonstration purposes, we only log the form fields here.
        You can put your custom logic here. For example, you can store the
        fields in a database, such as Amazon DynamoDB, and generate a response
        right from your Lambda@Edge function.
        '''
        for key, value in params.items():
            print("For %s use submitted %s" % (key, value))

    return request
```

Exemple : utilisation d'un déclencheur de demande pour modifier un formulaire HTML

Cette fonction montre comment vous pouvez modifier le corps d'une requête POST générée par un formulaire HTML (formulaire web). La fonction est déclenchée dans une demande de CloudFront visualisation ou une demande d'origine.

Node.js

```
'use strict';

const querystring = require('querystring');

exports.handler = (event, context, callback) => {
    var request = event.Records[0].cf.request;
    if (request.method === 'POST') {
        /* Request body is being replaced. To do this, update the following
        /* three fields:
         *    1) body.action to 'replace'
         *    2) body.encoding to the encoding of the new data.
         *
         *       Set to one of the following values:
```

```
         *
         *           text - denotes that the generated body is in text format.
         *               Lambda@Edge will propagate this as is.
         *           base64 - denotes that the generated body is base64 encoded.
         *               Lambda@Edge will base64 decode the data before sending
         *               it to the origin.
         *    3) body.data to the new body.
         */
        request.body.action = 'replace';
        request.body.encoding = 'text';
        request.body.data = getUpdatedBody(request);
    }
    callback(null, request);
};

function getUpdatedBody(request) {
    /* HTTP body is always passed as base64-encoded string. Decode it. */
    const body = Buffer.from(request.body.data, 'base64').toString();

    /* HTML forms send data in query string format. Parse it. */
    const params = querystring.parse(body);

    /* For demonstration purposes, we're adding one more param.
     *
     * You can put your custom logic here. For example, you can truncate long
     * bodies from malicious requests.
     */
    params['new-param-name'] = 'new-param-value';
    return querystring.stringify(params);
}
```

Python

```
import base64
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    if request['method'] == 'POST':
        '''
        Request body is being replaced. To do this, update the following
        three fields:
            1) body.action to 'replace'
```

```
            2) body.encoding to the encoding of the new data.

            Set to one of the following values:

                text - denotes that the generated body is in text format.
                    Lambda@Edge will propagate this as is.
                base64 - denotes that the generated body is base64 encoded.
                    Lambda@Edge will base64 decode the data before sending
                    it to the origin.
            3) body.data to the new body.
        '''
        request['body']['action'] = 'replace'
        request['body']['encoding'] = 'text'
        request['body']['data'] = getUpdatedBody(request)
    return request

def getUpdatedBody(request):
    # HTTP body is always passed as base64-encoded string. Decode it
    body = base64.b64decode(request['body']['data'])

    # HTML forms send data in query string format. Parse it
    params = {k: v[0] for k, v in parse_qs(body).items()}

    # For demonstration purposes, we're adding one more param

    # You can put your custom logic here. For example, you can truncate long
    # bodies from malicious requests
    params['new-param-name'] = 'new-param-value'
    return urlencode(params)
```

Restrictions sur les fonctions périphériques

Les rubriques suivantes décrivent les restrictions qui s'appliquent aux CloudFront fonctions et à Lambda @Edge. Certaines restrictions s'appliquent à toutes les fonctions Edge, tandis que d'autres s'appliquent uniquement à CloudFront Functions ou à Lambda @Edge.

Pour plus d'informations sur les quotas (anciennement appelés limites), consultez Quotas relatifs aux CloudFront fonctions et Quotas sur Lambda@Edge.

Rubriques

- Restrictions sur toutes les fonctions périphériques

- Restrictions relatives aux CloudFront fonctions
- Restrictions sur Lambda@Edge

Restrictions sur toutes les fonctions périphériques

Les restrictions suivantes s'appliquent à toutes les fonctions Edge, à la fois à CloudFront Functions et à Lambda @Edge.

Rubriques

PropriétéCompte AWS

Pour associer une fonction de périphérie à une CloudFront distribution, la fonction et la distribution doivent appartenir à la même entité Compte AWS.

Combinaison de CloudFront fonctions avec Lambda @Edge

Pour un comportement de cache donné, les restrictions suivantes s'appliquent :

- Chaque type d'événement (requête de l'utilisateur, requête de l'origine, réponse de l'origine et réponse de l'utilisateur) ne peut posséder qu'une association de fonctions périphériques.
- Vous ne pouvez pas combiner CloudFront Functions et Lambda @Edge dans les événements du visualiseur (demande du visualiseur et réponse du visualiseur).

Toutes les autres combinaisons de fonctions périphériques sont autorisées. Le tableau suivant explique les combinaisons autorisées.

		CloudFront Fonctions	
		Demande utilisateur	Réponse utilisateur
Lambda@Edge	Demande utilisateur	Non autorisée	Non autorisée
	Demande de l'origine	Autorisé	Autorisé
	Réponse de l'origine	Autorisé	Autorisé
	Réponse utilisateur	Non autorisée	Non autorisée

Codes d'état HTTP

CloudFront n'invoque pas les fonctions Edge pour les événements de réponse du spectateur lorsque l'origine renvoie le code d'état HTTP 400 ou supérieur.

Pour les événements de réponse d'origine, les fonctions Lambda@Edge sont appelées pour toutes les réponses d'origine, notamment lorsque l'origine renvoie un code de statut HTTP supérieur ou supérieur à 400. Pour de plus amples informations, veuillez consulter Mettre à jour les réponses HTTP dans les déclencheurs de réponse d'origine.

En-têtes HTTP

Certains en-têtes HTTP ne sont pas autorisés, ce qui signifie qu'ils ne sont pas exposés aux fonctions de périphérie et que les fonctions ne peuvent pas les ajouter. Les autres en-têtes sont en lecture seule, ce qui signifie que les fonctions peuvent les lire mais ne peuvent pas les ajouter ou les modifier.

Rubriques

- En-têtes non autorisés
- En-têtes en lecture seule

En-têtes non autorisés

Les en-têtes HTTP suivants ne sont pas exposés aux fonctions périphériques, et les fonctions ne peuvent pas les ajouter. Si votre fonction ajoute l'un de ces en-têtes, la CloudFront validation échoue et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

- Connection
- Expect
- Keep-Alive
- Proxy-Authenticate
- Proxy-Authorization
- Proxy-Connection
- Trailer
- Upgrade
- X-Accel-Buffering
- X-Accel-Charset
- X-Accel-Limit-Rate
- X-Accel-Redirect
- X-Amz-Cf-*
- X-Amzn-Auth
- X-Amzn-Cf-Billing
- X-Amzn-Cf-Id
- X-Amzn-Cf-Xff
- X-Amzn-Errortype
- X-Amzn-Fle-Profile
- X-Amzn-Header-Count
- X-Amzn-Header-Order
- X-Amzn-Lambda-Integration-Tag
- X-Amzn-RequestId
- X-Cache
- X-Edge-*
- X-Forwarded-Proto
- X-Real-IP

En-têtes en lecture seule

Les en-têtes suivants sont en lecture seule. Votre fonction peut les lire et les utiliser comme entrée de la logique de la fonction, mais elle ne peut pas modifier les valeurs. Si votre fonction ajoute ou modifie un en-tête en lecture seule, la demande échoue à la CloudFront validation et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

En-têtes en lecture seule pour les événements de demande de l'utilisateur

Les en-têtes suivants sont en lecture seule dans les événements de demande de l'utilisateur.

- `Content-Length`
- `Host`
- `Transfer-Encoding`
- `Via`

En-têtes en lecture seule dans les événements de demande d'origine (Lambda@Edge uniquement)

Les en-têtes suivants sont en lecture seule dans les événements de demande d'origine, qui n'existent que dans Lambda@Edge.

- `Accept-Encoding`
- `Content-Length`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Transfer-Encoding`
- `Via`

En-têtes en lecture seule dans les événements de réponse d'origine (Lambda@Edge uniquement)

Les en-têtes suivants sont en lecture seule dans les événements de réponse d'origine, qui n'existent que dans Lambda@Edge.

- `Transfer-Encoding`

- `Via`

En-têtes en lecture seule dans les événements de réponse de l'utilisateur

Les en-têtes suivants sont en lecture seule dans les événements de réponse du visualiseur pour Functions CloudFront et Lambda @Edge.

- `Warning`
- `Via`

Les en-têtes suivants sont en lecture seule dans les événements de réponse d'utilisateur pour Lambda@Edge.

- `Content-Length`
- `Content-Encoding`
- `Transfer-Encoding`

Chaînes de requête

Les restrictions suivantes s'appliquent aux fonctions qui lisent, mettent à jour ou créent une chaîne de requête dans un URI de demande.

- (Lambda@Edge uniquement) Pour accéder à la chaîne de requête dans une fonction de demande de l'origine ou de réponse de l'origine, votre stratégie de cache ou stratégie de demande de l'origine doit être définie sur Toutes pour Chaînes de requête.
- Une fonction peut créer ou mettre à jour une chaîne de requête pour les événements de demande de l'utilisateur et de demande de l'origine (les événements de demande de l'origine n'existent que dans Lambda@Edge).
- Une fonction peut lire une chaîne de requête, mais ne peut pas en créer ou en mettre à jour, pour les événements de réponse de l'origine et de réponse de l'utilisateur (les événements de réponse de l'origine n'existent que dans Lambda@Edge).
- Si une fonction crée ou met à jour une chaîne de requête, les restrictions suivantes s'appliquent :
  - La chaîne de requête mise à jour ne peut pas inclure des espaces, des caractères de contrôle ou l'identificateur de fragment (#).
  - La taille totale de l’URI, comprenant la chaîne de requête, doit être inférieure à 8 192 caractères.

- Nous vous recommandons d'utiliser l'encodage de pourcentage pour l'URI et la chaîne de requête. Pour plus d'informations, consultez Encodage de l'URI et de la chaîne de requête.

URI

Si une fonction modifie l'URI pour une demande, cela ne modifie pas le comportement du cache pour la demande ou l'origine vers laquelle la demande est transférée.

La taille totale de l'URI, comprenant la chaîne de requête, doit être inférieure à 8 192 caractères.

Encodage de l'URI et de la chaîne de requête

Les valeurs de chaîne de requête et de l'URI transmises aux fonctions périphériques sont codées en UTF-8. Votre fonction doit utiliser l'encodage UTF-8 pour les valeurs d'URI et de chaîne de requête qu'elle renvoie. L'encodage de pourcentage est compatible avec l'encodage UTF-8.

La liste suivante explique comment CloudFront gérer le codage des valeurs d'URI et de chaîne de requête :

- Lorsque les valeurs de la requête sont codées en UTF-8, CloudFront elles sont transmises à votre fonction sans les modifier.
- Lorsque les valeurs de la demande sont codées ISO-8859-1, CloudFront convertit les valeurs en codage UTF-8 avant de les transmettre à votre fonction.
- Lorsque les valeurs de la demande sont codées à l'aide d'un autre codage de caractères, CloudFront suppose qu'elles sont codées ISO-8859-1 et essaie de les convertir de l'ISO-8859-1 en UTF-8.

> **Important**
>
> Les caractères convertis peuvent résulter d'une interprétation inexacte des valeurs de la demande de l'origine. Cela peut conduire votre fonction ou votre origine à produire un résultat indésirable.

Les valeurs d'URI et de chaîne de CloudFront requête qui sont transmises à votre origine dépendent de la modification des valeurs par une fonction :

- Si une fonction ne modifie pas l'URI ou la chaîne de requête, elle CloudFront transmet les valeurs qu'elle a reçues dans la demande à votre origine.

- Si une fonction modifie l'URI ou la chaîne de requête, elle CloudFront transmet les valeurs codées en UTF-8.

Microsoft Smooth Streaming

Vous ne pouvez pas utiliser les fonctions Edge avec une CloudFront distribution que vous utilisez pour diffuser des fichiers multimédia que vous avez transcodés au format Microsoft Smooth Streaming.

Identification

Vous ne pouvez pas ajouter de balises aux fonctions périphériques. Pour en savoir plus sur le balisage CloudFront, voirMarquer une distribution.

Restrictions relatives aux CloudFront fonctions

Les restrictions suivantes s'appliquent uniquement aux CloudFront fonctions.

Pour plus d'informations sur les quotas (anciennement appelés limites), consultezQuotas relatifs aux CloudFront fonctions.

Journaux

Les journaux de CloudFront fonctions dans Functions sont tronqués à 10 Ko.

Corps de la demande

CloudFront Les fonctions ne peuvent pas accéder au corps de la requête HTTP.

AWS Security Token Service Points de terminaison régionaux lors de l'utilisation de l'API CloudFront KeyValueStore

Lorsque vous appelez l'CloudFront KeyValueStore API à l'aide de Signature Version 4A (SigV4A) avec des informations d'identification de sécurité temporaires, par exemple, lorsque vous utilisez des rôles AWS Identity and Access Management (IAM), assurez-vous de demander les informations d'identification temporaires à un point de terminaison régional dans. AWS STS Si vous utilisez le point de terminaison global pour AWS STS (`sts.amazonaws.com`), AWS STS cela générera des informations d'identification temporaires à partir d'un point de terminaison global, ce qui n'est pas

pris en charge par SIGv4a. Par conséquent, vous recevrez un message d'erreur d'authentification. Pour résoudre ce problème, utilisez l'un des points de terminaison régionaux répertoriés AWS STS dans le guide de l'utilisateur IAM. Si vous configurez le protocole SAML pour utiliser des points de terminaison AWS STS régionaux, consultez le billet de blog Comment utiliser les points de terminaison SAML régionaux pour le basculement.

Environnement d’exécution

L'environnement d'exécution CloudFront Functions ne prend pas en charge l'évaluation dynamique du code et restreint l'accès au réseau, au système de fichiers et aux minuteries. Pour plus d’informations, consultez Fonctions limitées.

> **Note**
>
> Pour être utilisée CloudFront KeyValueStore, votre CloudFront fonction doit utiliser le JavaScript runtime 2.0.

Utilisation du calcul

CloudFront Le temps d'exécution des fonctions est limité, mesuré en termes d'utilisation du calcul. L'utilisation du calcul est un nombre compris entre 0 et 100 qui indique la durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une utilisation du calcul de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé.

Lorsque vous testez une fonction, la valeur d'utilisation du calcul figure dans la sortie de l'événement test. Pour les fonctions de production, vous pouvez consulter la métrique d'utilisation du calcul sur la page Surveillance de la CloudFront console ou dans CloudWatch.

Restrictions sur Lambda@Edge

Les restrictions suivantes s'appliquent uniquement à Lambda@Edge.

Pour obtenir des informations sur les quotas, veuillez consulter Quotas sur Lambda@Edge.

Résolution DNS

CloudFront effectue une résolution DNS sur le nom de domaine d'origine avant d'exécuter la fonction Lambda @Edge de votre demande d'origine. Si le service DNS de votre domaine rencontre des

problèmes et ne CloudFront parvient pas à résoudre le nom de domaine pour obtenir l'adresse IP, votre fonction Lambda @Edge ne sera pas invoquée. CloudFrontrenverra un code d'état HTTP 502 (Bad Gateway) au client. Pour plus d'informations, consultez Erreur DNS (`NonS3OriginDnsError`).

Pour plus d'informations sur la gestion du basculement DNS, consultez la section Configuration du basculement DNS dans le manuel Amazon Route 53 Developer Guide.

Codes d'état HTTP

Les fonctions Lambda @Edge pour les événements de réponse du spectateur ne peuvent pas modifier le code d'état HTTP de la réponse, que la réponse provienne de l'origine ou du CloudFront cache.

Version de la fonction Lambda

Vous devez utiliser une version numérotée de la fonction Lambda, et non `$LATEST` ou des alias.

Région de Lambda

La fonction Lambda doit résider dans la région USA Est (Virginie du Nord).

Autorisations de rôle Lambda

Le rôle d'exécution IAM associé à la fonction Lambda doit autoriser les principaux de service `lambda.amazonaws.com` et `edgelambda.amazonaws.com` à endosser le rôle. Pour plus d'informations, consultez Configuration des autorisations et des rôles IAM pour Lambda @Edge.

Fonctionnalités de Lambda

Les fonctionnalités Lambda suivantes ne sont pas prises en charge par Lambda@Edge :

- Configurations de gestion d'exécution Lambda autres que Auto (par défaut)
- Configuration de votre fonction Lambda pour accéder aux ressources de votre VPC
- files d'attente de lettres mortes de la fonction Lambda
- Variables d'environnement Lambda (à l'exception des variables d'environnement réservées, qui sont automatiquement prises en charge)
- Fonctions Lambda avec couches AWS Lambda
- Utilisation de AWS X-Ray

- Simultanéité allouée Lambda

> **Note**
>
> Les fonctions Lambda @Edge ont les mêmes capacités de simultanéité régionale que les fonctions Lambda. Toutefois, lorsque le quota est augmenté pour les exécutions simultanées de Lambda @Edge, il est augmenté pour tous les Régions AWS endroits où la fonction Lambda @Edge est répliquée. Pour plus d'informations, consultez Quotas sur Lambda@Edge.

- Fonctions Lambda définies sous forme d'images de conteneurs
- Fonctions Lambda utilisant l'architecture arm64
- Lambda fonctionne avec plus de 512 Mo de stockage éphémère
- Capture des journaux de fonctions Lambda au format structuré JSON
- Contrôle de la granularité des journaux des fonctions Lambda
- Définition du groupe de CloudWatch journaux Amazon auquel Lambda envoie les journaux

Environnements d'exécution pris en charge

Lambda@Edge prend en charge les fonctions Lambda avec les environnements d'exécution suivants :

Node.js	Python
• Node.js 20 • Node.js 18 • Node.js 16[1] • Node.js 14m[2] • Node.js 12[2] • Node.js 10[2] • Node.js 8m[2] • Node.js 6m[2]	• Python 3.12 • Python 3.11 • Python 3.10 • Python 3.9 • Python 3.8 • Python 3.7

[1] Cette version de Node.js est arrivée à expiration et sera bientôt déconseillée par. AWS Lambda

[2]Cette version de Node.js est arrivée en fin de vie et est totalement obsolète par. AWS Lambda

Vous ne pouvez pas créer ou mettre à jour des fonctions avec des versions obsolètes de Node.js. Vous ne pouvez associer les fonctions existantes à ces versions qu'à des CloudFront distributions. Les fonctions associées à ces versions et associées à des distributions continueront de s'exécuter. Toutefois, nous vous recommandons de déplacer votre fonction vers des versions plus récentes de Node.js. Pour plus d'informations, consultez la politique de dépréciation des environnements d'exécution dans le guide du AWS Lambda développeur et le calendrier de publication de Node.js sur. GitHub

> **Tip**
>
> Il est recommandé d'utiliser les dernières versions des environnements d'exécution fournis pour améliorer les performances et créer de nouvelles fonctionnalités.

CloudFronten-têtes

Les fonctions Lambda @Edge peuvent lire, modifier, supprimer ou ajouter n'importe lequel des CloudFront en-têtes répertoriés dans. Ajouter des en-têtes de CloudFront demande

> **Remarques**
>
> - Si vous CloudFront souhaitez ajouter ces en-têtes, vous devez les configurer CloudFront pour les ajouter à l'aide d'une politique de cache ou d'une politique de demande d'origine.
> - CloudFront ajoute les en-têtes après l'événement de demande de visualisation, ce qui signifie que les en-têtes ne sont pas disponibles pour les fonctions Lambda @Edge dans une demande de visualisation. Les en-têtes ne sont disponibles que pour les fonctions Lambda @Edge dans une demande d'origine et une réponse d'origine.
> - Si la demande du lecteur inclut des en-têtes portant ces noms et que vous avez configuré pour ajouter ces en-têtes CloudFront à l'aide d'une politique de cache ou d'une politique de demande d'origine, les valeurs d'en-tête CloudFront figurant dans la demande du lecteur sont alors remplacées. Les fonctions orientées vers le spectateur voient la valeur d'en-tête de la demande du lecteur, tandis que les fonctions orientées vers l'origine voient la valeur d'en-tête ajoutée. CloudFront

- Si une fonction de demande d'affichage ajoute l'`CloudFront-Viewer-Country`en-tête, elle échoue à la validation et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

Restrictions relatives au corps de la requête avec l'option Inclure le corps

Lorsque vous choisissez l'option Include Body (Inclure le corps) pour exposer le corps de la requête à votre fonction Lambda@Edge, les informations et les quotas de taille suivants s'appliquent aux parties du corps qui sont exposées ou remplacées.

- CloudFront base64 code toujours le corps de la requête avant de l'exposer à Lambda @Edge.
- Si le corps de la requête est volumineux, CloudFront tronquez-le avant de l'exposer à Lambda @Edge, comme suit :
  - Pour les événements de requête d'utilisateur, le corps est tronqué à 40 Ko.
  - Pour les événements de requête de l'origine, le corps est tronqué à 1 Mo.
- Si vous accédez au corps de la demande en lecture seule, CloudFront envoie le corps de la demande d'origine complet à l'origine.
- Si votre fonction Lambda@Edge remplace le corps de la requête, les quotas de taille suivantes s'appliquent au corps que la fonction renvoie :
  - Si la fonction Lambda@Edge renvoie le corps en texte brut :
    - Pour les événements de requête d'utilisateur, le corps est tronqué à 40 Ko.
    - Pour les événements de requête de l'origine, le corps est tronqué à 1 Mo.
  - Si la fonction Lambda@Edge renvoie le corps en tant que texte codé base64 :
    - Pour les événements de requête d'utilisateur, le corps est tronqué à 53,2 Ko.
    - Pour les événements de requête de l'origine, le corps est tronqué à 1,33 Mo.

Délai de réponse et délai de maintien en vie (origines personnalisées uniquement)

Si vous utilisez les fonctions Lambda @Edge pour définir le délai de réponse ou le délai de maintien en vie pour les origines de votre distribution, vérifiez que vous spécifiez une valeur que votre origine peut prendre en charge. Pour plus d'informations, voir Quotas de délai de réponse et de maintien en vie.

Rapports, métriques et journaux

CloudFront propose plusieurs options pour la création de rapports, le suivi et la journalisation de vos CloudFront ressources :

- Vous pouvez consulter et télécharger des rapports pour connaître l'utilisation et l'activité de vos CloudFront distributions, notamment les rapports de facturation, les statistiques du cache, le contenu populaire et les principaux référents.
- Vous pouvez surveiller et suivre CloudFront, y compris vos fonctions informatiques de pointe, directement dans la CloudFront console ou en utilisant Amazon CloudWatch. CloudFront envoie diverses métriques à des distributions et CloudWatch à des fonctions de périphérie, à la fois Lambda @Edge et CloudFront Functions.
- Vous pouvez consulter les journaux des demandes des utilisateurs que vos CloudFront distributions reçoivent à l'aide de journaux standard ou de journaux en temps réel. Outre les journaux des demandes des utilisateurs, vous pouvez utiliser CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Vous pouvez également l'utiliser AWS CloudTrail pour obtenir des journaux de l'activité de l' CloudFront API dans votre Compte AWS.
- Vous pouvez suivre les modifications de configuration apportées à vos CloudFront ressources à l'aide de AWS Config.

Pour plus d'informations sur ces fonctions, consultez les rubriques suivantes.

Rubriques

AWS rapports de facturation et d'utilisation pour CloudFront

AWS fournit deux rapports d'utilisation pour CloudFront :

- Le rapport AWS de facturation est une vue d'ensemble de toutes les activités Services AWS que vous utilisez, y compris CloudFront.
- Le rapport AWS d'utilisation est un résumé de l'activité d'un service spécifique, agrégé par heure, jour ou mois. Il inclut également des tableaux d'utilisation qui fournissent une représentation graphique de votre CloudFront utilisation.

> **Note**
>
> Comme les autres Services AWS, il ne vous CloudFront facture que ce que vous utilisez. Pour en savoir plus, consultez CloudFront Tarification.

Rubriques

Consultez le rapport AWS de facturation pour CloudFront

Vous pouvez consulter un résumé de votre AWS consommation et de vos frais, listé par service, sur la page Factures de la AWS Billing and Cost Management console.

Pour consulter le rapport AWS de facturation

1. Connectez-vous à la AWS Billing console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/billing/.
2. Dans le volet de navigation, choisissez Factures.
3. Choisissez une Période de facturation (par exemple, août 2023).
4. Dans l'onglet Frais par service, choisissez CloudFront, puis développez Global ou le Région AWS nom.
5. Pour télécharger un rapport de facturation détaillé au format CSV, choisissez Tout télécharger au format CSV.

Pour plus d'informations sur votre AWS facture, consultez la section Consulter votre facture dans le Guide de AWS Billing l'utilisateur.

Le rapport de facturation inclut les valeurs suivantes qui s'appliquent à CloudFront :

- ProductCode – `AmazonCloudFront`
- UsageType— L'une des valeurs suivantes :
  - Code qui identifie le type de transfert de données
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- ItemDescription— Une description du taux de facturation pour le UsageType.
- UsageStart Date et UsageEndDate— Le jour auquel l'utilisation s'applique, en temps universel coordonné (UTC).
- UsageQuantity— L'une des valeurs suivantes :
  - Nombre de requêtes au cours de la période spécifiée
  - Quantité de données transférée en gigaoctets
  - Nombre d’objets invalidés
  - Somme des mois au prorata pendant lesquels vous avez associé des certificats SSL aux CloudFront distributions activées. Si vous avez, par exemple, un certificat associé à une distribution activée pendant un mois tout entier et un autre certificat associé à une distribution activée pendant la moitié du mois, cette valeur sera 1,5.

Consultez le rapport AWS d'utilisation pour CloudFront

AWS fournit un rapport CloudFront d'utilisation plus détaillé que le rapport de facturation mais moins détaillé que les journaux CloudFront d'accès. Le rapport d’utilisation offre des totaux de données d’utilisation par heure, jour ou mois et répertorie les opérations par région et type d’utilisation, par exemple les données transférées hors de la région Australie.

Pour consulter le rapport AWS d'utilisation

1. Connectez-vous à la AWS Billing console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/billing/.

2. Dans le volet de navigation, sélectionnez Cost & Reports.
3. Dans la section Rapport AWS d'utilisation, choisissez Créer un rapport d'utilisation.
4. Sur la page Télécharger le rapport d'utilisation, sous Services, sélectionnez Amazon CloudFront
5. Choisissez le type d'utilisation.
6. Choisissez l'opération.
7. Choisissez la période du rapport. Si vous choisissez Plage de dates personnalisée, vous devez spécifier manuellement la plage de dates pour le rapport.
8. Sous Granularité du rapport, sélectionnez Horaire, Quotidien ou Mensuel.
9. Choisissez Télécharger, puis sélectionnez Rapport XML ou Rapport CSV.

Pour plus d'informations sur le rapport AWS d'utilisation, voir Rapport AWS d'utilisation dans le guide de Exportations de données AWS l'utilisateur.

Le rapport CloudFront d'utilisation inclut les valeurs suivantes :

- Service – `AmazonCloudFront`
- Opération : méthode HTTP. Les valeurs incluent `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST` et `PUT`.
- UsageType— L'une des valeurs suivantes :
  - Code qui identifie le type de transfert de données
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- Ressource : ID de la CloudFront distribution associée à l'utilisation ou ID de certificat d'un certificat SSL que vous avez associé à une CloudFront distribution.
- StartTime/EndTime— Le jour auquel l'utilisation s'applique, en temps universel coordonné (UTC).
- UsageValue— 1) Le nombre de demandes pendant la période spécifiée ou 2) la quantité de données transférées en octets.

Si vous utilisez Amazon S3 comme source CloudFront, pensez également à exécuter le rapport d'utilisation pour Amazon S3. Toutefois, si vous utilisez Amazon S3 à des fins autres que l'origine de vos CloudFront distributions, il est possible que la partie qui s'applique à votre CloudFront utilisation ne soit pas claire.

> **Tip**
>
> Pour obtenir des informations détaillées sur chaque demande CloudFront reçue pour vos objets, activez les journaux CloudFront d'accès pour votre distribution. Pour plus d'informations, consultez the section called “Utilisation des journaux standard (journaux d'accès)”.

Pour plus d'informations sur la compréhension des CloudFront frais et des types d'utilisation figurant dans vos rapports, consultezthe section called “Interprétez votre AWS facture et vos rapports d'utilisation pour CloudFront”.

Interprétez votre AWS facture et vos rapports d'utilisation pour CloudFront

Une fois que vous avez le rapport de facturation et le rapport d'utilisation, vous pouvez utiliser cette rubrique pour comprendre comment interpréter chaque CloudFront charge figurant sur votre facture et le type d'utilisation correspondant à chaque charge. Cette rubrique inclut les codes et les Région AWS abréviations qui peuvent apparaître sur les deux rapports.

La plupart des codes des deux colonnes comportent une abréviation à deux lettres qui indique l'emplacement de l'activité. Dans le tableau suivant, *`la région`* d'un code est remplacée dans votre AWS facture et dans le rapport d'utilisation par l'une des abréviations à deux lettres suivantes :

- AP : Hong Kong, Philippines, Corée du Sud, Taïwan, et Singapour (Asie-Pacifique)
- AU : Australie
- CA : Canada
- UE : Europe et Israël
- IN : Inde
- JP : Japon
- ME : Moyen-Orient
- SA : Amérique du Sud

- US : États-Unis
- ZA : Afrique du Sud

Pour plus d'informations sur la tarification par Région AWS, consultez la section CloudFront Tarification Amazon.

> **Remarques**
>
> - Ce tableau n'inclut pas les frais liés au transfert de vos objets d'un compartiment Amazon S3 vers des emplacements CloudFront périphériques. Le cas échéant, ces frais apparaissent dans la section Transfert de données AWS de votre facture AWS .
> - La première colonne répertorie les frais qui apparaissent dans votre rapport de AWS facturation et explique ce que chacun signifie.
> - La deuxième colonne répertorie les éléments qui apparaissent dans le rapport AWS d'utilisation et indique la corrélation entre les frais de facturation et les éléments du rapport d'utilisation.

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
région - DataTransfer -Out-Bytes Nombre total d'octets servis depuis des emplacements CloudFront périphériques de *la région* en réponse à des utilisateurs `GET` et à des `HEAD` demandes.	*région*-Out-Bytes-HTTP-Static : octets diffusés via HTTP pour des objets avec une durée de vie ≥ 3 600 secondes. *région*-Out-Bytes-HTTPS-Static : octets diffusés via HTTPS pour des objets avec une durée de vie ≥ 3 600 secondes. *région*-Out-Bytes-HTTP-Dynamic : octets diffusés via HTTP pour des objets avec une durée de vie < 3 600 secondes. *région*-Out-Bytes-HTTPS-Dynamic :

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
	octets diffusés via HTTPS pour des objets avec une durée de vie < 3 600 secondes. *région*-Out-OBytes-HTTP-Proxy Octets CloudFront renvoyés par les utilisateurs via HTTP en réponse à DELETEOPTIONS,PATCH,POST, et PUT demandes. *région*-Out-OBytes-HTTPS-Proxy Octets CloudFront renvoyés par les utilisateurs via HTTPS en réponse à DELETEOPTIONS,PATCH,POST, et PUT demandes.
région - DataTransfer -Out-Obytes Nombre total d'octets transférés depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou de périphérie en réponse àDELETE,OPTIONS, PATCHPOST, et à des PUT demandes. Les frais incluent le transfert de WebSocket données du client au serveur.	*région*-Out-OBytes-HTTP-Proxy Nombre total d'octets transférés via HTTP depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou de périphérie en réponse àDELETE,OPTIONS, PATCHPOST, et à des PUT demandes. *région*-Out-OBytes-HTTPS-Proxy Nombre total d'octets transférés via HTTPS depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou de périphérie en réponse àDELETE,OPTIONS, PATCHPOST, et à des PUT demandes.

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
région-Requests-Tier1 Nombre de requêtes HTTP `GET` et `HEAD`	*région*-Requests-HTTP-Static Nombre de requêtes HTTP `GET` et `HEAD` diffusées pour des objets avec une durée de vie ≥ 3600 secondes *région*-Requests-HTTP-Dynamic Nombre de requêtes HTTP `GET` et `HEAD` diffusées pour des objets avec une durée de vie < 3600 secondes
région-Requests-Tier2-HTTPS Nombre de requêtes HTTPS `GET` et `HEAD`	*région*-Requests-HTTPS-Static Nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie ≥ 3600 secondes *région*-Requests-HTTPS-Dynamic Nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie < 3600 secondes
région-Requests-HTTP-Proxy Nombre de `PUT` requêtes HTTP `DELETEOPTIONS`,`PATCH`,`POST`, et transmises à CloudFront votre fonction d'origine ou de périphérie. Inclut également le nombre de WebSocket requêtes HTTP (`GET`demandes avec `Upgrade: websocket` en-tête) qui sont transmises CloudFront à votre fonction d'origine ou de périphérie.	*région*-Requests-HTTP-Proxy Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
région-Requests-HTTPS-Proxy Nombre de HTTPS`DELETE`,,`OPTIONS`, `PATCH`, `POST`et de `PUT` requêtes qui sont CloudFront redirigées vers votre fonction d'origine ou de périphérie. Inclut également le nombre de WebSocket requêtes HTTPS (`GET`demandes avec `Upgrade: websocket` en-tête) qui sont transmises CloudFront à votre fonction d'origine ou de périphérie.	*région*-Requests-HTTPS-Proxy Identique à l'article correspondant sur votre CloudFront facture.
région-Requests-HTTPS-Proxy-FLE Nombre de `POST` requêtes HTTPS`DELETE`, `OPTIONS`, `PATCH`, et traitées avec un chiffrement au niveau du champ qui est redirigé CloudFront vers votre fonction d'origine ou de périphérie.	*région*-Requests-HTTPS-Proxy-FLE Identique à l'article correspondant sur votre CloudFront facture.
région -Bytes- OriginShield Nombre total d'octets transférés de l'origine vers n'importe quel cache périphérique régional, y compris le cache périphérique régional activé en tant que Origin Shield.	*région* -Bytes- OriginShield Identique à l'article correspondant sur votre CloudFront facture.
région -OBytes- OriginShield Nombre total d'octets transférés vers l'origine depuis n'importe quel cache périphérique régional, y compris le cache périphérique régional activé en tant que Origin Shield.	*région* -OBytes- OriginShield Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
région -Demandes- OriginShield Nombre de requêtes envoyées à Origin Shield sous forme de couche progressive. Pour les demandes dynamiques (ne pouvant pas être mises en cache) qui sont transmises par proxy à l'origine, Origin Shield est toujours une couche incrémentielle. Pour les requêtes pouvant être mises en cache, Origin Shield est parfois une couche progressive. Pour plus d'informations, consultez the section called "Estimation des frais liés à Origin Shield".	*région* -Demandes- OriginShield Identique à l'article correspondant sur votre CloudFront facture.
Invalidations Les frais d'invalidation d'objets (retrait des objets des zones CloudFront périphériques). Pour plus d'informations, consultez Payer pour l'invalidation du fichier.	Invalidations Identique à l'article correspondant sur votre CloudFront facture.
SSL-Cert-Custom Les frais d'utilisation d'un certificat SSL avec un CloudFront autre nom de domaine tel que exemple.com au lieu d'utiliser le certificat CloudFront SSL par défaut et le nom de domaine CloudFront attribué à votre distribution.	SSL-Cert-Custom Identique à l'article correspondant sur votre CloudFront facture.
RealTimeLog-KinesisDataStream Le tarif correspondant au nombre de lignes générées pour les journaux en temps réel.	RealTimeLog-KinesisDataStream Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
Exécutions- CloudFrontFunctions Le montant correspondant au nombre d'invocations de CloudFront fonctions.	Exécutions- CloudFrontFunctions Identique à l'article correspondant sur votre CloudFront facture.
***région* -Lambda-Edge** - Demande Le montant correspondant au nombre d'appels de fonctions Lambda @Edge.	***région* -Lambda-Edge** - Demande Identique à l'article correspondant sur votre CloudFront facture.
***région* -Lambda-Edge-GB-Second** Les frais pour la durée comprise entre le moment où votre fonction Lambda @Edge est invoquée et le moment où elle revient ou s'arrête.	***région* -Lambda-Edge-GB-Second** Identique à l'article correspondant sur votre CloudFront facture.
KeyValueStore-EdgeReads Les frais correspondant au nombre d'appels de lecture vers les CloudFront KeyValueStoreméthodes`get()`,`exists()`, et`meta()`. Pour plus d'informations, consultez Méthodes d'aide pour les magasins de clés-valeurs.	KeyValueStore-EdgeReads Identique à l'article correspondant sur votre CloudFront facture.
KeyValueStore- Opérations de l'API Le montant correspondant au nombre d'appels à l'CloudFront KeyValueStoreAPI.	KeyValueStore- Opérations de l'API Identique à l'article correspondant sur votre CloudFront facture.

Afficher CloudFront les rapports dans la console

Vous pouvez consulter les rapports suivants relatifs à votre CloudFront activité dans la console :

Rubriques

- Afficher les rapports statistiques du CloudFront cache

- Afficher les rapports sur les objets CloudFront populaires
- Afficher les rapports sur CloudFront les principaux référents
- Afficher les rapports CloudFront d'utilisation
- Afficher les rapports des CloudFront spectateurs

La plupart de ces rapports sont basés sur les données des journaux CloudFront d'accès, qui contiennent des informations détaillées sur chaque demande d'utilisateur CloudFront reçue. Vous n'avez pas besoin d'activer les journaux d'accès pour afficher les rapports. Pour plus d'informations, consultez Configuration et utilisation des journaux standard (journaux d'accès).

Afficher les rapports statistiques du CloudFront cache

Le rapport sur les statistiques du CloudFront cache Amazon inclut les informations suivantes :

- Total Requests (Nombre total de requêtes) – Présente le nombre total de requêtes pour tous les codes d'état HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, GET, HEAD ou POST).
- Pourcentage de demandes des spectateurs par type de résultat : affiche les résultats positifs, ratés et erreurs sous forme de pourcentage du nombre total de demandes des spectateurs pour la CloudFront distribution sélectionnée.
- Bytes Transferred to Viewers (Nombre d'octets transférés aux utilisateurs) – Indique le nombre total d'octets et le nombre d'octets des échecs.
- HTTP Status Codes (Codes d'état HTTP) – Présente les requêtes des utilisateurs par code d'état HTTP.
- Percentage of GET Requests that Didn't Finish Downloading (Pourcentage de requêtes GET qui n'ont pas terminé le téléchargement) – Présente, sous la forme d'un pourcentage du nombre total de requêtes, les requêtes utilisateur GET qui n'ont pas terminé de télécharger l'objet demandé.

Les données de ces statistiques proviennent de la même source que les journaux CloudFront d'accès, mais il n'est pas nécessaire d'activer la journalisation des accès pour consulter les statistiques du cache.

Vous pouvez afficher des graphiques pour une plage de dates donnée au cours des 60 derniers jours, avec des points de données chaque heure ou chaque jour. Vous pouvez généralement consulter les données relatives aux demandes CloudFront reçues il y a à peine une heure, mais les données peuvent parfois être retardées de 24 heures.

Rubriques

Afficher les rapports statistiques du CloudFront cache dans la console

Vous pouvez consulter le rapport des statistiques du CloudFront cache dans la console.

Pour consulter les statistiques CloudFront du cache

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Cache Statistics.
3. Dans le volet Rapports de statistiques du CloudFront cache, pour Date de début et Date de fin, sélectionnez la plage de dates pour laquelle vous souhaitez afficher les graphiques des statistiques du cache. Les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n'importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n'est pas possible de spécifier un point de données par heure.
5. Pour Viewer Location (Emplacement de l'utilisateur), choisissez le continent d'où proviennent les requêtes des utilisateurs ou bien All Locations (Tous les emplacements). Les graphiques de statistiques du cache incluent les données relatives aux demandes CloudFront reçues depuis l'emplacement spécifié.
6. Dans la liste Distribution, sélectionnez les distributions pour lesquelles vous voulez afficher des données dans les graphiques d'utilisation :

- Une distribution individuelle : les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution affiche l'ID de distribution et, le cas échéant, les noms de domaines alternatifs (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste indique les noms de domaines d'origine pour la distribution.
- Toutes les distributions : les graphiques affichent les données sommées pour toutes les distributions associées au AWS compte courant, à l'exception des distributions que vous avez supprimées.

7. Choisissez Mettre à jour.

Pour afficher les données d'un point de données quotidien ou horaire dans un graphique, survolez le point de données avec le pointeur de la souris.

Pour les graphiques qui indiquent les données transférées, notez bien que vous pouvez changer le dimensionnement vertical afin d'afficher des giga-octets, des méga-octets ou des kilo-octets pour chaque graphique.

Télécharger les données au format CSV

Vous pouvez télécharger le rapport de statistiques sur la mise en cache au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport de statistiques sur la mise en cache au format CSV

1. Lorsque vous consultez le rapport sur les statistiques du cache, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

ViewerLocation

Le continent duquel proviennent les requêtes des utilisateurs ou ALL, si vous avez choisi de télécharger le rapport pour tous les emplacements.

Données du rapport de statistiques sur la mise en cache

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

ViewerLocation

Le continent duquel proviennent les requêtes des utilisateurs ou ALL, si vous avez choisi de télécharger le rapport pour tous les emplacements.

TimeBucket

Heure du jour auquel les données s’appliquent, en heure UTC.

RequestCount

Le nombre total de requêtes pour tous les codes de statut HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, GET, HEAD ou POST).

HitCount

Nombre de demandes de visionnage pour lesquelles l'objet est traité à partir d'un cache CloudFront périphérique.

MissCount

Le nombre de demandes d'affichage pour lesquelles l'objet ne se trouve pas actuellement dans un cache périphérique et qui CloudFront doivent donc récupérer l'objet depuis votre origine.

ErrorCount

Le nombre de demandes d'affichage qui ont entraîné une erreur et qui CloudFront n'ont donc pas servi l'objet.

IncompleteDownloadCount

Le nombre de requêtes d’utilisateursqui ont commencé mais n’ont pas terminé de télécharger l’objet.

HTTP2xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 2xx (réussite).

HTTP3xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 3xx (action supplémentaire exigée).

HTTP4xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 4xx (erreur client).

HTTP5xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 5xx (erreur serveur).

TotalBytes

Nombre total d'octets fournis aux utilisateurs CloudFront en réponse à toutes les demandes pour toutes les méthodes HTTP.

BytesFromMisses

Nombre d’octets distribués aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la demande. Cette valeur est une bonne approximation des octets transférés de votre cache d'origine vers les caches CloudFront périphériques. Elle exclut toutefois les requêtes pour des objets se trouvant déjà dans le cache périphérique, mais qui ont expiré.

Comment les graphiques de statistiques du cache sont-ils liés aux données des journaux CloudFront standard (journaux d'accès)

Le tableau suivant montre comment les graphiques de statistiques du cache de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d’accès).

Total requests (Nombre total de requêtes)

Ce graphique présente le nombre total de requêtes pour tous les codes de statut HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, `GET`, `HEAD` ou `POST`). Le nombre total de requêtes illustré dans le graphique est égal au nombre total de requêtes dans les fichiers-journaux d’accès sur la même période.

Percentage of Viewer Requests by Result Type (Pourcentage des requêtes d’utilisateurs par type de résultat)

Ce graphique montre les visites, les échecs et les erreurs sous forme de pourcentage du nombre total de demandes des utilisateurs pour la CloudFront distribution sélectionnée :

- Hit : demande d'affichage pour laquelle l'objet est diffusé à partir d'un cache CloudFront périphérique. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Hit`.
- Miss — Une demande d'affichage pour laquelle l'objet ne se trouve pas actuellement dans un cache périphérique et CloudFront doit donc récupérer l'objet depuis votre origine. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Miss`.

- Erreur : demande d'affichage qui a entraîné une erreur et qui CloudFront n'a donc pas servi l'objet. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Error`, `LimitExceeded` ou `CapacityExceeded`.

Le graphique ne comprend pas les hits actualisés, c’est-à-dire les requêtes pour des objets se trouvant dans le cache périphérique mais ayant expiré. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `RefreshHit`.

Bytes Transferred to Viewers (Octets transférés aux utilisateurs)

Ce graphique indique deux valeurs :

- Nombre total d'octets : nombre total d'octets fournis aux utilisateurs CloudFront en réponse à toutes les demandes relatives à toutes les méthodes HTTP. Dans les journaux CloudFront d'accès, le nombre total d'octets est la somme des valeurs de la `sc-bytes` colonne pour toutes les demandes au cours de la même période.
- Bytes from Misses (Nombre d’octets provenant d’échecs) – Nombre d’octets servis aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la requête. Dans les journaux CloudFront d'accès, le nombre d'octets dus aux erreurs est la somme des valeurs de la `sc-bytes` colonne pour les demandes dont la valeur `x-edge-result-type` est `Miss` égale à. Cette valeur est une bonne approximation des octets transférés de votre cache d'origine vers les caches CloudFront périphériques. Elle exclut toutefois les requêtes pour des objets se trouvant déjà dans le cache périphérique, mais qui ont expiré.

Codes d’état HTTP

Ce graphique présente les requêtes des utilisateurs par code de statut HTTP. Dans les journaux CloudFront d'accès, les codes d'état apparaissent dans la `sc-status` colonne :

- 2xx – La requête a réussi.
- 3xx – Une action supplémentaire est nécessaire. Par exemple, 301 (Déplacé de façon permanente) signifie que l’objet demandé a été déplacé ailleurs.
- 4xx – Apparemment, le client a fait une erreur. Par exemple, 404 (Non trouvé) signifie que le client a demandé un objet qui est introuvable.
- 5xx – Le serveur d’origine n’a pas satisfait la demande. Par exemple, 503 (Service non disponible) signifie que le serveur d’origine n’est pas disponible actuellement.

Percentage of GET Requests that Didn't Finish Downloading (Pourcentage de requêtes GET qui n'ont pas terminé le téléchargement)

> Ce graphique présente les requêtes d'utilisateurs`GET` qui n'ont pas terminé de télécharger l'objet demandé sous la forme d'un pourcentage du nombre total de requêtes. Généralement, le téléchargement d'un objet ne se termine pas parce que l'utilisateur l'annule, par exemple, en cliquant sur un lien différent ou en fermant le navigateur. Dans les journaux CloudFront d'accès, ces demandes ont une valeur de `200` dans la `sc-status` colonne et une valeur de `Error` dans la `x-edge-result-type` colonne.

Afficher les rapports sur les objets CloudFront populaires

Consultez le rapport Amazon CloudFront Popular Objects pour découvrir les 50 objets les plus populaires pour une distribution pendant une période spécifiée au cours des 60 derniers jours. Vous pouvez également consulter les statistiques relatives à ces objets, notamment les suivantes :

- Nombre de demandes pour l'objet
- Nombre de succès et de ratés
- Hit Ratio (proportion de résultats)
- Nombre d'octets servis en cas d'échec
- Nombre total d'octets servis
- Nombre de téléchargements incomplets
- Nombre de requêtes par code d'état HTTP (2xx, 3xx, 4xx et 5xx)

Les données utilisées pour ces statistiques proviennent de la même source que les journaux CloudFront d'accès, mais il n'est pas nécessaire d'activer l'enregistrement des accès pour afficher les objets courants.

Rubriques

- Afficher CloudFront les rapports sur les objets populaires dans la console
- Comment CloudFront calcule les statistiques des objets populaires
- Télécharger les données au format CSV
- Comment les données du rapport sur les objets populaires sont liées aux données des journaux CloudFront standard (journaux d'accès)

Afficher CloudFront les rapports sur les objets populaires dans la console

Vous pouvez consulter le rapport sur les objets CloudFront populaires dans la console.

Pour afficher les objets populaires d'une CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Popular Objects.
3. Dans le volet Rapport sur CloudFront les objets populaires, pour Date de début et Date de fin, sélectionnez la plage de dates pour laquelle vous souhaitez afficher une liste des objets populaires. Vous pouvez choisir n'importe quelle période comprise dans les 60 jours qui précèdent.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous voulez afficher une liste des objets populaires.
5. Choisissez Mettre à jour.

Comment CloudFront calcule les statistiques des objets populaires

Pour obtenir un décompte précis des 50 principaux objets de votre distribution, CloudFront comptez les demandes pour tous vos objets par intervalles de 10 minutes à partir de minuit et conservez un total cumulé des 150 meilleurs objets pendant les 24 prochaines heures. (conserve CloudFront également les totaux quotidiens des 150 objets les plus populaires pendant 60 jours.)

Au bas de la liste, les objets apparaissent ou disparaissent constamment de la liste, de sorte que les totaux de ces objets sont des approximations. Les 50 objets figurant en haut de la liste de 150 objets peuvent monter ou descendre dans la liste, mais ils disparaissent rarement complètement de la liste, de sorte que les totaux de ces objets sont plus fiables.

Lorsqu'un objet disparaît de la liste des 150 principaux objets puis y figure à nouveau au cours d'une journée, CloudFront ajoute une estimation du nombre de demandes pour la période pendant laquelle l'objet était absent de la liste. Cette estimation est basée sur le nombre de requêtes reçues par le dernier objet de la liste pendant cette période.

Si l'objet figure parmi les 50 principaux objets plus tard dans la journée, les estimations du nombre de demandes CloudFront reçues alors que l'objet ne figurait pas parmi les 150 principaux objets font

généralement en sorte que le nombre de demandes figurant dans le rapport sur les objets les plus populaires dépasse le nombre de demandes qui apparaissent dans les journaux d'accès pour cet objet.

Télécharger les données au format CSV

Vous pouvez télécharger le rapport des objets populaires au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport des objets populaires au format CSV

1. Lorsque vous consultez le rapport sur les objets populaires, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Données du rapport des objets populaires

Le rapport inclut les valeurs suivantes :

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Objet

Les 500 derniers caractères de l'URL de l'objet.

RequestCount

Le nombre total de requêtes pour cet objet.

HitCount

Nombre de demandes de visionnage pour lesquelles l'objet est traité à partir d'un cache CloudFront périphérique.

MissCount

Le nombre de demandes d'affichage pour lesquelles l'objet ne se trouve pas actuellement dans un cache périphérique et qui CloudFront doivent donc récupérer l'objet depuis votre origine.

HitCountPct

La valeur de `HitCount` en pourcentage de la valeur de `RequestCount`.

BytesFromMisses

Nombre d'octets distribués aux utilisateurs pour cet objet alors que l'objet ne se trouvait pas dans le cache périphérique au moment de la demande.

TotalBytes

Nombre total d'octets fournis aux utilisateurs par CloudFront cet objet en réponse à toutes les demandes relatives à toutes les méthodes HTTP.

IncompleteDownloadCount

Le nombre de requêtes pour cet objet que les utilisateurs ont lancé sans terminer de télécharger l’objet.

HTTP2xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 2xx (réussite).

HTTP3xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 3xx (action supplémentaire exigée).

HTTP4xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 4xx (erreur client).

HTTP5xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 5xx (erreur serveur).

Comment les données du rapport sur les objets populaires sont liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les valeurs du rapport sur les objets populaires de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d’accès).

URL

Les 500 derniers caractères de l’URL employée par les utilisateurs pour accéder à l’objet.

Requêtes

Le nombre total de requêtes pour l’objet. Cette valeur correspond généralement étroitement au nombre de `GET` demandes relatives à l'objet dans les journaux CloudFront d'accès.

Hits

Nombre de demandes d'affichage pour lesquelles l'objet a été traité à partir d'un cache CloudFront périphérique. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Hit`.

Miss

Le nombre de demandes de consultation pour lesquelles l'objet ne se trouvait pas dans un cache périphérique. Vous avez donc CloudFront récupéré l'objet depuis votre origine. Dans les journaux d’accès, il s’agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Miss`.

Hit Ratio (proportion de résultats)

Valeur de la colonne Hits (Hits) en tant que pourcentage de la valeur de la colonne Requests (Requêtes).

Bytes from Misses (Octets provenant d’échecs)

Nombre d’octets distribués aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la demande. Dans les journaux CloudFront d'accès, le nombre d'octets dus aux erreurs est la somme des valeurs de la `sc-bytes` colonne pour les demandes dont la valeur `x-edge-result-type` est `Miss` égale à.

Total Bytes (Nombre total d’octets)

Nombre total d'octets transmis aux CloudFront utilisateurs en réponse à toutes les demandes relatives à l'objet pour toutes les méthodes HTTP. Dans les journaux CloudFront d'accès, le nombre total d'octets est la somme des valeurs de la `sc-bytes` colonne pour toutes les demandes au cours de la même période.

Incomplete Downloads (Téléchargements incomplets)

Le nombre de requêtes d’utilisateursqui n’ont pas terminé de téléchargé l’objet demandé. Généralement, le téléchargement d’un objet ne se termine pas, car il est annulé par l’utilisateur en cliquant sur un lien différent ou en fermant le navigateur par exemple. Dans les journaux CloudFront d'accès, ces demandes ont une valeur de `200` dans la `sc-status` colonne et une valeur de `Error` dans la `x-edge-result-type` colonne.

2xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est `2xx`, `Successful`. Dans les journaux CloudFront d'accès, les codes d'état apparaissent dans la `sc-status` colonne.

3xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `3xx`, `Redirection`. Le code de statut de type `3xx` indique qu'une action supplémentaire est exigée. Par exemple, 301 (Déplacé de façon permanente) signifie que l'objet demandé a été déplacé ailleurs.

4xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `4xx`, `Client Error`. Le code de statut de type `4xx` indique que le client aurait fait une erreur. Par exemple, 404 (Non trouvé) signifie que le client a demandé un objet qui est introuvable.

5xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `5xx`, `Server Error`. Le code de statut de type `5xx` indique que le serveur d'origine n'a pas satisfait la demande. Par exemple, 503 (Service non disponible) signifie que le serveur d'origine n'est pas disponible actuellement.

Afficher les rapports sur CloudFront les principaux référents

Le rapport sur les CloudFront principaux référents inclut les informations suivantes pour toutes les plages de dates des 60 derniers jours :

- Les 25 principaux référents (domaines des sites Web à l'origine du plus grand nombre de requêtes HTTP et HTTPS pour des objets CloudFront distribués pour votre distribution)
- Nombre de demandes provenant d'un référent
- Nombre de demandes provenant d'un référent en pourcentage du nombre total de demandes au cours de la période spécifiée

Les données du rapport sur les principaux référents proviennent de la même source que les journaux d' CloudFront accès, mais il n'est pas nécessaire d'activer la journalisation des accès pour afficher les principaux référents.

Les principaux référents peuvent être les moteurs de recherche, d'autres sites Web qui renvoient directement à vos objets ou votre propre site Web. Par exemple, s'il `https://example.com/index.html` renvoie à 10 graphiques, `example.com` est le référent pour les 10 graphiques.

> **Note**
>
> Si un utilisateur saisit une URL directement dans la ligne d'adresse d'un navigateur, il n'existe pas de référent pour l'objet demandé.

Rubriques

Afficher les rapports sur les CloudFront principaux référents dans la console

Vous pouvez consulter le rapport sur les CloudFront principaux référents dans la console.

Pour afficher les principaux référents d'une distribution CloudFront

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Top Referrers.
3. Dans le volet Rapport sur les CloudFront principaux référents, pour Date de début et Date de fin, sélectionnez la plage de dates pour laquelle vous souhaitez afficher une liste des principaux référents.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous voulez afficher une liste des principaux référents.
5. Choisissez Mettre à jour.

Comment CloudFront calcule les statistiques des meilleurs référents

Pour obtenir un décompte précis des 25 principaux référents, CloudFront comptez les demandes pour tous vos objets à intervalles de 10 minutes et conservez un total cumulé des 75 meilleurs

référents. Au bas de la liste, les référents apparaissent ou disparaissent constamment de la liste, de sorte que les totaux de ces référents sont des approximations.

Les 25 référents figurant en haut de la liste de 75 référents peuvent augmenter ou descendre dans la liste, mais ils sont rarement complètement retirés de la liste, de sorte que les totaux de ces référents sont généralement plus fiables.

Télécharger les données au format CSV

Vous pouvez télécharger le rapport sur les principaux référents au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport sur les principaux référents au format CSV

1. Lorsque vous consultez le rapport Top Referrers, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Données du rapport sur les principaux référents

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Referrer

Le nom de domaine du référent.

RequestCount

Le nombre total de requêtes en provenance du nom de domaine de la colonne `Referrer`.

RequestsPct

Le nombre de requêtes envoyées par le référent sous forme de pourcentage du nombre total de requêtes au cours de la période spécifiée.

Comment les données du rapport sur les principaux référents sont liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les valeurs du rapport Top Referrers de la CloudFront console correspondent aux valeurs des journaux d' CloudFront accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

Referrer

Le nom de domaine du référent. Dans les journaux d'accès, les référents figurent dans la colonne `cs(Referer)`.

Request Count

Le nombre total de requêtes en provenance du nom de domaine de la colonne Référent. Cette valeur correspond généralement étroitement au nombre de `GET` demandes du référent dans les journaux CloudFront d'accès.

Requête %

Le nombre de requêtes envoyées par le référent sous forme de pourcentage du nombre total de requêtes au cours de la période spécifiée. Si vous avez plus de 25 référents, vous ne pouvez pas calculer Request % (Requête %) sur la base des données de ce tableau, car la colonne Request Count (Nombre de requêtes) n'inclut pas toutes les requêtes pendant la période spécifiée.

Afficher les rapports CloudFront d'utilisation

Les rapports CloudFront d'utilisation contiennent les informations suivantes :

- Nombre de demandes — Indique le nombre total de demandes auxquelles il CloudFront est répondu depuis des emplacements périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée.
- Données transférées par protocole et données transférées par destination : les deux indiquent la quantité totale de données transférées depuis des emplacements CloudFront périphériques dans la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée. Les données sont séparées différemment, comme suit :
  - By protocol (Par protocole) — Sépare les données par protocole : HTTP ou HTTPS.
  - Par destination — Sépare les données par destination : vers vos spectateurs ou vers votre origine.

Le rapport CloudFront d'utilisation est basé sur le rapport AWS d'utilisation de CloudFront, qui ne nécessite aucune configuration particulière. Pour plus d'informations, consultez Consultez le rapport AWS d'utilisation pour CloudFront.

Vous pouvez consulter les rapports pour une plage de dates spécifiée au cours des 60 derniers jours, avec des points de données par heure ou par jour. Vous pouvez généralement consulter les données relatives aux demandes CloudFront reçues il y a à peine quatre heures, mais les données peuvent parfois être retardées de 24 heures.

Pour plus d'informations, consultez Comment les tableaux d'utilisation sont-ils liés aux données du rapport CloudFront d'utilisation.

Rubriques

Afficher les rapports CloudFront d'utilisation dans la console

Vous pouvez consulter le rapport CloudFront d'utilisation dans la console.

Pour consulter les rapports CloudFront d'utilisation

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Usage Reports.
3. Dans le volet Rapports CloudFront d'utilisation, pour Date de début et Date de fin, sélectionnez la plage de dates pour laquelle vous souhaitez afficher les graphiques d'utilisation. Les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n'importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n'est pas possible de spécifier un point de données par heure.
5. Pour Région de facturation, choisissez la région CloudFront de facturation contenant les données que vous souhaitez consulter ou choisissez Toutes les régions. Les diagrammes d'utilisation incluent les données relatives aux demandes CloudFront traitées dans des emplacements périphériques de la région spécifiée. La région dans laquelle CloudFront les demandes sont traitées peut correspondre ou non à la localisation de vos spectateurs.

Sélectionnez uniquement les régions incluses dans la classe de prix de votre distribution. Dans le cas contraire, les tableaux d'utilisation ne contiendront probablement aucune donnée. Par exemple, si vous avez choisi la classe de prix 200 pour votre distribution, les régions de facturation en Amérique du Sud et en Australie ne sont pas incluses. Par conséquent, nous ne traiterons CloudFront généralement pas vos demandes en provenance de ces régions. Pour plus d'informations sur les catégories de prix, consultez la section CloudFront tarification.

6. Dans la liste Distribution, sélectionnez les distributions pour lesquelles vous voulez afficher des données dans les graphiques d'utilisation :

   - Une distribution individuelle : les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution affiche l'ID de distribution et, le cas échéant, les noms de domaines alternatifs (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste indique les noms de domaines d'origine pour la distribution.
   - Toutes les distributions (excepté celles supprimées) – les graphiques affichent le total des données de toutes les distributions qui sont associées au compte AWS actuel, à l'exception des distributions que vous avez supprimées.
   - Toutes les distributions supprimées — Les graphiques affichent les données sommées pour toutes les distributions associées au AWS compte courant et supprimées au cours des 60 derniers jours.

7. Choisissez Mettre à jour les graphiques.

Pour afficher les données d'un point de données quotidien ou horaire dans un graphique, survolez le point de données avec le pointeur de la souris.

Pour les graphiques qui indiquent les données transférées, notez bien que vous pouvez changer le dimensionnement vertical afin d'afficher des giga-octets, des méga-octets ou des kilo-octets pour chaque graphique.

Télécharger les données au format CSV

Vous pouvez télécharger le rapport d'utilisation au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport d'utilisation au format CSV

1. Lorsque vous consultez le rapport d'utilisation, choisissez CSV.

2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport, `ALL` si le rapport concernait toutes les distributions, ou `ALL_DELETED` si le rapport concernait toutes les distributions supprimées.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

BillingRegion

Le continent duquel proviennent les requêtes des utilisateurs ou `ALL`, si vous avez choisi de télécharger le rapport pour toutes les régions de facturation.

Données du rapport d'utilisation

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport, `ALL` si le rapport concernait toutes les distributions, ou `ALL_DELETED` si le rapport concernait toutes les distributions supprimées.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

BillingRegion

La région CloudFront de facturation pour laquelle vous avez créé le rapport, ou`ALL`.

TimeBucket

Heure du jour auquel les données s'appliquent, en heure UTC.

HTTP

Le nombre de requêtes HTTP auxquelles on CloudFront a répondu depuis des emplacements périphériques dans la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Le nombre de `HEAD` demandes `GET` et le nombre de demandes qui CloudFront entraînent le transfert de données à vos spectateurs
- Le nombre de`DELETE`,`OPTIONS`, `PATCHPOST`, et de `PUT` demandes qui entraînent le transfert de données CloudFront vers votre origine

HTTPS

Le nombre de demandes HTTPS auxquelles on CloudFront a répondu depuis des emplacements périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Le nombre de `HEAD` demandes `GET` et le nombre de demandes qui CloudFront entraînent le transfert de données à vos spectateurs
- Le nombre de`DELETE`,`OPTIONS`, `PATCHPOST`, et de `PUT` demandes qui entraînent le transfert de données CloudFront vers votre origine

HTTPBytes

Quantité totale de données transférées via HTTP à partir d'emplacements CloudFront périphériques situés dans la région de facturation sélectionnée pendant la période de CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées CloudFront à vos spectateurs en réponse à des HEAD demandes GET et à des demandes
- Données transférées de vos spectateurs vers CloudFront les formulairesDELETE,OPTIONS, PATCHPOST, et les PUT demandes
- Données transférées CloudFront à vos spectateurs en réponse àDELETE, OPTIONSPATCH,POST, et PUT demandes

HTTPSBytes

Quantité totale de données transférées via HTTPS à partir d'emplacements CloudFront périphériques situés dans la région de facturation sélectionnée pendant la période de CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées CloudFront à vos spectateurs en réponse à des HEAD demandes GET et à des demandes
- Données transférées de vos spectateurs vers CloudFront les formulairesDELETE,OPTIONS, PATCHPOST, et les PUT demandes
- Données transférées CloudFront à vos spectateurs en réponse àDELETE, OPTIONSPATCH,POST, et PUT demandes

BytesIn

La quantité totale de données transférées depuis votre CloudFront point d'origine pourDELETE,OPTIONS,PATCH,POST, et les PUT demandes dans la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée.

BytesOut

La quantité totale de données transférées via HTTP et HTTPS CloudFront à destination de vos utilisateurs dans la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées CloudFront à vos spectateurs en réponse à des HEAD demandes GET et à des demandes
- Données transférées CloudFront à vos spectateurs en réponse àDELETE, OPTIONSPATCH,POST, et PUT demandes

Comment les tableaux d'utilisation sont-ils liés aux données du rapport CloudFront d'utilisation

La liste suivante montre comment les graphiques d'utilisation de la CloudFront console correspondent aux valeurs de la colonne Type d'utilisation du rapport CloudFront d'utilisation.

Rubriques

Nombre de requêtes

Ce graphique indique le nombre total de demandes auxquelles CloudFront répondent des emplacements périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée, séparées par protocole (HTTP ou HTTPS) et type (statique, dynamique ou proxy).

Nombre de requêtes HTTP

- *région*-Requests-HTTP-Static : nombre de requêtes HTTP `GET` et `HEAD` diffusées pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Requests-HTTP-Dynamic : nombre de requêtes HTTP `GET` et `HEAD` diffusées pour des objets avec une durée de vie < 3600 secondes.
- *region* -requests-HTTP-Proxy : nombre de requêtes HTTP`DELETE`,,, `OPTIONS` `PATCH``POST`, et `PUT` transmises à votre origine CloudFront

Nombre de requêtes HTTPS

- *région*-Requests-HTTPS-Static : nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Requests-HTTPS-Dynamic : nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie < 3600 secondes.
- *region* -requests-HTTps-Proxy : nombre de HTTPS`DELETE`,,,`OPTIONS`, et `PUT` de requêtes qui sont redirigées `PATCH` vers votre `POST` point d'origine CloudFront

Données transférées par protocole

Ce graphique montre la quantité totale de données transférées depuis les emplacements CloudFront périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée, séparée par protocole (HTTP ou HTTPS), type (statique, dynamique ou proxy) et destination (visualiseurs ou origine).

Données transférées par HTTP

- *région*-Out-Bytes-HTTP-Static : octets diffusés via HTTP pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Out-Bytes-HTTP-Dynamic : octets diffusés via HTTP pour des objets avec une durée de vie < 3600 secondes
- *region* -out-bytes-HTTP-Proxy : octets renvoyés par les utilisateurs via HTTP en réponse CloudFront à,,, et aux requêtes `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-obytes-HTTP-Proxy : nombre total d'octets transférés via HTTP depuis des emplacements CloudFront périphériques vers votre origine en réponse à,,, et demandes `DELETE` `OPTIONS` `PATCH` `POST` `PUT`

Données transférées par HTTPS

- *region*-Out-Bytes-HTTPS-Static : octets diffusés via HTTPS pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Out-Bytes-HTTPS-Dynamic : octets diffusés via HTTPS pour des objets avec une durée de vie < 3600 secondes
- *region* -out-bytes-HTTps-Proxy : octets renvoyés par les utilisateurs via HTTPS en réponse CloudFront à,,, et aux requêtes `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-obytes-HTTps-proxy : nombre total d'octets transférés via HTTPS depuis des emplacements CloudFront périphériques vers votre origine en réponse à,,, et à des demandes `DELETE` `OPTIONS` `PATCH` `POST` `PUT`

Données transférées par destination

Ce graphique montre la quantité totale de données transférées depuis les emplacements CloudFront périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée, séparée par destination (utilisateurs ou origine), protocole (HTTP ou HTTPS) et type (statique, dynamique ou proxy).

Données transférées CloudFront de vos spectateurs

- *région*-Out-Bytes-HTTP-Static : octets diffusés via HTTP pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Out-Bytes-HTTPS-Static : octets diffusés via HTTPS pour des objets avec une durée de vie ≥ 3 600 secondes
- *region*-Out-Bytes-HTTP-Dynamic : octets diffusés via HTTP pour des objets avec une durée de vie < 3600 secondes
- *region*-Out-Bytes-HTTPS-Dynamic : octets diffusés via HTTPS pour des objets avec une durée de vie < 3600 secondes
- *region* -out-bytes-HTTP-Proxy : octets renvoyés par les utilisateurs via HTTP en réponse CloudFront à,,, et aux requêtes `DELETE OPTIONS PATCH POST PUT`
- *region* -out-bytes-HTTps-Proxy : octets renvoyés par les utilisateurs via HTTPS en réponse CloudFront à,,, et aux requêtes `DELETE OPTIONS PATCH POST PUT`

Données transférées depuis votre CloudFront point d'origine

- *region* -out-obytes-HTTP-Proxy : nombre total d'octets transférés via HTTP depuis des emplacements CloudFront périphériques vers votre origine en réponse à,,, et demandes `DELETE OPTIONS PATCH POST PUT`
- *region* -out-obytes-HTTps-proxy : nombre total d'octets transférés via HTTPS depuis des emplacements CloudFront périphériques vers votre origine en réponse à,,, et à des demandes `DELETE OPTIONS PATCH POST PUT`

Afficher les rapports des CloudFront spectateurs

CloudFront Les rapports destinés aux spectateurs incluent les informations suivantes pour toutes les plages de dates des 60 derniers jours :

- Appareils — Les types d'appareils les plus fréquemment utilisés pour accéder à votre contenu (tels que les ordinateurs de bureau ou les appareils mobiles)
- Navigateurs — Les 10 navigateurs les plus fréquemment utilisés pour accéder à votre contenu (tels que Chrome ou Firefox)
- Systèmes d'exploitation : les 10 systèmes d'exploitation les plus fréquemment utilisés pour accéder à votre contenu (tels que Linux, macOS ou Windows)
- Emplacements : les 50 principaux sites (pays ou États/territoires des États-Unis) des spectateurs qui accèdent le plus fréquemment à votre contenu

- Peut également afficher les emplacements avec des points de données horaires pour toute plage de dates allant jusqu'à 14 jours au cours des 60 derniers jours

Il n'est pas nécessaire d'activer la journalisation des accès pour voir les graphiques et les rapports des utilisateurs.

Rubriques

- Afficher les graphiques et les rapports des utilisateurs dans la console
- Télécharger les données au format CSV
- Données incluses dans les rapports des spectateurs
- Comment les données du rapport sur les emplacements sont liées aux données des journaux CloudFront standard (journaux d'accès)

Afficher les graphiques et les rapports des utilisateurs dans la console

Vous pouvez consulter CloudFront les graphiques et les rapports des utilisateurs dans la console.

Pour consulter les graphiques et les rapports relatifs aux CloudFront spectateurs

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Viewers.
3. Dans le volet CloudFront Viewers, pour Date de début et Date de fin, sélectionnez la plage de dates pour laquelle vous souhaitez afficher les graphiques et les rapports des spectateurs.

   Pour le graphique Locations (Emplacements), les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n’importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. (Graphiques Browsers (Navigateurs) et Operating Systems (Systèmes d’exploitation) uniquement) Pour Grouping (Groupement), indiquez si vous souhaitez regrouper les navigateurs

et systèmes d’exploitation par nom (Chrome, Firefox) ou par nom et version (Chrome 40.0, Firefox 35.0).

5. (Graphique Locations (Emplacements) uniquement) Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n’est pas possible de spécifier un point de données par heure.
6. (Graphique Locations (Emplacements) uniquement) Pour Details (Détails), spécifiez si vous souhaitez afficher les principaux emplacements par pays ou par États américains.
7. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous souhaitez afficher des données dans les graphiques d’utilisation :

   - Une distribution individuelle : les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution (Distribution) affiche l’ID de distribution et, le cas échéant, un nom de domaine alternatif (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d’origine pour la distribution.
   - Toutes les distributions (sauf les distributions supprimées) : les graphiques affichent les données sommées pour toutes les distributions associées au AWS compte courant, à l'exception des distributions que vous avez supprimées.
8. Choisissez Mettre à jour.

Pour afficher les données d'un point de données quotidien ou horaire dans un graphique, survolez le point de données avec le pointeur de la souris.

Télécharger les données au format CSV

Vous pouvez télécharger chacun des rapports sur les utilisateurs au format CSV. Cette section explique comment télécharger les rapports et décrit les valeurs des rapports.

Pour télécharger les rapports sur les utilisateurs au format CSV

1. Lorsque vous consultez le rapport Viewer, choisissez CSV.
2. Choisissez les données à télécharger, par exemple Devices (Appareils) ou Devices Trends (Tendances des appareils).
3. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Données incluses dans les rapports des spectateurs

Les premières lignes de chaque rapport contiennent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Regroupement (rapports sur les navigateurs et les systèmes d'exploitation uniquement)

Groupement des données par nom ou par nom et version des navigateurs et systèmes d'exploitation.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

Détails (rapport sur les emplacements uniquement)

Liste des requêtes par pays ou par États américains.

Les rubriques suivantes décrivent les informations contenues dans les différents rapports destinés aux utilisateurs.

Rubriques

- Rapport sur les périphériques

- Rapport sur les tendances des périphériques
- Rapport sur les navigateurs
- Rapport sur les tendances des navigateurs
- Rapport sur les systèmes d'exploitation
- Rapport sur les tendances des systèmes d'exploitation
- Rapport sur les emplacements
- Rapport sur les tendances des emplacements

Rapport sur les périphériques

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Requêtes

Le nombre de demandes CloudFront reçues de chaque type d'appareil.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque type d'appareil en pourcentage du nombre total de demandes CloudFront reçues de tous les appareils.

Rapport sur les tendances des périphériques

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

Desktop

Nombre de demandes CloudFront reçues d'ordinateurs de bureau au cours de la période.

Applications mobiles

Le nombre de demandes CloudFront reçues d'appareils mobiles au cours de la période. Les appareils mobiles peuvent inclure les tablettes et les téléphones portables. Si CloudFront vous ne parvenez pas à déterminer si une demande provient d'un appareil mobile ou d'une tablette, elle est comptabilisée dans la `Mobile` colonne.

Smart-TV

Le nombre de demandes CloudFront reçues de téléviseurs intelligents au cours de la période.

Tablet

Le nombre de demandes CloudFront reçues depuis des tablettes au cours de la période. Si CloudFront vous ne parvenez pas à déterminer si une demande provient d'un appareil mobile ou d'une tablette, elle est comptabilisée dans la `Mobile` colonne.

Je ne sais pas

Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à l'un des types d'appareils standard, par exemple `Desktop` ou `Mobile`.

Empty

Le nombre de demandes CloudFront reçues qui n'incluaient aucune valeur dans l'`User-Agent`en-tête HTTP au cours de la période.

Rapport sur les navigateurs

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Groupe

Le navigateur ou le navigateur et la version de qui CloudFront ont reçu les demandes, selon la valeur de`Grouping`. En plus des noms de navigateur, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler (Robot) – Principalement des requêtes émanant de moteurs de recherche qui procèdent à l'indexation de votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : navigateurs CloudFront identifiés mais ne figurant pas parmi les plus populaires. Si `Bot/Crawler`, `Empty` et/ou `Unknown` n'apparaissent pas dans les neuf premières valeurs, elles sont aussi incluses dans `Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d'applications ou de scripts personnalisés.

Requêtes

Le nombre de demandes CloudFront reçues de chaque type de navigateur.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque type de navigateur en pourcentage du nombre total de demandes CloudFront reçues au cours de la période.

Rapport sur les tendances des navigateurs

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Browsers)

Les colonnes restantes du rapport répertorient les navigateurs ou les navigateurs et versions, en fonction de la valeur de `Grouping`. En plus des noms de navigateur, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler (Robot) – Principalement des requêtes émanant de moteurs de recherche qui procèdent à l'indexation de votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : navigateurs CloudFront identifiés mais ne figurant pas parmi les plus populaires. Si `Bot/Crawler`, `Empty` et/ou `Unknown` n'apparaissent pas dans les neuf premières valeurs, elles sont aussi incluses dans `Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d'applications ou de scripts personnalisés.

Rapport sur les systèmes d'exploitation

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Groupe

Le système d'exploitation ou le système d'exploitation et la version de qui CloudFront ont reçu les demandes, en fonction de la valeur de`Grouping`. En plus des noms de systèmes d'exploitation, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler (Robot) – Principalement des requêtes émanant de moteurs de recherche qui procèdent à l'indexation de votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : systèmes d'exploitation CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si `Bot/Crawler`, `Empty` et/ou `Unknown` n'apparaissent pas dans les neuf premières valeurs, elles sont aussi incluses dans `Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d'applications ou de scripts personnalisés.

Requêtes

Nombre de demandes CloudFront reçues de chaque type de système d'exploitation.

RequestsPct

Nombre de demandes CloudFront reçues de chaque type de système d'exploitation en pourcentage du nombre total de demandes CloudFront reçues au cours de la période.

Rapport sur les tendances des systèmes d'exploitation

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Operating systems)

Les colonnes restantes du rapport répertorient les systèmes d'exploitation ou les systèmes d'exploitation et versions, en fonction de la valeur de `Grouping`. En plus des noms de systèmes d'exploitation, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler (Robot) – Principalement des requêtes émanant de moteurs de recherche qui procèdent à l'indexation de votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : systèmes d'exploitation CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si `Bot/Crawler`, `Empty` et/ou `Unknown` n'apparaissent pas dans les neuf premières valeurs, elles sont aussi incluses dans `Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles le système d'exploitation n'est pas spécifié dans l'en-tête HTTP `User-Agent`.

Rapport sur les emplacements

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

LocationCode

Abréviation du lieu dont les demandes CloudFront ont été reçues. Pour plus d'informations sur les valeurs possibles, consultez la description de Location dans Comment les données du rapport sur les emplacements sont liées aux données des journaux CloudFront standard (journaux d'accès).

LocationName

Le nom de l'emplacement qui CloudFront a reçu les demandes.

Requêtes

Le nombre de demandes CloudFront reçues de chaque emplacement.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque emplacement en pourcentage du nombre total de demandes CloudFront reçues de tous les sites au cours de la période.

TotalBytes

Le nombre d'octets CloudFront diffusés aux spectateurs de ce pays ou de cet État, pour la distribution et la période spécifiées.

Rapport sur les tendances des emplacements

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Emplacements)

Les autres colonnes du rapport répertorient les sites qui CloudFront ont reçu des demandes. Pour plus d'informations sur les valeurs possibles, consultez la description de Location dans Comment

les données du rapport sur les emplacements sont liées aux données des journaux CloudFront standard (journaux d'accès).

Comment les données du rapport sur les emplacements sont liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les données du rapport de localisation de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezConfiguration et utilisation des journaux standard (journaux d'accès).

Emplacement

Pays ou État américain où se trouve la visionneuse. Dans les journaux d'accès, la colonne `c-ip` contient l'adresse IP de l'appareil employé par l'utilisateur. Nous employons des données de géolocalisation pour identifier l'emplacement géographique de l'appareil sur la base de l'adresse IP.

Si vous affichez le rapport Locations (Emplacements) par pays, notez que la liste des pays est basée sur la norme ISO 3166-2, Codes pour la représentation des noms des pays et de leurs subdivisions – Partie 2 : Codes des subdivisions des pays. La liste des pays inclut les valeurs supplémentaires suivantes :

- Anonymous Proxy (Proxy anonyme) – Requête en provenance d'un proxy anonyme.
- Satellite Provider (Fournisseur satellite) – Requête en provenance d'un fournisseur de services Internet par satellite qui propose ses services à plusieurs pays. Les spectateurs peuvent se trouver dans des pays présentant un risque élevé de fraude.
- Europe (Unknown) (Europe (Inconnu)) – Requête en provenance d'une IP dans un bloc utilisé par plusieurs pays européens. Le pays d'origine de la demande ne peut pas être déterminé. CloudFront utilise Europe (Inconnu) comme valeur par défaut.
- Asia/Pacific (Unknown) (Asie-Pacifique (Inconnu)) – Requête en provenance d'un protocole Internet dans un bloc utilisé par plusieurs pays de la région Asie-Pacifique. Le pays d'origine de la demande ne peut pas être déterminé. CloudFront utilise Asie/Pacifique (inconnu) comme valeur par défaut.

Si vous affichez le rapport Locations par État américain, notez qu'il peut inclure les zones militaires et les territoires américains.

> **Note**
>
> S'il n'est pas CloudFront possible de déterminer l'emplacement d'un utilisateur, celui-ci apparaîtra comme Inconnu dans les rapports des utilisateurs.

Request Count

Le nombre total de requêtes du pays ou de l'État américain où se trouve l'utilisateur, pour la distribution et la période spécifiées. Cette valeur correspond généralement étroitement au nombre de `GET` demandes provenant d'adresses IP de ce pays ou de cet État dans les journaux CloudFront d'accès.

Requête %

L'une des options suivantes, en fonction de la valeur sélectionnée sous Details (Détails) :

- Countries (Pays) – Les requêtes de ce pays sous la forme d'un pourcentage du nombre total de requêtes.
- U.S. States (États américains) – Les requêtes de cet État sous la forme d'un pourcentage du nombre total de requêtes en provenance des États-Unis.

Si les requêtes proviennent de plus de 50 pays, vous ne pouvez pas calculer Request % (Requête %) sur la base des données de ce tableau, car la colonne Request Count (Nombre de requêtes) n'inclut pas toutes les requêtes pendant la période spécifiée.

Octets

Le nombre d'octets CloudFront diffusés aux spectateurs de ce pays ou de cet État, pour la distribution et la période spécifiées. Pour modifier l'affichage des données de cette colonne en Ko, Mo ou Go, cliquez sur le lien dans l'en-tête de la colonne.

Surveillance CloudFront des métriques avec Amazon CloudWatch

Amazon CloudFront est intégré à Amazon CloudWatch et publie automatiquement des métriques opérationnelles pour les distributions et les fonctions périphériques (Lambda @Edge et CloudFront Functions). Nombre de ces métriques sont affichées sous forme de graphiques dans la CloudFront console et sont également accessibles à l'aide de l' CloudFront API ou de la CLI. Toutes ces métriques sont disponibles dans la CloudWatch console ou via l' CloudWatch API ou la CLI. Les

CloudFront statistiques ne sont pas prises en compte dans les CloudWatch quotas (anciennement appelés limites) et n'entraînent aucun coût supplémentaire.

Outre les mesures par défaut pour les CloudFront distributions, vous pouvez activer des mesures supplémentaires moyennant des frais supplémentaires. Les mesures supplémentaires s'appliquent aux CloudFront distributions et doivent être activées séparément pour chaque distribution. Pour de plus amples informations sur le coût, veuillez consulter the section called “Estimation du coût des CloudFront mesures supplémentaires”.

Ces métriques peut vous aider à résoudre, suivre et déboguer des problèmes. Pour consulter ces mesures dans la CloudFront console, consultez la page de surveillance. Pour afficher des graphiques relatifs à l'activité d'une CloudFront distribution ou d'une fonction de périphérie spécifique, choisissez-en une, puis choisissez Afficher les métriques de distribution ou Afficher les métriques.

Vous pouvez également définir des alarmes en fonction de ces métriques dans la CloudFront console, ou dans la CloudWatch console, l'API ou la CLI (la CloudWatch tarification standard s'applique). Par exemple, vous pouvez définir une alarme basée sur la métrique `5xxErrorRate`, qui représente le pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse se trouve dans la plage `500` à `599`, incluses. Lorsque le taux d'erreur atteint une certaine valeur pendant un certain laps de temps (par exemple, 5 % des demandes pendant 5 minutes continues), l'alarme est déclenchée. Vous spécifiez la valeur de l'alarme et son unité de temps lorsque vous créez l'alarme. Pour plus d’informations, consultez Création d’alarmes.

> **Note**
>
> Lorsque vous créez une CloudWatch alarme dans la CloudFront console, elle en crée une pour vous dans la région USA Est (Virginie du Nord) (`us-east-1`). Si vous créez une alarme à partir de la CloudWatch console, vous devez utiliser la même région. Comme il CloudFront s'agit d'un service mondial, les mesures relatives au service sont envoyées vers l'est des États-Unis (Virginie du Nord).

Rubriques

- Indicateurs CloudFront de visualisation et de fonction des bords
- Création d'alarmes pour les métriques
- Téléchargement des données de métriques au format CSV
- Obtenir des métriques à l'aide de l' CloudWatch API

Indicateurs CloudFront de visualisation et de fonction des bords

Vous pouvez consulter les statistiques opérationnelles relatives à vos CloudFront distributions et à vos fonctions de périphérie dans la CloudFront console. Pour consulter ces statistiques, consultez la page de surveillance de la CloudFront console. Pour afficher des graphiques relatifs à l'activité d'une CloudFront distribution ou d'une fonction de périphérie spécifique, choisissez-en une, puis choisissez Afficher les métriques de distribution ou Afficher les métriques.

Rubriques

Afficher les métriques de CloudFront distribution par défaut

Les métriques par défaut suivantes sont incluses pour toutes les CloudFront distributions, sans frais supplémentaires :

Requêtes

Le nombre total de demandes d'affichage reçues par CloudFront, pour toutes les méthodes HTTP et pour les requêtes HTTP et HTTPS.

Octets téléchargés

Nombre total d'octets téléchargés par les visionneuses pour les demandes `GET`, `HEAD` et `OPTIONS`.

Octets chargés

Nombre total d'octets vers lesquels les utilisateurs ont transféré CloudFront, utilisés `POST` et `PUT` demandés.

Taux d'erreurs 4xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `4xx`.

Taux d'erreurs 5xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `5xx`.

Taux d'erreurs total

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `4xx` ou `5xx`.

Ces mesures sont affichées sous forme de graphiques pour chaque CloudFront distribution sur la page de surveillance de la CloudFront console. Sur chaque graphique, les totaux sont affichés avec un niveau de précision d'une minute. Outre l'affichage des graphiques, vous pouvez également télécharger des rapports de métriques sous forme de fichiers CSV.

Vous pouvez personnaliser les graphiques en procédant comme suit :

- Pour modifier la plage de temps des informations affichées sur les graphiques, choisissez 1h (1 heure), 3h (3 heures) ou une autre plage, ou spécifiez une plage personnalisée.
- Pour modifier la fréquence de CloudFront mise à jour des informations du graphique, cliquez sur la flèche vers le bas à côté de l'icône d'actualisation, puis choisissez une fréquence de rafraîchissement. Le taux d'actualisation par défaut est d'une minute, mais vous pouvez choisir 10 secondes, 2 minutes ou d'autres options.

Pour afficher CloudFront des graphiques dans la CloudWatch console, choisissez Ajouter au tableau de bord.

Activer des métriques CloudFront de distribution supplémentaires

En plus des métriques par défaut, vous pouvez activer des métriques supplémentaires pour un coût additionnel. Pour de plus amples informations sur le coût, veuillez consulter the section called “Estimation du coût des CloudFront mesures supplémentaires”.

Ces métriques supplémentaires doivent être activées séparément pour chaque distribution :

Taux d'accès au cache

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache.

Latence d'origine

Temps total passé entre le moment où une demande est CloudFront reçue et le moment où elle commence à fournir une réponse au réseau (et non à l'utilisateur), pour les demandes traitées depuis l'origine, et non depuis le CloudFront cache. Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte.

Taux d'erreur par code d'état

Pourcentage de toutes les requêtes de visionneuse pour lesquelles le code d'état HTTP de la réponse est un code particulier dans la plage `4xx` ou `5xx`. Cette métrique est disponible pour tous les codes d'erreur suivants : `401`, `403`, `404`, `502`, `503` et `504`.

Activation de métriques supplémentaires

Vous pouvez activer des métriques supplémentaires dans la CloudFront console, avec AWS CloudFormation, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Console

Pour activer des métriques supplémentaires (console)

1. Connectez-vous à la page de surveillance AWS Management Console et ouvrez-la dans la CloudFront console.
2. Choisissez la distribution pour laquelle vous souhaitez activer des métriques supplémentaires, puis choisissez View distribution metrics (Afficher les métriques de distribution).
3. Choisissez Manage additional metrics (Gérer des indicateurs supplémentaires).
4. Dans la fenêtre Manage additional metrics (Gérer des métriques supplémentaires), activez Enabled (Activé). Lorsque les métriques supplémentaires sont activées, vous pouvez fermer la fenêtre Manage additional metrics (Gérer des métriques supplémentaires).

Lorsque les métriques supplémentaires sont activées, elles apparaissent dans les graphiques. Sur chaque graphique, les totaux sont affichés avec un niveau de précision d'une minute. Outre l'affichage des graphiques, vous pouvez également télécharger des rapports de métriques sous forme de fichiers CSV.

Vous pouvez personnaliser les graphiques en procédant comme suit :

- Pour modifier la plage de temps des informations affichées sur les graphiques, choisissez 1h (1 heure), 3h (3 heures) ou une autre plage, ou spécifiez une plage personnalisée.
- Pour modifier la fréquence de CloudFront mise à jour des informations du graphique, cliquez sur la flèche vers le bas à côté de l'icône d'actualisation, puis choisissez une fréquence de rafraîchissement. Le taux d'actualisation par défaut est d'une minute, mais vous pouvez choisir 10 secondes, 2 minutes ou d'autres options.

Pour afficher CloudFront des graphiques dans la CloudWatch console, choisissez Ajouter au tableau de bord.

AWS CloudFormation

Pour activer des métriques supplémentaires avec AWS CloudFormation, utilisez le type de `AWS::CloudFront::MonitoringSubscription` ressource. L'exemple suivant montre la syntaxe du AWS CloudFormation modèle, au format YAML, permettant d'activer des métriques supplémentaires.

```
Type: AWS::CloudFront::MonitoringSubscription
Properties:
  DistributionId: EDFDVBD6EXAMPLE
  MonitoringSubscription:
    RealtimeMetricsSubscriptionConfig:
      RealtimeMetricsSubscriptionStatus: Enabled
```

CLI

Pour gérer des métriques supplémentaires avec le AWS Command Line Interface (AWS CLI), utilisez l'une des commandes suivantes :

Pour activer des métriques supplémentaires pour une distribution (CLI)

- Utilisez la commande create-monitoring-subscription, comme dans l'exemple suivant. Remplacez *EDFDVBD6EXAMPLE* par l'ID de la distribution pour laquelle vous activez des métriques supplémentaires.

```
aws cloudfront create-monitoring-subscription --
distribution-id EDFDVBD6EXAMPLE --monitoring-subscription
 RealtimeMetricsSubscriptionConfig={RealtimeMetricsSubscriptionStatus=Enabled}
```

Pour savoir si des métriques supplémentaires sont activées pour une distribution (CLI)

- Utilisez la commande get-monitoring-subscription, comme dans l'exemple suivant. Remplacez *EDFDVBD6EXEMPLE* par l'ID de la distribution que vous vérifiez.

```
aws cloudfront get-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

Pour activer des métriques supplémentaires pour une distribution (CLI)

- Utilisez la commande delete-monitoring-subscription, comme dans l'exemple suivant. Remplacez *EDFDVBD6EXAMPLE* par l'ID de la distribution pour laquelle vous désactivez des métriques supplémentaires.

```
aws cloudfront delete-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

API

Pour gérer des métriques supplémentaires avec l' CloudFront API, utilisez l'une des opérations d'API suivantes.

- Pour activer des mesures supplémentaires pour une distribution, utilisez CreateMonitoringSubscription.
- Pour savoir si des métriques supplémentaires sont activées pour une distribution, utilisez GetMonitoringSubscription.
- Pour désactiver des mesures supplémentaires pour une distribution, utilisez DeleteMonitoringSubscription.

Pour plus d'informations sur ces appels d'API, consultez la documentation de référence d'API de votre AWS SDK ou d'un autre client d'API.

Estimation du coût des CloudFront mesures supplémentaires

Lorsque vous activez des métriques supplémentaires pour une distribution, CloudFront envoie jusqu'à 8 métriques CloudWatch dans la région USA Est (Virginie du Nord). CloudWatch facture un

faible taux fixe pour chaque métrique. Ce tarif n'est facturé qu'une fois par mois, par métrique (jusqu'à 8 métriques par distribution). Il s'agit d'un tarif fixe, de sorte que vos coûts restent les mêmes quel que soit le nombre de demandes ou de réponses que la CloudFront distribution reçoit ou envoie. Pour le tarif par métrique, consultez la page de CloudWatch tarification d'Amazon et le calculateur de CloudWatch prix. Des frais d'API supplémentaires s'appliquent lorsque vous récupérez les métriques avec l' CloudWatch API.

Affichage des métriques de fonction Lambda@Edge par défaut

Vous pouvez utiliser CloudWatch des métriques pour surveiller, en temps réel, les problèmes liés à vos fonctions Lambda @Edge. L'utilisation de ces métriques n'implique aucun coût supplémentaire.

Lorsque vous associez une fonction Lambda @Edge à un comportement de cache dans une CloudFront distribution, Lambda commence à envoyer des métriques automatiquement à. CloudWatch Les métriques sont disponibles pour toutes les régions Lambda, mais pour afficher les métriques dans la CloudWatch console ou obtenir les données métriques depuis l'CloudWatch API, vous devez utiliser la région USA Est (Virginie du Nord) (`us-east-1`). Le nom du groupe de métriques est formaté comme suit :`AWS/CloudFront/`*`distribution-ID`*, où *`Distribution-ID`* est l'ID de la CloudFront distribution à laquelle la fonction Lambda @Edge est associée. Pour plus d'informations sur CloudWatch les métriques, consultez le guide de CloudWatch l'utilisateur Amazon.

Les métriques par défaut suivantes sont affichées sous forme de graphiques pour chaque fonction Lambda @Edge sur la page Monitoring de la CloudFront console :

- `5xx`Taux d'erreur pour Lambda@Edge
- Erreurs d'exécution Lambda
- Lambda réponses invalides
- Limitations Lambda

Les graphiques incluent les nombres d'appels, d'erreurs, de limitations, etc. Sur chaque graphique, les totaux sont affichés avec une granularité d'une minute, regroupés par région. AWS

Si vous constatez un pic d'erreurs que vous souhaitez examiner, vous pouvez choisir une fonction, puis consulter les fichiers journaux par AWS région, jusqu'à ce que vous déterminiez quelle fonction est à l'origine des problèmes et dans quelle AWS région. Pour de plus amples informations sur le dépannage des erreurs Lambda@Edge, veuillez consulter :

- the section called “Comment déterminer le type d'échec”

- Quatre étapes pour débugger la diffusion de votre contenu sur AWS

Vous pouvez personnaliser les graphiques en procédant comme suit :

- Pour modifier la plage de temps des informations affichées sur les graphiques, choisissez 1h (1 heure), 3h (3 heures) ou une autre plage, ou spécifiez une plage personnalisée.
- Pour modifier la fréquence de CloudFront mise à jour des informations du graphique, cliquez sur la flèche vers le bas à côté de l'icône d'actualisation, puis choisissez une fréquence de rafraîchissement. Le taux d'actualisation par défaut est d'une minute, mais vous pouvez choisir 10 secondes, 2 minutes ou d'autres options.

Pour afficher les graphiques dans la CloudWatch console, choisissez Ajouter au tableau de bord. Vous devez utiliser la région USA Est (Virginie du Nord) (us-east-1) pour afficher les graphiques dans la console. CloudWatch

Afficher les métriques CloudFront Functions par défaut

CloudFront Functions envoie des métriques opérationnelles à Amazon CloudWatch afin que vous puissiez surveiller vos fonctions. Ces métriques peut vous aider à résoudre, suivre et déboguer des problèmes. CloudFront Functions publie les métriques suivantes pour CloudWatch :

- Appels (`FunctionInvocations`) – nombre de fois où la fonction a été lancée (appelée) au cours d'une période donnée.
- Erreurs de validation (`FunctionValidationErrors`) – nombre d'erreurs de validation générées par la fonction au cours d'une période donnée. Des erreurs de validation se produisent lorsque la fonction s'exécute correctement, mais renvoie des données non valides (un objet d'événement non valide).
- Erreurs d'exécution (`FunctionExecutionErrors`) – nombre d'erreurs d'exécution survenues au cours d'une période donnée. Des erreurs d'exécution se produisent lorsque la fonction échoue.
- Utilisation du calcul (`FunctionComputeUtilization`) – durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé. Cette métrique est un nombre compris entre 0 et 100.

  Si cette valeur atteint ou est proche de 100, la fonction a utilisé ou est sur le point d'utiliser le temps d'exécution autorisé et les demandes suivantes peuvent être limitées. Si votre fonction fonctionne à 80 % ou plus, nous vous recommandons de revoir votre fonction afin de réduire le

temps d'exécution et d'améliorer le taux d'utilisation. Par exemple, vous souhaiterez peut-être uniquement enregistrer les erreurs, simplifier les expressions regex complexes ou supprimer l'analyse inutile d'objets JSON complexes.

- Limitations(`FunctionThrottles`) – nombre de fois où la fonction a été limitée au cours d'une période donnée. Les fonctions peuvent être limitées pour les raisons suivantes :
  - La fonction dépasse continuellement la durée maximale autorisée pour l'exécution.
  - La fonction entraîne des erreurs de compilation.
  - Le nombre de demandes par seconde est exceptionnellement élevé.

CloudFront KeyValueStore envoie également les métriques opérationnelles suivantes à Amazon CloudWatch :

- Read requests (`KvsReadRequests`) : nombre de fois où la fonction a été lue avec succès dans le magasin de valeurs clés au cours d'une période donnée.
- Erreurs de lecture (`KvsReadErrors`) : nombre de fois où la fonction n'a pas pu lire dans le magasin de valeurs clés au cours d'une période donnée.

Pour consulter ces statistiques dans la CloudFront console, rendez-vous sur la page de surveillance. Pour afficher les graphiques d'une fonction spécifique, choisissez Fonctions, choisissez la fonction en question, puis Afficher les métriques de fonction.

Toutes ces métriques sont publiées CloudWatch dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`), dans l'espace de CloudFront noms. Vous pouvez également consulter ces statistiques dans la CloudWatch console. Dans la CloudWatch console, vous pouvez consulter les métriques par fonction ou par fonction par distribution.

Vous pouvez également l'utiliser CloudWatch pour définir des alarmes en fonction de ces mesures. Par exemple, vous pouvez définir une alarme basée sur la métrique du temps d'exécution (`FunctionComputeUilization`), qui représente le pourcentage du temps disponible que votre fonction a pris pour s'exécuter. Lorsque le temps d'exécution atteint une certaine valeur pendant un certain temps (par exemple, plus de 70 % du temps disponible pour 15 minutes continues), l'alarme est déclenchée. Vous spécifiez la valeur de l'alarme et son unité de temps lorsque vous créez l'alarme.

> **Note**
>
> CloudFront Functions envoie des métriques CloudWatch uniquement pour les fonctions de la `LIVE` phase qui s'exécutent en réponse aux demandes et réponses de production. Lorsque vous testez une fonction, CloudFront elle n'envoie aucune métrique à CloudWatch. Le résultat du test contient des informations sur les erreurs, l'utilisation du calcul et les journaux de fonctionnement (`console.log()`instructions), mais ces informations ne sont pas envoyées à CloudWatch.

Pour plus d'informations sur la façon d'obtenir ces métriques avec l' CloudWatch API, consultezthe section called “Obtention de métriques à l'aide de l'API”.

Création d'alarmes pour les métriques

Dans la CloudFront console, vous pouvez définir des alarmes pour vous avertir par Amazon Simple Notification Service (Amazon SNS) en fonction de mesures spécifiques. CloudFront Vous pouvez définir une alarme sur la page Alarmes de la CloudFront console.

Pour créer une alarme dans la console, vous spécifiez les valeurs suivantes :

Métrique

Métrique pour laquelle vous créez l'alarme.

Distribution

La CloudFront distribution pour laquelle vous créez l'alarme.

Name of alarm (Nom de l'alarme)

Nom de l'alarme.

Send a notification to (Envoyer une notification à)

Rubrique Amazon SNS à laquelle envoyer une notification si cette métrique déclenche une alarme.

Whenever ***<métrique> <opérateur> <valeur>***

Spécifiez le moment où une alarme CloudWatch doit être déclenchée et envoyez une notification à la rubrique Amazon SNS. Par exemple, pour recevoir une notification lorsque le taux d'erreurs `5xx` dépasse 1 %, spécifiez ce qui suit :

Chaque fois que la moyenne est de 5 xxErrorRate **>** **1**

Notez ce qui suit à propos de la spécification des valeurs :

- Entrez uniquement des nombres entiers sans ponctuation. Par exemple, pour spécifier mille, entrez **1000**.
- Pour `4xx`, `5xx` et les taux de nombre total d'erreurs, vous spécifiez un pourcentage.
- Pour les requêtes, les octets téléchargés et les octets chargés, vous spécifiez des unités. Par exemple, 1073742000 octets.

Pour au moins ***<nombre>*** périodes consécutives de ***<période>***

Spécifiez le nombre de périodes consécutives de la durée spécifiée pendant lesquelles la métrique doit répondre aux critères avant de CloudWatch déclencher une alarme. Lorsque vous choisissez une valeur, essayez de trouver l'équilibre approprié entre une valeur qui ne déclenche par une alarme pour des problèmes temporaires ou éphémères, mais qui en déclenche une pour des problèmes durables ou réels.

Téléchargement des données de métriques au format CSV

Vous pouvez télécharger les données CloudWatch métriques d'une CloudFront distribution au format CSV. Vous pouvez télécharger les données lorsque vous consultez les métriques de distribution pour une distribution particulière dans la CloudFrontconsole.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version CloudFront de rapport.

Rapport

Nom du rapport.

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Durée de chaque ligne du rapport, par exemple, `ONE_MINUTE`.

Données du rapport Metrics

Le rapport inclut les valeurs suivantes :

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

Requêtes

Nombre total de demandes pour tous les codes d'état HTTP (par exemple, `200`, `404`, etc.) et toutes les méthodes (par exemple, `GET`, `HEAD`, `POST`) pendant la période.

BytesDownloaded

Nombre d'octets que les utilisateurs ont téléchargé pour la distribution spécifiée pendant la période.

BytesUploaded

Nombre d'octets que les utilisateurs ont chargé pour la distribution spécifiée pendant la période.

TotalErrorRatePct

Pourcentage des requêtes pour lesquelles le code d'état HTTP était une erreur `4xx` ou `5xx` pour la distribution spécifiée pendant la période.

4 xxErrorRate pct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `4xx` pour la distribution spécifiée pendant la période.

5 xxErrorRate pct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `5xx` pour la distribution spécifiée pendant la période.

Si vous avez activé des métriques supplémentaires pour votre distribution, le rapport inclut également les valeurs supplémentaires suivantes :

401 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `401` pour la distribution spécifiée pendant la période.

403 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `403` pour la distribution spécifiée pendant la période.

404 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `404` pour la distribution spécifiée pendant la période.

502 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `502` pour la distribution spécifiée pendant la période.

503 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `503` pour la distribution spécifiée pendant la période.

504 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `504` pour la distribution spécifiée pendant la période.

OriginLatency

Temps total passé, en millisecondes, entre le moment où une demande CloudFront a été reçue et le moment où elle a commencé à fournir une réponse au réseau (et non au téléspectateur), pour les demandes traitées depuis l'origine, et non depuis le cache. CloudFront Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte.

CacheHitRate

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache.

Obtenir des métriques à l'aide de l' CloudWatch API

Vous pouvez utiliser l' CloudWatch API ou la CLI Amazon pour obtenir les CloudFront métriques dans les programmes ou applications que vous créez. Vous pouvez utiliser les données brutes pour créer vos propres tableaux de bord personnalisés, vos propres outils d'alarme, etc.

Pour obtenir les CloudFront métriques à partir de l' CloudWatch API, vous devez utiliser la région USA Est (Virginie du Nord) (`us-east-1`). Vous devez également connaître certaines valeurs et types pour chaque métrique.

Rubriques

- Valeurs pour tous les CloudFront indicateurs
- Valeurs pour les métriques CloudFront de distribution
- Valeurs pour les métriques des CloudFront fonctions

Valeurs pour tous les CloudFront indicateurs

Les valeurs suivantes s'appliquent à toutes les CloudFront mesures :

`Namespace`

La valeur pour `Namespace` est toujours `AWS/CloudFront`.

Dimensions

Chaque CloudFront métrique possède les deux dimensions suivantes :

`DistributionId`

L'ID de la CloudFront distribution pour laquelle vous souhaitez obtenir des métriques.

`FunctionName`

Nom de la fonction (dans CloudFront Fonctions) pour laquelle vous souhaitez obtenir des métriques.

Cette dimension s'applique uniquement aux fonctions.

`Region`

La valeur pour « `Region` c'est toujours `Global` parce que CloudFront c'est un service mondial ».

> **Note**
>
> Pour obtenir les CloudFront métriques à partir de l' CloudWatch API, vous devez utiliser la région USA Est (Virginie du Nord) (us-east-1).

Valeurs pour les métriques CloudFront de distribution

Utilisez les informations de la liste suivante pour obtenir des informations sur des métriques de CloudFront distribution spécifiques à partir de l' CloudWatch API. Certaines de ces métriques sont disponibles uniquement lorsque vous avez activé les métriques supplémentaires pour la distribution.

> **Note**
>
> Une seule statistique, `Average` ou `Sum`, est applicable à chaque métrique. La liste suivante indique quelle statistique est applicable à cette métrique.

Taux d'erreurs 4xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `4xx`.

- Nom de métrique : `4xxErrorRate`

- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 401

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `401`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `401ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 403

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `403`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `403ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 404

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `404`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `404ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d'erreurs 5xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `5xx`.

- Nom de métrique : `5xxErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d'erreurs 502

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `502`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `502ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d'erreurs 503

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `503`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `503ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d'erreurs 504

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `504`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `504ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Octets téléchargés

Nombre total d'octets téléchargés par les visionneuses pour les demandes `GET`, `HEAD` et `OPTIONS`.

- Nom de métrique : `BytesDownloaded`
- Statistique valide : `Sum`
- Unité : `None`

Octets chargés

Le nombre total d'octets que les utilisateurs ont téléchargés vers votre origine avecCloudFront, utilisés `POST` et `PUT` demandés.

- Nom de métrique : `BytesUploaded`
- Statistique valide : `Sum`
- Unité : `None`

Taux d'accès au cache

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `CacheHitRate`
- Statistique valide : `Average`
- Unité : `Percent`

Latence d'origine

Temps total passé, en millisecondes, entre le moment où une demande est CloudFront reçue et le moment où elle commence à fournir une réponse au réseau (et non à l'utilisateur), pour les demandes traitées depuis l'origine, et non depuis le cache. CloudFront Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `OriginLatency`
- Statistique valide : `Percentile`
- Unité : `Milliseconds`

> **Note**
>
> Pour obtenir une `Percentile` statistique à partir de l' CloudWatch API, utilisez le `ExtendedStatistics` paramètre, not`Statistics`. Pour plus d'informations, consultez GetMetricStatisticsle Amazon CloudWatch API Reference ou la documentation de référence des AWS SDK.

Requêtes

Le nombre total de demandes d'affichage reçues par CloudFront, pour toutes les méthodes HTTP et pour les requêtes HTTP et HTTPS.

- Nom de métrique : `Requests`
- Statistique valide : `Sum`
- Unité : `None`

Taux d'erreurs total

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `4xx` ou `5xx`.

- Nom de métrique : `TotalErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Valeurs pour les métriques des CloudFront fonctions

Utilisez les informations de la liste suivante pour obtenir des informations sur des métriques de CloudFront fonction spécifiques à partir de l' CloudWatch API.

> **Note**
>
> Une seule statistique, `Average` ou `Sum`, est applicable à chaque métrique. La liste suivante indique quelle statistique est applicable à cette métrique.

Appels

Nombre de fois où la fonction a été démarrée (appelée) au cours d'une période donnée.

- Nom de métrique : `FunctionInvocations`
- Statistique valide : `Sum`
- Unité : `None`

Erreurs de validation

Nombre d'erreurs de validation générées par la fonction au cours d'une période donnée. Des erreurs de validation se produisent lorsque la fonction s'exécute correctement, mais renvoie des données non valides (un objet d'événement non valide).

- Nom de métrique : `FunctionValidationErrors`
- Statistique valide : `Sum`

- Unité : `None`

Erreurs d'exécution

Nombre d'erreurs d'exécution générées au cours d'une période donnée. Des erreurs d'exécution se produisent lorsque la fonction échoue.

- Nom de métrique : `FunctionExecutionErrors`
- Statistique valide : `Sum`
- Unité : `None`

Utilisation du calcul

Durée nécessaire (0-100) pour l'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé.

- Nom de métrique : `FunctionComputeUtilization`
- Statistique valide : `Average`
- Unité : `Percent`

Throttles

Nombre de fois où la fonction a été limitée au cours d'une période donnée.

- Nom de métrique : `FunctionThrottles`
- Statistique valide : `Sum`
- Unité : `None`

CloudFront et journalisation des fonctions Edge

Amazon CloudFront propose différents types de journalisation. Vous pouvez enregistrer les demandes des utilisateurs qui arrivent à vos CloudFront distributions, ou vous pouvez enregistrer l'activité du CloudFront service (activité de l'API) dans votre AWS compte. Vous pouvez également obtenir des journaux à partir de vos fonctions informatiques de périphérie.

Demandes d'enregistrement

CloudFront fournit les méthodes suivantes pour enregistrer les demandes envoyées à vos distributions.

Journaux standard (journaux d'accès)

CloudFront les journaux standard fournissent des informations détaillées sur chaque demande adressée à une distribution. Ces journaux sont utiles pour de nombreux scénarios, y compris les audits de sécurité et d'accès.

CloudFront les journaux standard sont envoyés dans le compartiment Amazon S3 de votre choix. CloudFrontne facture pas les journaux standard, mais vous devez payer des frais Amazon S3 pour le stockage et l'accès aux fichiers journaux.

Pour plus d’informations, consultez Utilisation des journaux standard (journaux d’accès).

Journaux en temps réel

CloudFront les journaux en temps réel fournissent des informations sur les demandes adressées à une distribution, en temps réel (les enregistrements des journaux sont livrés quelques secondes après réception des demandes). Vous pouvez choisir le taux d'échantillonnage de vos journaux en temps réel, c'est-à-dire le pourcentage de demandes pour lesquelles vous souhaitez recevoir des journaux en temps réel. Vous pouvez également choisir les champs que vous souhaitez recevoir dans les enregistrements de journaux.

CloudFront les journaux en temps réel sont transmis au flux de données de votre choix dans Amazon Kinesis Data Streams. CloudFront des frais pour les journaux en temps réel, en plus des frais que vous devez payer pour utiliser Kinesis Data Streams.

Pour plus d’informations, consultez Journaux en temps réel.

Journalisation des fonctions de périphérie

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Vous pouvez accéder aux journaux à l'aide de la CloudWatch console ou de l'API CloudWatch Logs. Pour plus d’informations, consultez the section called “Journaux des fonctions Edge”.

Activité de service de journalisation

Vous pouvez l'utiliser AWS CloudTrail pour enregistrer l'activité du CloudFront service (activité de l'API) dans votre AWS compte. CloudTrail fournit un enregistrement des actions d'API effectuées par un utilisateur, un rôle ou un AWS service dans CloudFront. À l'aide des informations collectées

par CloudTrail, vous pouvez déterminer la demande d'API qui a été faite CloudFront, 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, voir Journalisation des appels d' CloudFront API Amazon à l'aide de AWS CloudTrail.

Rubriques

Configuration et utilisation des journaux standard (journaux d’accès)

Vous pouvez configurer CloudFront pour créer des fichiers journaux contenant des informations détaillées sur chaque demande utilisateur CloudFront reçue. Ceux-ci sont appelés journaux standard, également nommés journaux d’accès. Si vous activez les journaux standard, vous pouvez également spécifier le compartiment Amazon S3 dans lequel vous CloudFront souhaitez enregistrer les fichiers.

Vous pouvez activer les journaux standard lorsque vous créez ou mettez à jour une distribution. Pour plus d’informations, consultez Référence des paramètres de distribution.

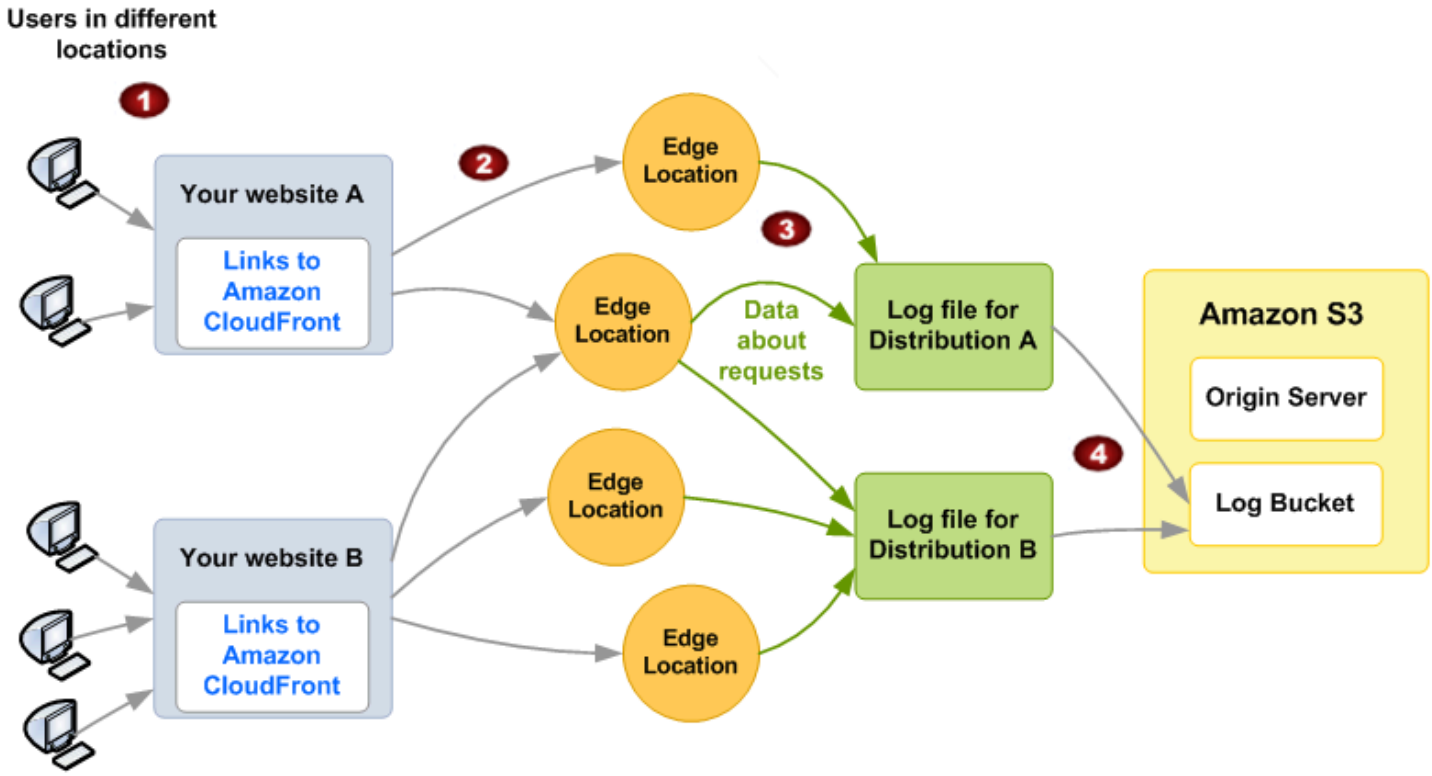
CloudFront propose également des journaux en temps réel, qui vous fournissent des informations sur les demandes adressées à une distribution en temps réel (les journaux sont livrés quelques secondes après réception des demandes). Vous pouvez utiliser des journaux en temps réel pour surveiller, analyser et prendre des mesures en fonction de la performance de diffusion de contenu. Pour de plus amples informations, veuillez consulter Journaux en temps réel.

Rubriques

- Comment les demandes sont consignées lorsque l'URL de la demande ou les en-têtes dépassent la taille maximale
- Analyse des journaux standard
- Modification de vos paramètres de journalisation standard
- Suppression de fichiers journaux standard d'un compartiment Amazon S3
- Format de fichier journal standard
- Frais pour les journaux standard

Fonctionnement de la journalisation standard

Le schéma suivant montre comment CloudFront enregistre les informations relatives aux demandes relatives à vos objets.



Ce qui suit explique comment CloudFront enregistre les informations relatives aux demandes relatives à vos objets, comme illustré dans le schéma précédent.

1. Dans ce diagramme, vous avez deux sites Web, A et B, et deux CloudFront distributions correspondantes. Les utilisateurs demandent vos objets à l'aide des URL associées à vos distributions.

2. CloudFront achemine chaque demande vers l'emplacement périphérique approprié.
3. CloudFront écrit les données relatives à chaque demande dans un fichier journal spécifique à cette distribution. Dans cet exemple, les informations sur les demandes associées à Distribution A vont dans un fichier journal réservé à Distribution A et celles sur les demandes associées à Distribution B dans un fichier journal réservé à Distribution B.
4. CloudFront enregistre régulièrement le fichier journal d'une distribution dans le compartiment Amazon S3 que vous avez spécifié lorsque vous avez activé la journalisation. CloudFront commence ensuite à enregistrer les informations relatives aux demandes suivantes dans un nouveau fichier journal pour la distribution.

Si aucun utilisateur n’accède à votre contenu pendant une heure donnée, vous ne recevez aucun fichier journal pour cette heure.

Chaque entrée d’un fichier journal fournit des informations détaillées sur une seule demande. Pour plus d’informations sur le format du fichier journal, consultez Format de fichier journal standard.

> **Note**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes. CloudFront fournit des journaux d'accès dans les meilleures conditions. L’entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Lorsqu'une entrée de journal est omise des journaux d'accès, le nombre d'entrées dans les journaux d'accès ne correspond pas à l'utilisation indiquée dans les rapports AWS de facturation et d'utilisation.

Choix d’un compartiment Amazon S3 pour vos journaux standard

Lorsque vous activez la journalisation pour une distribution, vous spécifiez le compartiment Amazon S3 dans lequel vous CloudFront souhaitez stocker les fichiers journaux. Si vous optez pour Amazon S3 comme origine, nous vous recommandons de ne pas utiliser le même compartiment pour vos fichiers journaux ; l’utilisation d’un compartiment distinct simplifie la maintenance.

Important

Ne choisissez pas un compartiment Amazon S3 avec l'option S3 Object Ownership (Propriété de l'objet S3) définie sur bucket owner enforced (appliqué par le propriétaire du compartiment). Ce paramètre désactive les ACL pour le compartiment et les objets qu'il contient, ce qui CloudFront empêche de fournir des fichiers journaux au compartiment.

Important

Ne choisissez pas de compartiment Amazon S3 dans l'une des régions suivantes, car il CloudFront ne fournit pas de journaux standard aux compartiments de ces régions :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Canada Ouest (Calgary)
- Europe (Milan)
- Europe (Espagne)
- Europe (Zurich)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)

Vous pouvez stocker les fichiers journaux de plusieurs distributions dans le même compartiment. Lorsque vous activez la journalisation, vous pouvez spécifier un préfixe facultatif pour les noms de fichier et vous pouvez ainsi savoir quels fichiers journaux sont associés à quelles distributions.

Autorisations requises pour configurer la journalisation standard et accéder à vos fichiers journaux

> **Important**
>
> À partir d'avril 2023, vous devrez activer les listes de contrôle d'accès (ACL) S3 pour les nouveaux compartiments S3 utilisés pour les journaux CloudFront standard. Les listes ACL peuvent être activées pendant les étapes de création de compartiment ou après la création d'un compartiment.
> Pour plus d'informations sur ces modifications, consultez Paramètres par défaut pour les nouveaux compartiments S3 FAQ dans le Guide de l'utilisateur d'Amazon Simple Storage Service et Attention : des modifications de sécurité seront apportées à Amazon S3 en avril 2023 dans le Blog d'actualités AWS .

Votre AWS compte doit disposer des autorisations suivantes pour le compartiment que vous spécifiez pour les fichiers journaux :

- La liste de contrôle d'accès (ACL) S3 définie pour le compartiment doit vous accorder l'autorisation `FULL_CONTROL`. Si vous êtes le propriétaire du compartiment, votre compte dispose de cette autorisation par défaut. Si vous ne l'êtes pas, le propriétaire du compartiment doit mettre à jour l'ACL de ce compartiment.
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

Remarques :

Liste ACL pour le compartiment

Lorsque vous créez ou mettez à jour une distribution et que vous activez la CloudFront journalisation, utilisez ces autorisations pour mettre à jour l'ACL du bucket afin d'`FULL_CONTROL`autoriser le `awslogsdelivery` compte. Le compte `awslogsdelivery` écrit les fichiers journaux dans le compartiment. Si votre compte ne dispose pas des autorisations requises pour mettre à jour la liste ACL, la création ou la mise à jour de la distribution échouera.

Dans certaines circonstances, si vous envoyez par programmation une demande pour créer un compartiment, mais qu'un compartiment avec le nom spécifié existe déjà, S3 réinitialise les

autorisations sur le compartiment à la valeur par défaut. Si vous avez configuré CloudFront pour enregistrer les journaux d'accès dans un compartiment S3 et que vous ne recevez plus de journaux dans ce compartiment, vérifiez les autorisations sur le compartiment pour vous assurer qu'il CloudFront dispose des autorisations nécessaires.

Restauration de la liste ACL pour le compartiment

Si vous supprimez les autorisations pour le `awslogsdelivery` compte, vous CloudFront ne pourrez pas enregistrer les journaux dans le compartiment S3. Pour permettre CloudFront de recommencer à enregistrer les journaux pour votre distribution, restaurez l'autorisation ACL en effectuant l'une des opérations suivantes :

- Désactivez la connexion à votre distribution CloudFront, puis réactivez-la. Pour plus d'informations, consultez Référence des paramètres de distribution.
- Ajoutez manuellement l'autorisation de la liste ACL pour le compte `awslogsdelivery` en accédant au compartiment S3 dans la console Amazon S3 et en ajoutant l'autorisation. Afin d'ajouter la liste ACL pour le compte `awslogsdelivery`, vous devez fournir l'ID canonique suivant pour le compte :

  ```
  c4c1ede66af53448b93c283ce9448c4ba468c9432aa01d700d3878632f77d2d0
  ```

  Pour plus d'informations sur l'ajout d'une liste ACL aux compartiments S3, consultez Comment définir des autorisations de compartiment ACL ? dans le Guide de l'utilisateur Amazon Simple Storage Service.

Liste ACL pour chaque fichier journal

En plus de la liste ACL sur le compartiment, il existe une ACL sur chaque fichier journal. Le propriétaire du compartiment dispose de l'autorisation `FULL_CONTROL` sur chaque fichier journal, le propriétaire de la distribution (s'il est différent du propriétaire du compartiment) n'a aucune autorisation et le compte `awslogsdelivery` a les autorisations en lecture et écriture.

Désactivation de la journalisation

Si vous désactivez la journalisation, les ACL du bucket ou des fichiers journaux CloudFront ne sont pas supprimées. Si vous le voulez, vous pouvez le faire vous-même.

Politique de clé requise pour les compartiments SSE-KMS

Si le compartiment S3 de vos journaux standard utilise le chiffrement côté serveur avec AWS KMS keys (SSE-KMS) utilisant une clé gérée par le client, vous devez ajouter l'instruction suivante à

la politique de clé pour la clé gérée par votre client. Cela permet CloudFront d'écrire des fichiers journaux dans le compartiment. (Vous ne pouvez pas utiliser SSE-KMS avec le Clé gérée par AWS car vous CloudFront ne pourrez pas écrire de fichiers journaux dans le compartiment.)

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Si le compartiment S3 de vos journaux standard utilise SSE-KMS avec une clé de compartiment S3, vous devez également ajouter l'autorisation `kms:Decrypt` à l'instruction de politique. Dans ce cas, l'énoncé de stratégie complet ressemble à ce qui suit.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Format de nom de fichier

Le nom de chaque fichier journal enregistré CloudFront dans votre compartiment Amazon S3 utilise le format de nom de fichier suivant :

<optional prefix>/*<distribution ID>*.*YYYY*-*MM*-*DD*-*HH*.*unique-ID*.gz

Les dates et heures sont exprimées en heure UTC (temps universel coordonné).

Par exemple, si vous utilisez `example-prefix` comme préfixe et que votre ID de distribution est `EMLARXS9EXAMPLE`, les noms de fichiers ressemblent à ceci :

```
example-prefix/EMLARXS9EXAMPLE.2019-11-14-20.RT4KCN4SGK9.gz
```

Lorsque vous activez la journalisation pour une distribution, vous pouvez spécifier un préfixe facultatif pour les noms de fichier et vous pouvez ainsi savoir quels fichiers journaux sont associés à quelles distributions. Si vous incluez une valeur pour le préfixe du fichier journal et que celui-ci ne se termine pas par une barre oblique (/), il en CloudFront ajoute une automatiquement. Si votre préfixe se termine par une barre oblique, CloudFront il n'en ajoute pas un autre.

Le nom `.gz` à la fin du fichier indique que le fichier journal CloudFront a été compressé à l'aide de gzip.

Délai de distribution des fichiers journaux standard

CloudFront fournit des journaux standard pour une distribution jusqu'à plusieurs fois par heure. En général, un fichier journal contient des informations sur les demandes CloudFront reçues au cours d'une période donnée. CloudFront fournit généralement le fichier journal pour cette période à votre compartiment Amazon S3 dans l'heure qui suit l'apparition des événements dans le journal. Notez, cependant, que tout ou partie des entrées d'un fichier journal d'une période peut parfois être retardé de 24 heures au plus. Lorsque les entrées du journal sont retardées, les CloudFront enregistre dans un fichier journal dont le nom inclut la date et l'heure de la période au cours de laquelle les demandes ont été effectuées, et non la date et l'heure de livraison du fichier.

Lorsque vous créez un fichier journal, CloudFront consolide les informations relatives à votre distribution provenant de tous les emplacements périphériques ayant reçu des demandes pour vos objets pendant la période couverte par le fichier journal.

CloudFront peut enregistrer plusieurs fichiers pendant une période en fonction du nombre de demandes CloudFront reçues pour les objets associés à une distribution.

CloudFront commence à fournir des journaux d'accès de manière fiable environ quatre heures après l'activation de la journalisation. Vous pourriez obtenir quelques journaux d'accès avant ce moment-là.

> **Note**
>
> Si aucun utilisateur ne demande vos objets pendant la période, vous ne recevez aucun fichier journal pour cette dernière.

CloudFront propose également des journaux en temps réel, qui vous fournissent des informations sur les demandes adressées à une distribution en temps réel (les journaux sont livrés quelques

secondes après réception des demandes). Vous pouvez utiliser des journaux en temps réel pour surveiller, analyser et prendre des mesures en fonction de la performance de diffusion de contenu. Pour de plus amples informations, veuillez consulter Journaux en temps réel.

Comment les demandes sont consignées lorsque l'URL de la demande ou les en-têtes dépassent la taille maximale

Si la taille totale de tous les en-têtes de demande, y compris les cookies, dépasse 20 Ko, ou si l'URL dépasse 8 192 octets, CloudFront vous ne pouvez pas analyser complètement la demande ni l'enregistrer. Étant donné que la demande n'est pas consignée, vous ne verrez pas dans les fichiers journaux le code de statut d'erreur HTTP renvoyé.

Si le corps de la demande dépasse la taille maximale, la demande est consignée, y compris le code de statut d'erreur HTTP.

Analyse des journaux standard

Comme vous pouvez recevoir plusieurs journaux d'accès par heure, nous vous recommandons de combiner tous les fichiers journaux que vous avez reçus pour une période donnée en un seul fichier. Vous pouvez alors analyser les données de cette période plus précisément et plus complètement.

Pour analyser vos journaux d'accès, une solution possible consiste à utiliser Amazon Athena. Athena est un service de requêtes interactif qui peut vous aider à analyser les données pour les AWS services, notamment. CloudFront Pour en savoir plus, consultez la section Interrogation d'Amazon CloudFront Logs dans le guide de l'utilisateur d'Amazon Athena.

En outre, les articles de AWS blog suivants décrivent certaines méthodes d'analyse des journaux d'accès.

- Amazon CloudFront Request Logging (pour le contenu diffusé via HTTP)
- Enhanced CloudFront Logs, Now With Query Strings

> **Important**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes. CloudFront fournit des journaux d'accès dans les meilleures conditions. L'entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Lorsqu'une

entrée de journal est omise des journaux d'accès, le nombre d'entrées dans les journaux d'accès ne correspond pas à l'utilisation indiquée dans les rapports AWS d'utilisation et de facturation.

Modification de vos paramètres de journalisation standard

Vous pouvez activer ou désactiver la journalisation, modifier le compartiment Amazon S3 dans lequel vos journaux sont stockés et modifier le préfixe des fichiers journaux à l'aide de la CloudFront console ou de l' CloudFront API. Les modifications apportées aux paramètres de journalisation prennent effet dans les 12 heures.

Pour plus d'informations, consultez les rubriques suivantes :

- Pour mettre à jour une distribution à l'aide de la CloudFront console, consultezMettre à jour une distribution.
- Pour mettre à jour une distribution à l'aide de l' CloudFront API, consultez UpdateDistributionle Amazon CloudFront API Reference.

Suppression de fichiers journaux standard d'un compartiment Amazon S3

CloudFront ne supprime pas automatiquement les fichiers journaux de votre compartiment Amazon S3. Pour plus d'informations sur la suppression des fichiers journaux à partir d'un compartiment Amazon S3, consultez les rubriques suivantes :

- Utilisation de la console Amazon S3 : Suppression d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Utilisation de l'API REST : DeleteObjectdans le manuel Amazon Simple Storage Service API Reference.

Format de fichier journal standard

Chaque entrée d'un fichier journal fournit des informations détaillées sur une seule demande utilisateur. Les fichiers journaux présentent les caractéristiques suivantes :

- Utilisez le format de fichier journal étendu W3C.
- Contiennent des valeurs séparées par des virgules.

- Contiennent des enregistrements qui ne sont pas nécessairement dans l'ordre chronologique.
- Contiennent deux lignes d'en-tête : l'une avec la version fichier-format et l'autre qui répertorie les champs W3C inclus dans chaque enregistrement.
- Contiennent des équivalents encodés en URL pour des espaces et certains autres caractères dans les valeurs de champ.

  Les équivalents encodés en URL sont utilisés pour les caractères suivants :

  - Codes de caractères ASCII 0 à 32 inclus
  - Codes de caractères ASCII 127 et suivants
  - Tous les caractères du tableau suivant

  La norme d'encodage d'URL est définie dans la norme RFC 1738.

Valeur codée par URL	Caractère
%3C	<
%3E	>
%22	"
%23	#
%25	%
%7B	{
%7D	}
%7C	|
%5C	\
%5E	^
%7E	~
%5B	[

Valeur codée par URL	Caractère
%5D	]
%60	`
%27	'
%20	espace

Champs d’un fichier journal standard

Le fichier journal d’une distribution contient 33 champs. La liste suivante contient chaque nom de champ, dans l’ordre, ainsi qu’une description des informations contenues dans ce champ.

1. **`date`**

   Date à laquelle l’événement s’est produit au format `YYYY-MM-DD`. Par exemple, `2019-06-30`. Les dates et heures sont exprimées en heure UTC (temps universel coordonné). Pour WebSocket les connexions, il s'agit de la date de fermeture de la connexion.

2. **`time`**

   Heure à laquelle le CloudFront serveur a fini de répondre à la demande (en UTC), par exemple,`01:42:39`. Pour WebSocket les connexions, il s'agit de l'heure à laquelle la connexion est fermée.

3. **`x-edge-location`**

   Emplacement périphérique ayant servi la demande. Chaque emplacement périphérique est identifié par un code à trois lettres et un numéro attribué arbitrairement (par exemple, DFW3). Le code à trois lettres correspond généralement au code IATA (International Air Transport Association) d’un aéroport proche de l’emplacement périphérique. (Ces abréviations peuvent changer à l’avenir.)

4. **`sc-bytes`**

   Nombre total d’octets envoyés par le serveur à l’utilisateur en réponse à la demande, en-têtes inclus. Pour WebSocket les connexions, il s'agit du nombre total d'octets envoyés par le serveur au client via la connexion.

5. **`c-ip`**

Adresse IP de la visionneuse qui a émis la demande, par exemple, `192.0.2.183` ou `2001:0db8:85a3::8a2e:0370:7334`. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur de ce champ est l'adresse IP du proxy ou de l'équilibreur de charge. Voir aussi le champ `x-forwarded-for`.

6. **`cs-method`**

   Méthode de demande HTTP reçue de l'utilisateur.

7. **`cs(Host)`**

   Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net).

8. **`cs-uri-stem`**

   Partie de l'URL de la requête qui identifie le chemin d'accès et l'objet (par exemple, `/images/cat.jpg`). Les points d'interrogation (?) des URL et des chaînes de requête ne sont pas inclus dans le journal.

9. **`sc-status`**

   Contient une des valeurs suivantes :

   - Code de statut HTTP de la réponse du serveur (par exemple, `200`).
   - `000`, ce qui indique que l'utilisateur a fermé la connexion avant que le serveur puisse répondre à la demande. Si l'utilisateur ferme la connexion après que le serveur a commencé à envoyer la réponse, ce champ contient le code de statut HTTP de la réponse que le serveur a commencé à envoyer.

10. **`cs(Referer)`**

    Valeur de l'en-tête `Referer` dans la demande. Nom du domaine à l'origine de la demande. Les référents courants incluent des moteurs de recherche, d'autres sites Web contenant des liens directs vers vos objets ou encore votre propre site web.

11. **`cs(User-Agent)`**

    Valeur de l'en-tête `User-Agent` dans la demande. L'en-tête `User-Agent` identifie la source de la demande, comme le type d'appareil et le navigateur ayant envoyé la demande et, si la demande provenait d'un moteur de recherche, le moteur utilisé.

12. **`cs-uri-query`**

    Partie de la chaîne de requête de l'URL de la demande, le cas échéant.

Quand un URL ne contient pas de chaîne de requête, la valeur de ce champ est un trait d'union (-). Pour plus d'informations, consultez Contenu du cache basé sur les paramètres de chaîne de requête.

13 **`cs(Cookie)`**

En-tête `Cookie` de la demande, y compris les paires nom-valeur et les attributs associés.

Si vous activez l'enregistrement des cookies, les CloudFront enregistre dans toutes les demandes, quels que soient les cookies que vous choisissez de transférer à l'origine. Quand une demande n'inclut pas un en-tête de cookie, la valeur de ce champ est un trait d'union (-). Pour plus d'informations sur les cookies, consultez Contenu du cache basé sur les cookies.

14 **`x-edge-result-type`**

Comment le serveur a classé la réponse après que le dernier octet a quitté le serveur. Dans certains cas, le type de résultat peut changer entre le moment où le serveur est prêt à envoyer la réponse et celui où il a fini d'envoyer celle-ci. Voir aussi le champ `x-edge-response-result-type`.

Par exemple, dans le streaming HTTP, supposons que le serveur trouve un segment du flux dans le cache. Dans ce scénario, la valeur de ce champ est normalement `Hit`. Cependant, si l'utilisateur ferme la connexion avant que le serveur ait livré la totalité du segment, le type de résultat final (et donc la valeur de ce champ) est `Error`.

WebSocket les connexions auront une valeur égale à `Miss` pour ce champ car le contenu ne peut pas être mis en cache et est directement transmis par proxy à l'origine.

Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'ayant pas pu être satisfaite par un objet du cache, le serveur a transmis la demande à l'origine et retourné le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé un code d'erreur HTTP 503, car la capacité était insuffisante pour servir l'objet au moment de la demande.

- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`). Si la valeur du champ `sc-status` est `200`, ou si la valeur de ce champ est `Error` et que la valeur du champ `x-edge-response-result-type` est différente de `Error`, cela signifie que la demande HTTP a réussi mais que le client a été déconnecté avant de recevoir tous les octets.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.

15 **`x-edge-request-id`**

Chaîne opaque qui identifie une demande de manière unique. CloudFront envoie également cette chaîne dans l'en-tête de `x-amz-cf-id` réponse.

16 **`x-host-header`**

Valeur que l'utilisateur a incluse dans l'en-tête `Host` de la demande. Si vous utilisez le nom de CloudFront domaine dans les URL de vos objets (par exemple d111111abcdef8.cloudfront.net), ce champ contient ce nom de domaine. Si vous utilisez des noms de domaine alternatifs (CNAMES) dans vos URL d'objet (tels que www.example.com), ce champ contient l'autre nom de domaine.

Si vous utilisez des noms de domaine alternatifs, consultez `cs(Host)` dans le champ 7 pour connaître le nom de domaine associé à votre distribution.

17 **`cs-protocol`**

Protocole de la demande de l'utilisateur (`http`, `https`, `ws` ou `wss`).

18 **`cs-bytes`**

Nombre total d'octets de données que l'utilisateur a inclus dans la demande, en-têtes inclus. Pour WebSocket les connexions, il s'agit du nombre total d'octets envoyés par le client au serveur lors de la connexion.

19 **`time-taken`**

Nombre de secondes (au millième de seconde, par exemple 0,082) entre le moment où le serveur reçoit la demande de l'utilisateur et le moment où le serveur écrit le dernier octet de la réponse à la file d'attente de sortie, tel que mesuré sur le serveur. Du point de vue de l'utilisateur, le temps total pour obtenir la réponse complète sera plus long que cette valeur en raison de la latence réseau et de la mise en tampon TCP.

20 **`x-forwarded-for`**

Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur du champ `c-ip` est l'adresse IP du proxy ou de l'équilibreur de charge. Dans ce cas, ce champ est l'adresse IP de l'utilisateur à l'origine de la demande. Ce champ peut contenir plusieurs adresses IP séparées par des virgules. Chaque adresse IP peut être une adresse IPv4 (par exemple`192.0.2.183`) ou une adresse IPv6 (par exemple,`2001:0db8:85a3::8a2e:0370:7334`).

Si l'utilisateur n'a pas utilisé de proxy HTTP ou d'équilibreur de charge, la valeur de ce champ est un trait d'union (-).

21 **`ssl-protocol`**

Lorsque la demande a utilisé HTTPS, ce champ contient le protocole SSL/TLS que l'utilisateur et le serveur ont négocié pour transmettre la demande et la réponse. Pour obtenir la liste des valeurs possibles, consultez les chiffrements SSL/TLS pris en charge dans Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

Quand `cs-protocol` dans le champ 17 est `http`, la valeur de ce champ est un trait d'union (-).

22 **`ssl-cipher`**

Lorsque la demande utilise HTTPS, ce champ contient le chiffrement SSL/TLS que l'utilisateur et le serveur ont négocié pour chiffrer la demande et la réponse. Pour obtenir la liste des valeurs possibles, consultez les chiffrements SSL/TLS pris en charge dans Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

Quand `cs-protocol` dans le champ 17 est `http`, la valeur de ce champ est un trait d'union (-).

23 **`x-edge-response-result-type`**

Comment le serveur a classé la réponse juste avant de la retourner à l'utilisateur. Voir aussi le champ `x-edge-result-type`. Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'a pas pu être satisfaite par un objet du cache, c'est pourquoi le serveur a transmis la demande au serveur d'origine et a renvoyé le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.

- `CapacityExceeded` : le serveur a renvoyé une erreur 503 car il n'avait pas suffisamment de capacité au moment de la demande pour servir l'objet.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`).

  Si la valeur du champ `x-edge-result-type` est `Error` et que la valeur de ce champ n'est pas `Error`, le client s'est déconnecté avant d'avoir fini le téléchargement.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.

24. **`cs-protocol-version`**

    Version de HTTP que l'utilisateur a spécifiée dans la requête. Les valeurs possibles incluent `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` et `HTTP/3.0`.

25. **`fle-status`**

    Lorsque le chiffrement au niveau du champ est configuré pour une distribution, ce champ contient un code indiquant si le corps de la demande a bien été traité. Quand le serveur traite le corps de la demande, chiffre les valeurs dans les champs spécifiés et transfère la demande à l'origine correctement, la valeur de ce champ est `Processed`. La valeur `x-edge-result-type` peut toujours indiquer une erreur côté client ou côté serveur dans ce cas.

    Les valeurs possibles pour ce champ sont les suivantes :

    - `ForwardedByContentType` – Le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car aucun type de contenu n'était configuré.
    - `ForwardedByQueryArgs` : le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car la demande contient un argument de requête qui n'était pas dans la configuration du chiffrement au niveau du champ.
    - `ForwardedDueToNoProfile` – Le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car aucun profil n'était spécifié dans la configuration du chiffrement au niveau du champ.
    - `MalformedContentTypeClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format de la valeur de l'en-tête `Content-Type` n'était pas valide.
    - `MalformedInputClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format du corps de la requête n'était pas valide.

- `MalformedQueryArgsClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car un argument de requête était vide ou son format n'était pas valide.
- `RejectedByContentType` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun type de contenu n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `RejectedByQueryArgs` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun argument de requête n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `ServerError` – Le serveur d'origine a renvoyé une erreur.

Si la demande dépasse un quota de chiffrement au niveau du champ (précédemment appelé limite), ce champ contient l'un des codes d'erreur suivants, et le serveur renvoie le code d'état HTTP 400 à l'utilisateur. Pour obtenir une liste des quotas actuels de chiffrement au niveau du champ, consultez Quotas sur le chiffrement au niveau du champ.

- `FieldLengthLimitClientError` – Un champ configuré pour être chiffré a dépassé la longueur maximale autorisée.
- `FieldNumberLimitClientError` – Une demande de configuration de la distribution pour le chiffrement contient un nombre de champs supérieur à celui autorisé.
- `RequestLengthLimitClientError` – La longueur du corps de la demande dépasse la longueur maximale autorisée lorsque le chiffrement au niveau du champ est configuré.

Si le chiffrement au niveau du champ n'est pas configuré pour la distribution, la valeur de ce champ est un trait d'union (-).

26. **`fle-encrypted-fields`**

Nombre de champs de chiffrement au niveau des champs que le serveur a chiffrés et transmis à l'origine. CloudFront les serveurs transmettent la demande traitée à l'origine au fur et à mesure qu'ils chiffrent les données. Ce champ peut donc avoir une valeur même si la valeur de `fle-status` est une erreur.

Si le chiffrement au niveau du champ n'est pas configuré pour la distribution, la valeur de ce champ est un trait d'union (-).

27. **`c-port`**

Numéro de port de la demande depuis l'utilisateur.

28. **`time-to-first-byte`**

    Nombre de secondes entre la réception de la demande et l'écriture du premier octet de la réponse, tel que mesuré sur le serveur.

29. **`x-edge-detailed-result-type`**

    Ce champ contient la même valeur que le champ `x-edge-result-type`, sauf dans les cas suivants :

    - Lorsque l'objet a été servi à l'utilisateur à partir de la couche Origin Shield, ce champ contient `OriginShieldHit`.
    - Lorsque l'objet n'était pas dans le CloudFront cache et que la réponse a été générée par une fonction Lambda @Edge de demande d'origine, ce champ contient. `MissGeneratedResponse`
    - Lorsque la valeur du champ `x-edge-result-type` est `Error`, ce champ contient l'une des valeurs suivantes et présente des informations supplémentaires sur l'erreur :
      - `AbortedOrigin` – Le serveur a rencontré un problème avec l'origine.
      - `ClientCommError` – La réponse à l'utilisateur a été interrompue en raison d'un problème de communication entre le serveur et l'utilisateur.
      - `ClientGeoBlocked` : la distribution est configurée de manière à refuser les demandes en provenance de l'emplacement géographique de l'utilisateur.
      - `ClientHungUpRequest` – La visionneuse s'est arrêtée prématurément lors de l'envoi de la demande.
      - `Error` : une erreur s'est produite pour laquelle le type d'erreur ne correspond à aucune des autres catégories. Ce type d'erreur peut se produire lorsque le serveur sert une réponse d'erreur à partir du cache.
      - `InvalidRequest` – Le serveur a reçu une demande non valide de la part de l'utilisateur.
      - `InvalidRequestBlocked` – L'accès à la ressource demandée est bloqué.
      - `InvalidRequestCertificate` : la distribution ne correspond pas au certificat SSL/TLS pour lequel la connexion HTTPS a été établie.
      - `InvalidRequestHeader` – La demande contenait un en-tête non valide.
      - `InvalidRequestMethod` – La distribution n'est pas configurée pour gérer la méthode de demande HTTP utilisée. Cela peut se produire lorsque la distribution prend en charge uniquement les demandes pouvant être mises en cache.
      - `OriginCommError` – La demande a expiré lors de la connexion à l'origine ou lors de la lecture de données à partir de l'origine.

- `OriginConnectError` : le serveur n'a pas pu se connecter à l'origine.
- `OriginContentRangeLengthError` : l'en-tête `Content-Length` de la réponse de l'origine ne correspond pas à la longueur de l'en-tête `Content-Range`.
- `OriginDnsError` : le serveur n'a pas pu résoudre le nom de domaine de l'origine.
- `OriginError` — L'origine a renvoyé une réponse incorrecte.
- `OriginHeaderTooBigError` – Un en-tête renvoyé par l'origine est trop volumineux pour être traité.
- `OriginInvalidResponseError` — L'origine a renvoyé une réponse non valide.
- `OriginReadError` : le serveur n'a pas pu lire à partir de l'origine.
- `OriginWriteError` : le serveur n'a pas pu écrire à l'origine.
- `OriginZeroSizeObjectError` — Un objet de taille zéro envoyé depuis l'origine a provoqué une erreur.
- `SlowReaderOriginError` — La visionneuse a été lente à lire le message qui a provoqué l'erreur d'origine.

30 **`sc-content-type`**

Valeur de l'en-tête `Content-Type` HTTP de la réponse.

31 **`sc-content-len`**

Valeur de l'en-tête `Content-Length` HTTP de la réponse.

32 **`sc-range-start`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de début de plage.

33 **`sc-range-end`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de fin de plage.

L'exemple suivant est celui d'un fichier journal pour une distribution :

```
#Version: 1.0
#Fields: date time x-edge-location sc-bytes c-ip cs-method cs(Host) cs-uri-stem sc-
status cs(Referer) cs(User-Agent) cs-uri-query cs(Cookie) x-edge-result-type x-edge-
request-id x-host-header cs-protocol cs-bytes time-taken x-forwarded-for ssl-protocol
```

```
 ssl-cipher x-edge-response-result-type cs-protocol-version fle-status fle-encrypted-
fields c-port time-to-first-byte x-edge-detailed-result-type sc-content-type sc-
content-len sc-range-start sc-range-end
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 SOX4xwn4XV6Q4rgb7XiVGOHms_BGlTAC4KyHmureZmBNrjGdRLiNIQ== d111111abcdef8.cloudfront.net
 https 23 0.001 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.001 Hit
 text/html 78 - -
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 k6WGMNkEzR5BEM_SaF47gjtX9zBDO2m349OY2an0QPEaUum1ZOLrow== d111111abcdef8.cloudfront.net
 https 23 0.000 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.000 Hit
 text/html 78 - -
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 f37nTMVvnKvV2ZSvEsivup_c2kZ7VXzYdjC-GUQZ5qNs-89BlWazbw== d111111abcdef8.cloudfront.net
 https 23 0.001 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.001 Hit
 text/html 78 - -
2019-12-13 22:36:27 SEA19-C1 900 192.0.2.200 GET d111111abcdef8.cloudfront.net /
favicon.ico 502 http://www.example.com/ Mozilla/5.0%20(Windows
%20NT%2010.0;%20Win64;%20x64)%20AppleWebKit/537.36%20(KHTML,
%20like%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Error
 1pkpNfBQ39sYMnjjUQjmH2w1wdJnbHYTbag21o_3OfcQgPzdL2RSSQ== www.example.com http 675
 0.102 - - - Error HTTP/1.1 - - 25260 0.102 OriginDnsError text/html 507 - -
2019-12-13 22:36:26 SEA19-C1 900 192.0.2.200 GET d111111abcdef8.cloudfront.net / 502
 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;%20x64)%20AppleWebKit/537.36%20(KHTML,
%20like%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Error
 3AqrZGCnF_g0-5KOvfA7c9XLcf4YGvMFSeFdIetR1N_2y8jSis8Zxg== www.example.com http 735
 0.107 - - - Error HTTP/1.1 - - 3802 0.107 OriginDnsError text/html 507 - -
2019-12-13 22:37:02 SEA19-C2 900 192.0.2.200 GET d111111abcdef8.cloudfront.net / 502
 - curl/7.55.1 - - Error kBkDzGnceVtWHqSCqBUqtA_cEs2T3tFUBbnBNkB9El_uVRhHgcZfcw==
 www.example.com http 387 0.103 - - - Error HTTP/1.1 - - 12644 0.103 OriginDnsError
 text/html 507 - -
```

Frais pour les journaux standard

La journalisation standard est une fonctionnalité facultative de CloudFront. L'activation de la journalisation standard n'entraîne pas de frais supplémentaires. Cependant, les frais Amazon S3 usuels sont facturés pour stocker les fichiers et y accéder sur Amazon S3 (notez que vous pouvez supprimer ces fichiers à tout moment).

Pour plus d'informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

Pour plus d'informations sur la CloudFront tarification, consultez la section CloudFront Tarification.

Journaux en temps réel

Avec les journaux CloudFront en temps réel, vous pouvez obtenir des informations sur les demandes adressées à une distribution en temps réel (les journaux sont livrés quelques secondes après réception des demandes). Vous pouvez utiliser des journaux en temps réel pour surveiller, analyser et prendre des mesures en fonction de la performance de diffusion de contenu.

CloudFront les journaux en temps réel sont configurables. Vous pouvez choisir :

- Vous pouvez choisir le taux d'échantillonnage des journaux en temps réel, c'est-à-dire le pourcentage de demandes pour lesquelles vous souhaitez recevoir des journaux en temps réel.
- Champs spécifiques que vous souhaitez recevoir dans les enregistrements de journal.
- Comportements de cache spécifiques (modèles de chemin) pour lesquels vous souhaitez recevoir des journaux en temps réel.

CloudFront les journaux en temps réel sont transmis au flux de données de votre choix dans Amazon Kinesis Data Streams. Vous pouvez créer votre propre consommateur de flux de données Kinesis ou utiliser Amazon Data Firehose pour envoyer les données de journal à Amazon Simple Storage Service (Amazon S3), Amazon Redshift, OpenSearch Amazon Service OpenSearch (Service) ou à un service de traitement des journaux tiers.

CloudFront des frais pour les journaux en temps réel, en plus des frais que vous devez payer pour utiliser Kinesis Data Streams. Pour plus d'informations sur les tarifs, consultez les rubriques Amazon CloudFront Pricing et Amazon Kinesis Data Streams.

> **Important**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes. CloudFront fournit des journaux en temps réel dans les meilleures conditions. L'entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Lorsqu'une entrée de journal est omise dans les journaux en temps réel, le nombre d'entrées dans les journaux en temps réel ne correspond pas à l'utilisation indiquée dans les rapports AWS de facturation et d'utilisation.

Comprendre les configurations en temps réel

Pour utiliser les journaux CloudFront en temps réel, vous devez commencer par créer une configuration de journal en temps réel. La configuration du journal en temps réel contient des informations sur les champs de journal que vous souhaitez recevoir, la fréquence d'échantillonnage des enregistrements de journaux et le flux de données Kinesis où vous souhaitez distribuer les journaux.

Plus précisément, une configuration de journal en temps réel contient les paramètres suivants :

- Nom
- Taux d'échantillonnage
- Champs
- Point de terminaison (flux de données Kinesis)
- Rôle IAM

Nom

Nom permettant d'identifier la configuration du journal en temps réel.

Taux d'échantillonnage

Le taux d'échantillonnage est un nombre entier compris entre 1 et 100 (inclus) qui détermine le pourcentage de demandes de l'utilisateur envoyées à Kinesis Data Streams sous forme d'enregistrements de journal en temps réel. Pour inclure chaque demande d'utilisateur dans

vos journaux en temps réel, spécifiez 100 pour la fréquence d'échantillonnage. Vous pouvez choisir un taux d'échantillonnage inférieur pour réduire les coûts tout en recevant un échantillon représentatif des données de demande dans vos journaux en temps réel.

Champs

Liste des champs inclus dans chaque enregistrement de journal en temps réel. Chaque enregistrement de journal peut contenir jusqu'à 40 champs ; vous pouvez choisir de recevoir tous les champs disponibles ou uniquement les champs dont vous avez besoin pour surveiller et analyser les performances.

La liste suivante contient chaque nom de champ et une description des informations contenues dans ce champ. Les champs sont répertoriés dans l'ordre dans lequel ils apparaissent dans les enregistrements de journal qui sont distribués à Kinesis Data Streams.

Les champs 46 à 63 sont des données communes sur les clients multimédia (CMCD) que les clients des lecteurs multimédias peuvent envoyer aux CDN à chaque demande. Vous pouvez utiliser ces données pour comprendre chaque demande, notamment le type de média (audio, vidéo), le taux de lecture et la durée de diffusion. Ces champs n'apparaîtront dans vos journaux en temps réel que s'ils sont envoyés à CloudFront.

1. **`timestamp`**

   Date et heure auxquelles le serveur Edge a fini de répondre à la demande.

2. **`c-ip`**

   Adresse IP de la visionneuse qui a émis la demande, par exemple, `192.0.2.183` ou `2001:0db8:85a3::8a2e:0370:7334`. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur de ce champ est l'adresse IP du proxy ou de l'équilibreur de charge. Voir aussi le champ `x-forwarded-for`.

3. **`time-to-first-byte`**

   Nombre de secondes entre la réception de la demande et l'écriture du premier octet de la réponse, tel que mesuré sur le serveur.

4. **`sc-status`**

   Code de statut HTTP de la réponse du serveur (par exemple, `200`).

5. **`sc-bytes`**

Nombre total d'octets envoyés par le serveur à l'utilisateur en réponse à la demande, en-têtes inclus. Pour WebSocket les connexions, il s'agit du nombre total d'octets envoyés par le serveur au client via la connexion.

6. **`cs-method`**

   Méthode de demande HTTP reçue de l'utilisateur.

7. **`cs-protocol`**

   Protocole de la demande de l'utilisateur (`http`, `https`, `ws` ou `wss`).

8. **`cs-host`**

   Valeur que l'utilisateur a incluse dans l'en-tête `Host` de la demande. Si vous utilisez le nom de CloudFront domaine dans les URL de vos objets (par exemple d111111abcdef8.cloudfront.net), ce champ contient ce nom de domaine. Si vous utilisez des noms de domaine alternatifs (CNAMES) dans vos URL d'objet (tels que www.example.com), ce champ contient l'autre nom de domaine.

9. **`cs-uri-stem`**

   L'URL entière de la demande, y compris la chaîne de requête (le cas échéant), mais sans le nom de domaine. Par exemple, `/images/cat.jpg?mobile=true`.

   > **Note**
   >
   > Dans les journaux standard, la valeur `cs-uri-stem` n'inclut pas la chaîne de requête.

10. **`cs-bytes`**

    Nombre total d'octets de données que l'utilisateur a inclus dans la demande, en-têtes inclus. Pour WebSocket les connexions, il s'agit du nombre total d'octets envoyés par le client au serveur lors de la connexion.

11. **`x-edge-location`**

    Emplacement périphérique ayant servi la demande. Chaque emplacement périphérique est identifié par un code à trois lettres et un numéro attribué arbitrairement (par exemple, DFW3). Le code à trois lettres correspond généralement au code IATA (International Air Transport Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.)

12. **`x-edge-request-id`**

Chaîne opaque qui identifie une demande de manière unique. CloudFront envoie également cette chaîne dans l'en-tête de `x-amz-cf-id` réponse.

13. **`x-host-header`**

    Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net).

14. **`time-taken`**

    Nombre de secondes (au millième de seconde, par exemple 0,082) entre le moment où le serveur reçoit la demande de l'utilisateur et le moment où le serveur écrit le dernier octet de la réponse à la file d'attente de sortie, tel que mesuré sur le serveur. Du point de vue de l'utilisateur, le temps total pour obtenir la réponse complète sera plus long que cette valeur en raison de la latence réseau et de la mise en tampon TCP.

15. **`cs-protocol-version`**

    Version de HTTP que l'utilisateur a spécifiée dans la requête. Les valeurs possibles incluent `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` et `HTTP/3.0`.

16. **`c-ip-version`**

    Version IP de la demande (IPv4 ou IPv6).

17. **`cs-user-agent`**

    Valeur de l'en-tête `User-Agent` dans la demande. L'en-tête `User-Agent` identifie la source de la demande, comme le type d'appareil et le navigateur ayant envoyé la demande et, si la demande provenait d'un moteur de recherche, le moteur utilisé.

18. **`cs-referer`**

    Valeur de l'en-tête `Referer` dans la demande. Nom du domaine à l'origine de la demande. Les référents courants incluent des moteurs de recherche, d'autres sites Web contenant des liens directs vers vos objets ou encore votre propre site web.

19. **`cs-cookie`**

    En-tête `Cookie` de la demande, y compris les paires nom-valeur et les attributs associés.

    > **Note**
    >
    > Ce champ est tronqué à 800 octets.

20. **`cs-uri-query`**

Partie de la chaîne de requête de l'URL de la demande, le cas échéant.

21. **`x-edge-response-result-type`**

Comment le serveur a classé la réponse juste avant de la retourner à l'utilisateur. Voir aussi le champ `x-edge-result-type`. Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'a pas pu être satisfaite par un objet du cache, c'est pourquoi le serveur a transmis la demande au serveur d'origine et a renvoyé le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé une erreur 503 car il n'avait pas suffisamment de capacité au moment de la demande pour servir l'objet.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`).

  Si la valeur du champ `x-edge-result-type` est `Error` et que la valeur de ce champ n'est pas `Error`, le client s'est déconnecté avant d'avoir fini le téléchargement.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.

22. **`x-forwarded-for`**

Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur du champ `c-ip` est l'adresse IP du proxy ou de l'équilibreur de charge. Dans ce cas, ce champ est l'adresse IP de l'utilisateur à l'origine de la demande. Ce champ peut contenir plusieurs adresses IP séparées par des virgules. Chaque adresse IP peut être une adresse IPv4 (par exemple`192.0.2.183`) ou une adresse IPv6 (par exemple,`2001:0db8:85a3::8a2e:0370:7334`).

23. **`ssl-protocol`**

Lorsque la demande a utilisé HTTPS, ce champ contient le protocole SSL/TLS que l'utilisateur et le serveur ont négocié pour transmettre la demande et la réponse. Pour obtenir la liste des valeurs

possibles, consultez les chiffrements SSL/TLS pris en charge dans Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

24 **`ssl-cipher`**

Lorsque la demande utilise HTTPS, ce champ contient le chiffrement SSL/TLS que l'utilisateur et le serveur ont négocié pour chiffrer la demande et la réponse. Pour obtenir la liste des valeurs possibles, consultez les chiffrements SSL/TLS pris en charge dans Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront.

25 **`x-edge-result-type`**

Comment le serveur a classé la réponse après que le dernier octet a quitté le serveur. Dans certains cas, le type de résultat peut changer entre le moment où le serveur est prêt à envoyer la réponse et celui où il a fini d'envoyer celle-ci. Voir aussi le champ `x-edge-response-result-type`.

Par exemple, dans le streaming HTTP, supposons que le serveur trouve un segment du flux dans le cache. Dans ce scénario, la valeur de ce champ est normalement `Hit`. Cependant, si l'utilisateur ferme la connexion avant que le serveur ait livré la totalité du segment, le type de résultat final (et donc la valeur de ce champ) est `Error`.

WebSocket les connexions auront une valeur égale à `Miss` pour ce champ car le contenu ne peut pas être mis en cache et est directement transmis par proxy à l'origine.

Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'ayant pas pu être satisfaite par un objet du cache, le serveur a transmis la demande à l'origine et retourné le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé un code d'erreur HTTP 503, car la capacité était insuffisante pour servir l'objet au moment de la demande.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`). Si la valeur du champ `sc-status` est `200`, ou si la valeur

de ce champ est `Error` et que la valeur du champ `x-edge-response-result-type` est différente de `Error`, cela signifie que la demande HTTP a réussi mais que le client a été déconnecté avant de recevoir tous les octets.

- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.

26. **`fle-encrypted-fields`**

    Nombre de champs de chiffrement au niveau des champs que le serveur a chiffrés et transmis à l'origine. CloudFront les serveurs transmettent la demande traitée à l'origine au fur et à mesure qu'ils chiffrent les données. Ce champ peut donc avoir une valeur même si la valeur de `fle-status` est une erreur.

27. **`fle-status`**

    Lorsque le chiffrement au niveau du champ est configuré pour une distribution, ce champ contient un code indiquant si le corps de la demande a bien été traité. Quand le serveur traite le corps de la demande, chiffre les valeurs dans les champs spécifiés et transfère la demande à l'origine correctement, la valeur de ce champ est `Processed`. La valeur `x-edge-result-type` peut toujours indiquer une erreur côté client ou côté serveur dans ce cas.

    Les valeurs possibles pour ce champ sont les suivantes :

    - `ForwardedByContentType` – Le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car aucun type de contenu n'était configuré.
    - `ForwardedByQueryArgs` : le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car la demande contient un argument de requête qui n'était pas dans la configuration du chiffrement au niveau du champ.
    - `ForwardedDueToNoProfile` – Le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car aucun profil n'était spécifié dans la configuration du chiffrement au niveau du champ.
    - `MalformedContentTypeClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format de la valeur de l'en-tête `Content-Type` n'était pas valide.
    - `MalformedInputClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format du corps de la requête n'était pas valide.
    - `MalformedQueryArgsClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car un argument de requête était vide ou son format n'était pas valide.

- `RejectedByContentType` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun type de contenu n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `RejectedByQueryArgs` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun argument de requête n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `ServerError` – Le serveur d'origine a renvoyé une erreur.

Si la demande dépasse un quota de chiffrement au niveau du champ (précédemment appelé limite), ce champ contient l'un des codes d'erreur suivants, et le serveur renvoie le code d'état HTTP 400 à l'utilisateur. Pour obtenir une liste des quotas actuels de chiffrement au niveau du champ, consultez Quotas sur le chiffrement au niveau du champ.

- `FieldLengthLimitClientError` – Un champ configuré pour être chiffré a dépassé la longueur maximale autorisée.
- `FieldNumberLimitClientError` – Une demande de configuration de la distribution pour le chiffrement contient un nombre de champs supérieur à celui autorisé.
- `RequestLengthLimitClientError` – La longueur du corps de la demande dépasse la longueur maximale autorisée lorsque le chiffrement au niveau du champ est configuré.

28 **`sc-content-type`**

Valeur de l'en-tête `Content-Type` HTTP de la réponse.

29 **`sc-content-len`**

Valeur de l'en-tête `Content-Length` HTTP de la réponse.

30 **`sc-range-start`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de début de plage.

31 **`sc-range-end`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de fin de plage.

32 **`c-port`**

Numéro de port de la demande depuis l'utilisateur.

33 **`x-edge-detailed-result-type`**

Ce champ contient la même valeur que le champ `x-edge-result-type`, sauf dans les cas suivants :

- Lorsque l'objet a été servi à l'utilisateur à partir de la couche Origin Shield, ce champ contient `OriginShieldHit`.
- Lorsque l'objet n'était pas dans le CloudFront cache et que la réponse a été générée par une fonction Lambda @Edge de demande d'origine, ce champ contient. `MissGeneratedResponse`
- Lorsque la valeur du champ `x-edge-result-type` est `Error`, ce champ contient l'une des valeurs suivantes et présente des informations supplémentaires sur l'erreur :
  - `AbortedOrigin` – Le serveur a rencontré un problème avec l'origine.
  - `ClientCommError` – La réponse à l'utilisateur a été interrompue en raison d'un problème de communication entre le serveur et l'utilisateur.
  - `ClientGeoBlocked` : la distribution est configurée de manière à refuser les demandes en provenance de l'emplacement géographique de l'utilisateur.
  - `ClientHungUpRequest` – La visionneuse s'est arrêtée prématurément lors de l'envoi de la demande.
  - `Error` : une erreur s'est produite pour laquelle le type d'erreur ne correspond à aucune des autres catégories. Ce type d'erreur peut se produire lorsque le serveur sert une réponse d'erreur à partir du cache.
  - `InvalidRequest` – Le serveur a reçu une demande non valide de la part de l'utilisateur.
  - `InvalidRequestBlocked` – L'accès à la ressource demandée est bloqué.
  - `InvalidRequestCertificate` : la distribution ne correspond pas au certificat SSL/TLS pour lequel la connexion HTTPS a été établie.
  - `InvalidRequestHeader` – La demande contenait un en-tête non valide.
  - `InvalidRequestMethod` – La distribution n'est pas configurée pour gérer la méthode de demande HTTP utilisée. Cela peut se produire lorsque la distribution prend en charge uniquement les demandes pouvant être mises en cache.
  - `OriginCommError` – La demande a expiré lors de la connexion à l'origine ou lors de la lecture de données à partir de l'origine.
  - `OriginConnectError` : le serveur n'a pas pu se connecter à l'origine.
  - `OriginContentRangeLengthError` : l'en-tête `Content-Length` de la réponse de l'origine ne correspond pas à la longueur de l'en-tête `Content-Range`.
  - `OriginDnsError` : le serveur n'a pas pu résoudre le nom de domaine de l'origine.

- `OriginError` — L'origine a renvoyé une réponse incorrecte.
- `OriginHeaderTooBigError` – Un en-tête renvoyé par l'origine est trop volumineux pour être traité.
- `OriginInvalidResponseError` — L'origine a renvoyé une réponse non valide.
- `OriginReadError` : le serveur n'a pas pu lire à partir de l'origine.
- `OriginWriteError` : le serveur n'a pas pu écrire à l'origine.
- `OriginZeroSizeObjectError` — Un objet de taille zéro envoyé depuis l'origine a provoqué une erreur.
- `SlowReaderOriginError` — La visionneuse a été lente à lire le message qui a provoqué l'erreur d'origine.

34 **`c-country`**

Code de pays qui représente l'emplacement géographique de l'utilisateur, déterminé par l'adresse IP de l'utilisateur. Pour obtenir une liste des codes de pays, consultez ISO 3166-1 alpha-2.

35 **`cs-accept-encoding`**

Valeur de l'en-tête `Accept-Encoding` dans la demande de l'utilisateur.

36 **`cs-accept`**

Valeur de l'en-tête `Accept` dans la demande de l'utilisateur.

37 **`cache-behavior-path-pattern`**

Modèle de chemin qui identifie le comportement du cache correspondant à la demande de l'utilisateur.

38 **`cs-headers`**

En-têtes HTTP (noms et valeurs) dans la demande de l'utilisateur.

> **Note**
>
> Ce champ est tronqué à 800 octets.

39 **`cs-header-names`**

Noms des en-têtes HTTP (et non des valeurs) dans la demande de l'utilisateur.

> **Note**
>
> Ce champ est tronqué à 800 octets.

40 **`cs-headers-count`**

Nombre d'en-têtes HTTP dans la demande de l'utilisateur.

41 **`origin-fbl`**

Le nombre de secondes de latence du premier octet entre CloudFront et votre origine.

42 **`origin-lbl`**

Le nombre de secondes de latence du dernier octet entre CloudFront et votre origine.

43 **`asn`**

Numéro de système autonome (ASN) de l'utilisateur.

44 **`primary-distribution-id`**

Lorsque le déploiement continu est activé, cet ID identifie la distribution principale de la distribution actuelle.

45 **`primary-distribution-dns-name`**

Lorsque le déploiement continu est activé, cette valeur indique le nom de domaine principal associé à la CloudFront distribution actuelle (par exemple, d111111abcdef8.cloudfront.net).

> **Champs CMCD dans les journaux en temps réel**
>
> Pour plus d'informations sur ces champs, consultez le document CTA Specification Web Application Video Ecosystem - Common Media Client Data CTA-5004.

46 **`cmcd-encoded-bitrate`**

Débit codé de l'objet audio ou vidéo demandé.

47 **`cmcd-buffer-length`**

La longueur de la mémoire tampon de l'objet multimédia demandé.

48 **`cmcd-buffer-starvation`**

Si la mémoire tampon a été épuisée à un moment donné entre la demande précédente et la demande d'objet. Cela peut entraîner une mise en mémoire tampon du lecteur, ce qui peut bloquer la lecture vidéo ou audio.

49. **`cmcd-content-id`**

    Chaîne unique qui identifie le contenu actuel.

50. **`cmcd-object-duration`**

    Durée de lecture de l'objet demandé (en millisecondes).

51. **`cmcd-deadline`**

    Date limite à compter de la date de demande pendant laquelle le premier échantillon de cet objet doit être disponible, afin d'éviter un état de sous-utilisation de la mémoire tampon ou d'autres problèmes de lecture.

52. **`cmcd-measured-throughput`**

    Le débit entre le client et le serveur, tel que mesuré par le client.

53. **`cmcd-next-object-request`**

    Le chemin relatif du prochain objet demandé.

54. **`cmcd-next-range-request`**

    Si la demande suivante est une demande d'objet partielle, cette chaîne indique la plage d'octets à demander.

55. **`cmcd-object-type`**

    Type de média de l'objet actuellement demandé.

56. **`cmcd-playback-rate`**

    1 si vous jouez en temps réel, 2 si vous êtes à double vitesse, 0 si vous ne jouez pas.

57. **`cmcd-requested-maximum-throughput`**

    Le débit maximal demandé que le client considère comme suffisant pour la livraison des actifs.

58. **`cmcd-streaming-format`**

    Le format de streaming qui définit la demande en cours.

59. **`cmcd-session-id`**

GUID identifiant la session de lecture en cours.

60. **`cmcd-stream-type`**

    Jeton identifiant la disponibilité du segment. `v`= tous les segments sont disponibles. `l`= les segments deviennent disponibles au fil du temps.

61. **`cmcd-startup`**

    La clé est incluse sans valeur si l'objet est requis de toute urgence lors du démarrage, de la recherche ou de la restauration après un événement de vide dans la mémoire tampon.

62. **`cmcd-top-bitrate`**

    Le rendu le plus haut débit que le client peut lire.

63. **`cmcd-version`**

    Version de cette spécification utilisée pour interpréter les noms et valeurs de clé définis. Si cette clé est omise, le client et le serveur doivent interpréter les valeurs telles qu'elles sont définies par la version 1.

Point de terminaison (flux de données Kinesis)

Le point de terminaison contient des informations sur le flux de données Kinesis dans lequel vous souhaitez envoyer des journaux en temps réel. Vous fournissez Amazon Resource Name (ARN) du flux de données.

Pour plus d'informations sur la création d'un flux de données Kinesis, consultez les rubriques suivantes du Guide de l'utilisateur Amazon Kinesis Data Streams.

- Gestion de flux à l’aide de la console
- Effectuez des opérations de base sur le flux de données Kinesis à l'aide du AWS CLI
- Création d'un flux (utilise le AWS SDK for Java)

Lorsque vous créez un flux de données, vous devez spécifier le nombre de partitions. Utilisez les informations suivantes pour vous aider à estimer le nombre de partitions dont vous avez besoin.

Pour estimer le nombre de partitions pour votre flux de données Kinesis

1. Calculez (ou estimez) le nombre de demandes par seconde reçues par votre CloudFront distribution.

Vous pouvez utiliser les rapports CloudFront d'utilisation (dans la CloudFront console) et les CloudFront métriques (dans les CloudWatch consoles CloudFront et Amazon) pour vous aider à calculer le nombre de demandes par seconde.

2. Déterminez la taille type d'un seul enregistrement en temps réel.

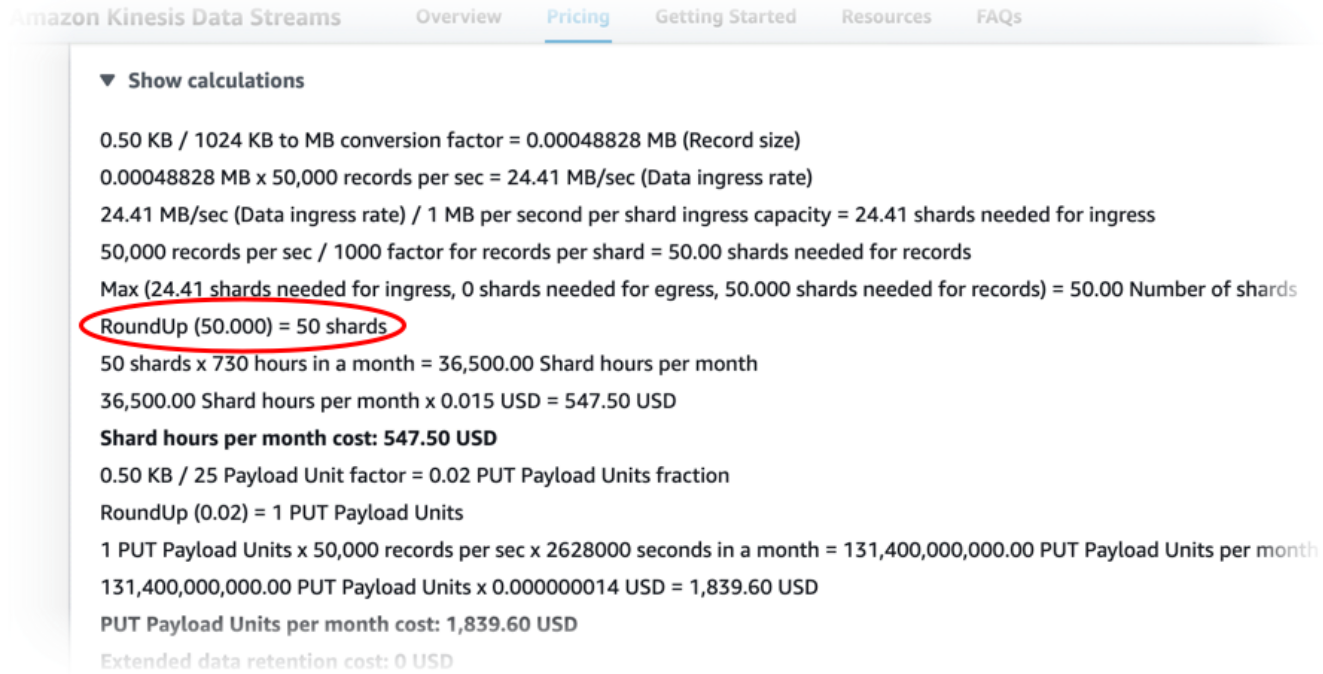
   En général, un seul enregistrement de journal est d'environ 500 octets. Un enregistrement volumineux qui contient tous les champs disponibles est généralement d'environ 1 Ko.

   Si vous ne connaissez pas la taille de vos enregistrements, vous pouvez activer les journaux en temps réel avec un faible taux d'échantillonnage (par exemple, 1 %), puis calculer la taille moyenne des enregistrements en utilisant les données de surveillance dans Kinesis Data Streams (nombre total d'octets entrants divisé par le nombre total d'enregistrements).

3. Dans le Calculateur de tarification de la page de tarification d'Amazon Kinesis Data Streams, entrez le nombre de demandes (enregistrements) par seconde et la taille moyenne de l'enregistrement d'un unique enregistrement de journal. Sélectionnez ensuite Show calculations (Afficher les calculs).

   Le calculateur de tarification vous indique le nombre de partitions nécessaire. (Il affiche également le coût estimé.)

   L'exemple suivant montre que pour une taille moyenne d'enregistrement de 0,5 Ko et 50 000 demandes par seconde, vous avez besoin de 50 partitions.



Rôle IAM

Rôle AWS Identity and Access Management (IAM) qui CloudFront autorise la transmission de journaux en temps réel à votre flux de données Kinesis.

Lorsque vous créez une configuration de journal en temps réel avec la CloudFront console, vous pouvez choisir Créer un nouveau rôle de service pour permettre à la console de créer le rôle IAM pour vous.

Lorsque vous créez une configuration de journal en temps réel avec AWS CloudFormation l' CloudFrontAPI (AWS CLI ou le SDK), vous devez créer vous-même le rôle IAM et fournir l'ARN du rôle. Pour créer le rôle IAM vous-même, utilisez les politiques suivantes.

Stratégie d’approbation de rôle IAM

Pour utiliser la stratégie d'approbation de rôle IAM suivante, remplacez *111122223333*par votre numéro de Compte AWS . L'`Condition`élément de cette politique permet d'éviter le problème de confusion des adjoints, car ils ne CloudFront peuvent assumer ce rôle qu'au nom d'une distribution de votre entreprise Compte AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Stratégie d’autorisations de rôle IAM pour un flux de données non chiffré

Pour appliquer la politique suivante, remplacez *arn:aws:kinesis:us-east-2:123456789012:stream/ par l'ARN de votre flux de données Kinesis*. StreamName

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        }
    ]
}
```

Stratégie d'autorisations de rôle IAM pour un flux de données chiffré

Pour appliquer la politique suivante, remplacez arn:aws:kinesis:us-east- 2:123456789012:stream/ par l'ARN de votre flux de données Kinesis et arn:aws:kms:us-east- 2:123456789012:key/e58a3d0b-fe4f-4047-a495-ae03cc73d486 par l'StreamNameARN de votre. AWS KMS key

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-
ae03cc73d486"
            ]
        }
    ]
}
```

Création et utilisation de configurations de journaux en temps réel

Vous pouvez utiliser une configuration de journal en temps réel pour obtenir des informations sur les demandes faites à une distribution en temps réel (les journaux sont livrés en quelques secondes après la réception des demandes). Vous pouvez créer une configuration de journal en temps réel dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Pour utiliser une configuration de journal en temps réel, vous devez l'associer à un ou plusieurs comportements de cache dans une CloudFront distribution.

Créer une configuration de journal en temps réel (console)

Pour créer une configuration de journal en temps réel

1. Connectez-vous à la page Logs AWS Management Console et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/logs.
2. Choisissez l'onglet Configurations en temps réel.
3. Choisissez Create configuration (Créer une configuration).
4. Dans Nom, entrez le nom de la configuration.
5. Pour Taux d'échantillonnage, entrez le pourcentage de demandes pour lesquelles vous souhaitez recevoir des enregistrements de journal.
6. Pour les champs, choisissez les champs à recevoir dans les journaux en temps réel.
   - Pour inclure tous les champs CMCD pour vos journaux, choisissez CMCD all keys.

7. Pour Endpoint, choisissez un ou plusieurs flux de données Kinesis pour recevoir des journaux en temps réel.

> **Note**
>
> CloudFront les journaux en temps réel sont transmis au flux de données que vous spécifiez dans Kinesis Data Streams. Pour lire et analyser vos journaux en temps réel, vous pouvez créer votre propre consommateur de flux de données Kinesis. Vous pouvez également utiliser Firehose pour envoyer les données du journal à Amazon S3, Amazon Redshift, Amazon Service ou à un service de traitement des journaux tiers. OpenSearch

8. Pour le rôle IAM, choisissez Créer un nouveau rôle de service ou choisissez un rôle existant. Vous devez être autorisé à créer des rôles IAM.
9. (Facultatif) Pour Distribution, choisissez un comportement CloudFront de distribution et de cache à associer à la configuration du journal en temps réel.
10. Choisissez Create configuration (Créer une configuration).

En cas de réussite, la console affiche les détails de la configuration du journal en temps réel que vous venez de créer.

Pour plus d'informations, consultez Comprendre les configurations en temps réel.

Créer une configuration de journal en temps réel (AWS CLI)

Pour créer une configuration de journal en temps réel avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-realtime-log-config commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une configuration de journal en temps réel (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `rtl-config.yaml` qui contient tous les paramètres d'entrée de la commande create-realtime-log-config.

```
aws cloudfront create-realtime-log-config --generate-cli-skeleton yaml-input > rtl-config.yaml
```

2. Ouvrez le fichier nommé `rtl-config.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de configuration du journal en temps réel que vous souhaitez, puis enregistrez le fichier. Remarques :

   - Pour `StreamType`, la seule valeur valide est `Kinesis`.

   Pour de plus amples informations sur les paramètres de configuration longue durée en temps réel, veuillez consulter Comprendre les configurations en temps réel.

3. Utilisez la commande suivante pour créer la configuration du journal en temps réel à l'aide des paramètres d'entrée du fichier `rtl-config.yaml`.

```
aws cloudfront create-realtime-log-config --cli-input-yaml file://rtl-config.yaml
```

En cas de réussite, la sortie de la commande affiche les détails de la configuration du journal en temps réel que vous venez de créer.

Pour attacher une configuration de journal en temps réel à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml > dist-
config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour pour utiliser une configuration de journal en temps réel.

   - Dans le comportement du cache, ajoutez un champ nommé `RealtimeLogConfigArn`. Pour la valeur du champ, utilisez l'ARN de la configuration du journal en temps réel que vous souhaitez attacher à ce comportement de cache.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la configuration du journal en temps réel. Remplacez *distribution_ID* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

En cas de réussite, la sortie de la commande affiche les détails de la distribution que vous venez de mettre à jour.

Créer une configuration de journal en temps réel (API)

Pour créer une configuration de journal en temps réel avec l' CloudFront API, utilisez CreateRealtimeLogConfig. Pour plus d'informations sur les paramètres que vous spécifiez dans cet appel d'API, consultez Comprendre les configurations en temps réel la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une configuration de journal en temps réel, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ARN de la configuration du journal en temps réel dans le champ `RealtimeLogConfigArn`, à l'intérieur d'un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence des paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Création d'un consommateur Kinesis Data Streams

Pour lire et analyser vos journaux en temps réel, vous créez ou utilisez un consommateur Kinesis Data Streams. Lorsque vous créez un consommateur pour les journaux CloudFront en temps réel, il est important de savoir que les champs de chaque enregistrement de journal en temps réel sont

toujours livrés dans le même ordre, comme indiqué dans la Champs section. Assurez-vous que vous créez votre consommateur en fonction de cet ordre fixe.

Prenons l'exemple d'une configuration de journal en temps réel qui inclut uniquement les trois champs suivants : `time-to-first-byte`, `sc-status` et `c-country`. Dans ce scénario, le dernier champ, `c-country`, est toujours le champ numéro 3 dans chaque enregistrement de journal. Toutefois, si vous ajoutez ultérieurement des champs à la configuration du journal en temps réel, le placement de chaque champ dans un enregistrement peut changer.

Par exemple, si vous ajoutez les champs `sc-bytes` et `time-taken` à la configuration du journal en temps réel, ces champs sont insérés dans chaque enregistrement de journal selon l'ordre indiqué à la section Champs. L'ordre final des cinq champs est `time-to-first-byte`, `sc-status`, `sc-bytes`, `time-taken` et `c-country`. Le champ `c-country` était à l'origine le champ numéro 3, mais il est maintenant le champ numéro 5. Assurez-vous que votre application grand public peut gérer les champs qui changent de position dans un enregistrement de journal, au cas où vous ajouteriez des champs à votre configuration de journal en temps réel.

Résolution des problèmes de journaux en temps réel

Une fois que vous avez créé une configuration de journal en temps réel, vous pouvez constater qu'aucun enregistrement (ou seulement certains d'entre eux) n'est remis à Kinesis Data Streams. Dans ce cas, vous devez d'abord vérifier que votre CloudFront distribution reçoit les demandes des spectateurs. Le cas échéant, vous pouvez vérifier le paramètre suivant pour poursuivre le dépannage.

Autorisations de rôle IAM

> Pour fournir des enregistrements de journal en temps réel à votre flux de données Kinesis, CloudFront utilisez le rôle IAM dans la configuration des journaux en temps réel. Assurez-vous que la stratégie d'approbation de rôle et la stratégie d'autorisations de rôle correspondent aux stratégies indiquées dans Rôle IAM.

Limitation des Kinesis Data Streams

> Si vous CloudFront enregistrez des enregistrements de journal en temps réel dans votre flux de données Kinesis plus rapidement que ce dernier ne peut le gérer, Kinesis Data Streams peut limiter le nombre de demandes provenant de. CloudFront Dans ce cas, vous pouvez augmenter le nombre de partitions dans votre flux de données Kinesis. Chaque partition peut prendre en charge des écritures jusqu'à 1 000 enregistrements par seconde, jusqu'à un maximum d'écritures de données de 1 Mo par seconde.

Journaux des fonctions Edge

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Accédez aux journaux à l'aide de la CloudWatch console ou de l'API CloudWatch Logs.

> **Important**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes. CloudFront fournit des journaux des fonctions de pointe dans les meilleures conditions. L'entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Quand une entrée de journal est omise des journaux de fonctions de périphérie, le nombre d'entrées des journaux de fonctions de périphérie ne correspond pas à l'utilisation qui apparaît dans les rapports d'utilisation et de facturation AWS .

Journaux Lambda@Edge

Lambda @Edge envoie automatiquement les journaux des fonctions à Logs, créant ainsi des flux de CloudWatch journaux dans l' Régions AWS endroit où les fonctions sont exécutées. Le nom du groupe de journaux est formaté comme `/aws/lambda/us-east-1.`*`function-name`* suit : où *`function-name`* est le nom que vous avez donné à la fonction lorsque vous l'avez créée et où `us-east-1` est le code de région Région AWS où la fonction a été créée. Le nom du groupe de journaux contient toujours`us-east-1`, même pour les groupes de journaux des autres régions dans lesquelles votre fonction s'exécute.

> **Note**
>
> Lambda@Edge limite les journaux en fonction du volume de la demande et de la taille des journaux.

Vous devez examiner correctement les fichiers CloudWatch journaux Région AWS pour voir les fichiers journaux de vos fonctions Lambda @Edge. Pour voir les régions dans lesquelles votre fonction Lambda @Edge est exécutée, consultez les graphiques des métriques de la fonction dans la CloudFront console. Les métriques sont affichées pour chaque Région AWS. Sur la même page,

vous pouvez choisir une région et afficher les fichiers journaux pour cette région afin de pouvoir rechercher des problèmes.

Pour en savoir plus sur l'utilisation des CloudWatch journaux avec les fonctions Lambda @Edge, consultez les rubriques suivantes :

- Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezthe section called “Surveillance CloudFront des métriques avec Amazon CloudWatch”.
- Pour plus d'informations sur les autorisations requises pour envoyer des données à CloudWatch Logs, consultezthe section called “Configuration des autorisations et des rôles IAM”.
- Pour plus d'informations sur l'ajout de la journalisation à une fonction Lambda, consultez Journalisation des fonctions AWS Lambda dans Node.js ou Journalisation des fonctions AWS Lambda dans Python dans le Guide du développeur AWS Lambda .
- Pour plus d'informations sur CloudWatch les quotas de journaux (anciennement appelés limites), consultez la section Quotas de CloudWatch journaux dans le guide de l'utilisateur Amazon CloudWatch Logs.

CloudFront Journaux de fonctions

Si le code d'une CloudFront fonction contient des `console.log()` instructions, CloudFront Functions envoie automatiquement ces lignes de journal à CloudWatch Logs. S'il n'y a aucune `console.log()` déclaration, rien n'est envoyé à CloudWatch Logs.

CloudFront Functions crée toujours des flux de journaux dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`), quel que soit l'emplacement périphérique sur lequel la fonction a été exécutée. Le nom du groupe de journaux est au format `/aws/cloudfront/function/`*`FunctionName`*, où *`FunctionName`* est le nom que vous avez donné à la fonction lors de sa création. Le nom du flux de journal est au format `YYYY/M/D/`*`UUID`*.

Voici un exemple de message de journal envoyé à CloudWatch Logs. Chaque ligne commence par un identifiant qui identifie de manière unique une CloudFront demande. Le message commence par une `START` ligne qui inclut l'ID CloudFront de distribution et se termine par une `END` ligne. Entre les lignes `START` et `END` se trouvent les lignes de journal générées par les instructions `console.log()` de la fonction.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADAXZZ
```

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== Example function log output
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

> **Note**
>
> CloudFront Functions envoie des journaux CloudWatch uniquement pour les fonctions de la `LIVE` phase qui s'exécutent en réponse aux demandes et réponses de production. Lorsque vous testez une fonction, CloudFront elle n'envoie aucun journal à CloudWatch. Le résultat du test contient des informations sur les erreurs, l'utilisation du calcul et les journaux de fonctionnement (`console.log()`instructions), mais ces informations ne sont pas envoyées à CloudWatch.

CloudFront Functions utilise un rôle lié à un service AWS Identity and Access Management (IAM) pour envoyer les journaux aux CloudWatch journaux de votre compte. Un rôle lié à un service est un rôle IAM directement lié à un service. AWS Les rôles liés au service sont prédéfinis par le service et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. CloudFront Functions utilise un rôle lié à un service appelé. AWSServiceRoleForCloudFrontLogger Pour plus d'informations sur ce rôle, consultez the section called “Rôles liés à un service pour Lambda@Edge” (Lambda@Edge utilise le même rôle lié au service).

Lorsqu'une fonction échoue en raison d'une erreur de validation ou d'exécution, les informations sont enregistrées dans les CloudFront journaux standard et les journaux en temps réel. Les informations relatives à l'erreur sont consignées dans les champs `x-edge-result-type`, `x-edge-response-result-type` et `x-edge-detailed-result-type`.

Journalisation des appels d' CloudFront API Amazon à l'aide de AWS CloudTrail

CloudFront est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API CloudFront sous forme d'événements. Les appels capturés incluent des appels provenant de la CloudFront console et des appels de code vers les opérations de l' CloudFront API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite CloudFront, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

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 effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur de l'IAM Identity Center.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous pouvez créer un parcours à région unique ou multirégionale à l'aide du. AWS CLI Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un parcours à région unique, vous ne pouvez voir que les événements enregistrés dans le parcours. Région AWS Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

> **Note**
>
> CloudFront est un service mondial. CloudTrail enregistre des événements CloudFront dans la région de l'est des États-Unis (Virginie du Nord). Pour plus d'informations, consultez la section Événements de service mondiaux dans le Guide de AWS CloudTrail l'utilisateur.
> Si vous utilisez des informations d'identification de sécurité temporaires en utilisant AWS Security Token Service, les appels vers les points de terminaison régionaux`us-west-2`, tels que, sont connectés CloudTrail à la région appropriée.
> Pour plus d'informations sur les CloudFront points de terminaison, consultez la section CloudFront Points de terminaison et quotas dans le. Références générales AWS

CloudFront événements de données dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture dans une CloudFront distribution). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail

n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de CloudFront ressources à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de consigner les événements liés aux données, consultez les sections Enregistrement des événements liés aux données avec le AWS Management Console et Enregistrement des événements liés aux données avec le AWS Command Line Interface dans le Guide de AWS CloudTrail l'utilisateur.

Le tableau suivant répertorie les types de CloudFront ressources pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide des API or. AWS CLI CloudTrail La CloudTrail colonne Data APIs logged to indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail
CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`	• DeleteKeys • DescribeKeyValueStore • GetKey • ListKeys • PutKeys • UpdateKeys

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les `eventName`, `readOnly`, et `resources.ARN` des champs pour enregistrer uniquement les événements importants pour vous. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelectorla référence de l'AWS CloudTrail API.

CloudFront événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Amazon CloudFront enregistre toutes les opérations CloudFront du plan de contrôle en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de CloudFront contrôle Amazon auxquelles CloudFront se connecte CloudTrail, consultez le Amazon CloudFront API Reference.

CloudFront exemples d'événements

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Table des matières

Exemple : UpdateDistribution

L'exemple suivant montre un CloudTrail événement illustrant l'UpdateDistributionopération.

Pour les appels à l' CloudFront API, `eventSource` c'est`cloudfront.amazonaws.com`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:role-session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/role-session-name",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
```

```
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-02-02T19:23:50Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-02-02T19:26:01Z",
    "eventSource": "cloudfront.amazonaws.com",
    "eventName": "UpdateDistribution",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "52.94.133.137",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36",
    "requestParameters": {
        "distributionConfig": {
            "defaultRootObject": "",
            "aliases": {
                "quantity": 3,
                "items": [
                    "alejandro_rosalez.awsps.myinstance.com",
                    "cross-testing.alejandro_rosalez.awsps.myinstance.com",
                    "*.alejandro_rosalez.awsps.myinstance.com"
                ]
            },
            "cacheBehaviors": {
                "quantity": 0,
                "items": []
            },
            "httpVersion": "http2and3",
            "originGroups": {
                "quantity": 0,
                "items": []
            },
            "viewerCertificate": {
                "minimumProtocolVersion": "TLSv1.2_2021",
                "cloudFrontDefaultCertificate": false,
                "aCMCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                "sSLSupportMethod": "sni-only"
            },
```

```
            "webACLId": "arn:aws:wafv2:us-east-1:111122223333:global/webacl/testing-
acl/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "customErrorResponses": {
                "quantity": 0,
                "items": []
            },
            "logging": {
                "includeCookies": false,
                "prefix": "",
                "enabled": false,
                "bucket": ""
            },
            "priceClass": "PriceClass_All",
            "restrictions": {
                "geoRestriction": {
                    "restrictionType": "none",
                    "quantity": 0,
                    "items": []
                }
            },
            "isIPV6Enabled": true,
            "callerReference": "1578329170895",
            "continuousDeploymentPolicyId": "",
            "enabled": true,
            "defaultCacheBehavior": {
                "targetOriginId": "d111111abcdef8",
                "minTTL": 0,
                "compress": false,
                "maxTTL": 31536000,
                "functionAssociations": {
                    "quantity": 0,
                    "items": []
                },
                "trustedKeyGroups": {
                    "quantity": 0,
                    "items": [],
                    "enabled": false
                },
                "smoothStreaming": false,
                "fieldLevelEncryptionId": "",
                "defaultTTL": 86400,
                "lambdaFunctionAssociations": {
                    "quantity": 0,
                    "items": []
```

```
                },
                "viewerProtocolPolicy": "redirect-to-https",
                "forwardedValues": {
                    "cookies": {"forward": "none"},
                    "queryStringCacheKeys": {
                        "quantity": 0,
                        "items": []
                    },
                    "queryString": false,
                    "headers": {
                        "quantity": 1,
                        "items": ["*"]
                    }
                },
                "trustedSigners": {
                    "items": [],
                    "enabled": false,
                    "quantity": 0
                },
                "allowedMethods": {
                    "quantity": 2,
                    "items": [
                        "HEAD",
                        "GET"
                    ],
                    "cachedMethods": {
                        "quantity": 2,
                        "items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                }
            },
            "staging": false,
            "origins": {
                "quantity": 1,
                "items": [
                    {
                        "originPath": "",
                        "connectionTimeout": 10,
                        "customOriginConfig": {
                            "originReadTimeout": 30,
                            "hTTPSPort": 443,
```

```
                        "originProtocolPolicy": "https-only",
                        "originKeepaliveTimeout": 5,
                        "hTTPPort": 80,
                        "originSslProtocols": {
                            "quantity": 3,
                            "items": [
                                "TLSv1",
                                "TLSv1.1",
                                "TLSv1.2"
                            ]
                        }
                    },
                    "id": "d111111abcdef8",
                    "domainName": "d111111abcdef8.cloudfront.net",
                    "connectionAttempts": 3,
                    "customHeaders": {
                        "quantity": 0,
                        "items": []
                    },
                    "originShield": {"enabled": false},
                    "originAccessControlId": ""
                }
            ]
        },
        "comment": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "id": "EDFDVBD6EXAMPLE",
    "ifMatch": "E1RTLUR9YES76O"
},
"responseElements": {
    "distribution": {
        "activeTrustedSigners": {
            "quantity": 0,
            "enabled": false
        },
        "id": "EDFDVBD6EXAMPLE",
        "domainName": "d111111abcdef8.cloudfront.net",
        "distributionConfig": {
            "defaultRootObject": "",
            "aliases": {
                "quantity": 3,
                "items": [
                    "alejandro_rosalez.awsps.myinstance.com",
                    "cross-testing.alejandro_rosalez.awsps.myinstance.com",
```

```
                        "*.alejandro_rosalez.awsps.myinstance.com"
                    ]
                },
                "cacheBehaviors": {"quantity": 0},
                "httpVersion": "http2and3",
                "originGroups": {"quantity": 0},
                "viewerCertificate": {
                    "minimumProtocolVersion": "TLSv1.2_2021",
                    "cloudFrontDefaultCertificate": false,
                    "aCMCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                    "sSLSupportMethod": "sni-only",
                    "certificateSource": "acm",
                    "certificate": "arn:aws:acm:us-east-1:111122223333:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "webACLId": "arn:aws:wafv2:us-east-1:111122223333:global/webacl/
testing-acl/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
                "customErrorResponses": {"quantity": 0},
                "logging": {
                    "includeCookies": false,
                    "prefix": "",
                    "enabled": false,
                    "bucket": ""
                },
                "priceClass": "PriceClass_All",
                "restrictions": {
                    "geoRestriction": {
                        "restrictionType": "none",
                        "quantity": 0
                    }
                },
                "isIPV6Enabled": true,
                "callerReference": "1578329170895",
                "continuousDeploymentPolicyId": "",
                "enabled": true,
                "defaultCacheBehavior": {
                    "targetOriginId": "d111111abcdef8",
                    "minTTL": 0,
                    "compress": false,
                    "maxTTL": 31536000,
                    "functionAssociations": {"quantity": 0},
                    "trustedKeyGroups": {
                        "quantity": 0,
```

```
                    "enabled": false
                },
                "smoothStreaming": false,
                "fieldLevelEncryptionId": "",
                "defaultTTL": 86400,
                "lambdaFunctionAssociations": {"quantity": 0},
                "viewerProtocolPolicy": "redirect-to-https",
                "forwardedValues": {
                    "cookies": {"forward": "none"},
                    "queryStringCacheKeys": {"quantity": 0},
                    "queryString": false,
                    "headers": {
                        "quantity": 1,
                        "items": ["*"]
                    }
                },
                "trustedSigners": {
                    "enabled": false,
                    "quantity": 0
                },
                "allowedMethods": {
                    "quantity": 2,
                    "items": [
                        "HEAD",
                        "GET"
                    ],
                    "cachedMethods": {
                        "quantity": 2,
                        "items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                }
            },
            "staging": false,
            "origins": {
                "quantity": 1,
                "items": [
                    {
                        "originPath": "",
                        "connectionTimeout": 10,
                        "customOriginConfig": {
                            "originReadTimeout": 30,
```

```
                            "hTTPSPort": 443,
                            "originProtocolPolicy": "https-only",
                            "originKeepaliveTimeout": 5,
                            "hTTPPort": 80,
                            "originSslProtocols": {
                                "quantity": 3,
                                "items": [
                                    "TLSv1",
                                    "TLSv1.1",
                                    "TLSv1.2"
                                ]
                            }
                        },
                        "id": "d111111abcdef8",
                        "domainName": "d111111abcdef8.cloudfront.net",
                        "connectionAttempts": 3,
                        "customHeaders": {"quantity": 0},
                        "originShield": {"enabled": false},
                        "originAccessControlId": ""
                    }
                ]
            },
            "comment": "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "aliasICPRecordals": [
            {
                "cNAME": "alejandro_rosalez.awsps.myinstance.com",
                "iCPRecordalStatus": "APPROVED"
            },
            {
                "cNAME": "cross-testing.alejandro_rosalez.awsps.myinstance.com",
                "iCPRecordalStatus": "APPROVED"
            },
            {
                "cNAME": "*.alejandro_rosalez.awsps.myinstance.com",
                "iCPRecordalStatus": "APPROVED"
            }
        ],
        "aRN": "arn:aws:cloudfront::111122223333:distribution/EDFDVBD6EXAMPLE",
        "status": "InProgress",
        "lastModifiedTime": "Feb 2, 2024 7:26:01 PM",
        "activeTrustedKeyGroups": {
            "enabled": false,
            "quantity": 0
```

```
            },
            "inProgressInvalidationBatches": 0
        },
        "eTag": "E1YHBLAB2BJY1G"
    },
    "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
    "eventID": "5ab02562-0fc5-43d0-b7b6-90293example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "apiVersion": "2020_05_31",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudfront.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Exemple : UpdateKeys

L'exemple suivant montre un CloudTrail événement illustrant l'UpdateKeysopération.

Pour les appels à l' CloudFront KeyValueStore API, le `eventSource` est `edgekeyvaluestore.amazonaws.com` au lieu de`cloudfront.amazonaws.com`.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:role-session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/role-session-name",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2023-11-01T23:41:14Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-01T23:41:28Z",
    "eventSource": "edgekeyvaluestore.amazonaws.com",
    "eventName": "UpdateKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.235.183.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36,
    "requestParameters": {
        "kvsARN": "arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "ifMatch": "KV3O6B1CX531EBP",
        "deletes": [
            {"key": "key1"}
        ]
    },
    "responseElements": {
        "itemCount": 0,
        "totalSizeInBytes": 0,
        "eTag": "KVDC9VEVZ71ZGO"
    },
    "requestID": "5ccf104c-acce-4ea1-b7fc-73e33example",
    "eventID": "a0b1b5c7-906c-439d-9925-90293example",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::CloudFront::KeyValueStore",
            "ARN": "arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
```

```
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "111122223333.cloudfront-kvs.global.api.aws"
    }
}
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Suivi des modifications de configuration avec AWS Config

Utilisez-le AWS Config pour enregistrer les modifications de configuration apportées à vos paramètres CloudFront de distribution. Vous pouvez saisir les modifications apportées aux états de distribution, aux classes de prix, aux origines, aux paramètres de restriction géographique et aux configurations Lambda @Edge.

> **Note**
>
> AWS Config n'enregistre pas de balises clé-valeur pour les distributions CloudFront en streaming.

Configurez AWS Config avec CloudFront

Lors de la configuration AWS Config, vous pouvez choisir d'enregistrer toutes les AWS ressources prises en charge ou de n'enregistrer que certaines ressources spécifiques, par exemple en enregistrant les modifications pour CloudFront uniquement. Pour obtenir la liste des CloudFront ressources prises en charge, consultez la CloudFront section Amazon de la rubrique Types de ressources pris en charge dans le Guide du AWS Config développeur.

Pour suivre les modifications de configuration apportées à votre CloudFront distribution, vous devez vous connecter à la CloudFront console dans l'est des États-Unis (Virginie du Nord) Région AWS.

> **Note**
>
> Il se peut qu'il y ait un retard dans l'enregistrement des ressources avec AWS Config. AWS Config enregistre les ressources uniquement après les avoir découvertes.

Console

À configurer AWS Config avec CloudFront (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisir Get Started Now (Démarrer maintenant).
3. Sur la page Paramètres, pour Types de ressources à enregistrer, spécifiez les types de AWS ressources que vous AWS Config souhaitez enregistrer. Si vous souhaitez enregistrer uniquement les CloudFront modifications, choisissez Types spécifiques, puis, sous CloudFront, choisissez la distribution ou la distribution en streaming dont vous souhaitez suivre les modifications.

   Pour ajouter ou modifier les distributions dont vous souhaitez effectuer le suivi, choisissez Settings (Paramètres) sur la gauche, à la fin de votre configuration initiale.
4. Spécifiez les options supplémentaires requises pour AWS Config : configurer une notification, spécifier un emplacement pour les informations de configuration et ajouter des règles pour évaluer les types de ressources.

Pour plus d'informations, consultez la section Configuration à l' AWS Config aide de la console dans le guide du AWS Config développeur.

AWS CLI

Pour configurer à CloudFront l' AWS Config aide du AWS CLI, consultez la section Configuration à l' AWS Config aide de la AWS CLI dans le guide du AWS Config développeur.

AWS Config API

Pour configurer CloudFront l'utilisation AWS Config de l' AWS Config API, consultez l' StartConfigurationRecorderaction et les autres informations dans la référence de l'AWS Config API.

Afficher l'historique CloudFront de configuration

Après avoir AWS Config commencé à enregistrer les modifications de configuration apportées à vos distributions, vous pouvez obtenir l'historique de configuration de toutes les distributions pour lesquelles vous avez configuré les distributions CloudFront.

Vous pouvez consulter l'historique des configurations de différentes manières.

Console

Pour chaque ressource enregistrée, vous pouvez consulter une page chronologique qui fournit un historique des détails de configuration. Pour visualiser cette page, choisissez l'icône grise dans la colonne Chronologie de configuration de la page Hôtes dédiés.

Pour plus d'informations, consultez la section Affichage des détails de configuration dans la AWS Config console dans le guide du AWS Config développeur.

AWS CLI

Pour obtenir la liste de toutes vos distributions, exécutez la list-discovered-resourcescommande, comme indiqué dans l'exemple suivant.

```
aws configservice list-discovered-resources --resource-type
 AWS::CloudFront::Distribution
```

Pour obtenir les détails de configuration d'une distribution pour un intervalle de temps spécifique, exécutez la get-resource-config-historycommande.

Pour plus d'informations, consultez Afficher les détails de configuration à l'aide de la CLI dans le Guide du développeur AWS Config .

AWS Config API

Pour obtenir la liste de toutes vos distributions, utilisez l'ListDiscoveredResourcesaction.

Pour obtenir les détails de configuration d'une distribution pour un intervalle de temps spécifique, utilisez l'GetResourceConfigHistoryaction. Pour plus d'informations, consultez la page Référence de l'API AWS Config.

Sécurité sur Amazon CloudFront

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les 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 conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon CloudFront, consultez la section AWSServices concernés par programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation CloudFront. Les rubriques suivantes expliquent comment procéder à la configuration CloudFront pour atteindre 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 CloudFront ressources.

Rubriques

Protection des données sur Amazon CloudFront

Le modèle de responsabilité AWS partagée de s'applique à la protection des données sur Amazon CloudFront. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. 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 en savoir plus 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 AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur 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 les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des 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 FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus 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 CloudFront ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez 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.

Amazon CloudFront propose plusieurs options que vous pouvez utiliser pour sécuriser le contenu diffusé :

- Configurer les connexions HTTPS.
- Configurez le chiffrement au niveau du champ pour fournir une sécurité supplémentaire pour des données spécifiques pendant le transit.
- Restreindre l'accès au contenu de manière à ce que seules des personnes spécifiques ou des personnes dans une zone spécifique puissent l'afficher.

Les rubriques suivantes expliquent les options plus en détail.

Rubriques

Chiffrement en transit

Pour chiffrer vos données pendant le transfert, vous configurez Amazon de manière CloudFront à ce que les visiteurs utilisent le protocole HTTPS pour demander vos fichiers, afin que les connexions soient cryptées lors des communications CloudFront avec les utilisateurs. Vous pouvez également configurer CloudFront l'utilisation du protocole HTTPS pour obtenir des fichiers depuis votre origine, afin que les connexions soient cryptées lorsque CloudFront vous communiquez avec votre origine.

Pour de plus amples informations, veuillez consulter Utilisez le protocole HTTPS avec CloudFront.

Le chiffrement au niveau du champ ajoute une couche de sécurité avec HTTPS, qui vous permet de protéger des données spécifiques tout au long du traitement du système, pour que seules certaines applications puissent les voir. En configurant le chiffrement au niveau du champ dans CloudFront, vous pouvez télécharger en toute sécurité les informations sensibles soumises par les utilisateurs sur

vos serveurs Web. Les informations sensibles fournies par vos clients sont chiffrées en périphérie plus près de l'utilisateur. Elles restent chiffrées sur l'ensemble de la pile applicative, garantissant ainsi que seules les applications nécessitant les données (et disposant des informations d'identification pour les déchiffrer) puissent y accéder.

Pour de plus amples informations, veuillez consulter Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Les points de terminaison de l' CloudFront API `cloudfront.amazonaws.com` et`cloudfront-fips.amazonaws.com`, n'acceptent que le trafic HTTPS. Cela signifie que lorsque vous envoyez et recevez des informations à l'aide de l' CloudFront API, vos données, y compris les configurations de distribution, les politiques de cache et les politiques de demande d'origine, les groupes de clés et les clés publiques, ainsi que le code de fonction dans CloudFront Functions, sont toujours cryptées pendant le transfert. En outre, toutes les demandes envoyées aux points de terminaison de l' CloudFront API sont signées avec des AWS informations d'identification et connectées. AWS CloudTrail

Le code de fonction et la configuration dans CloudFront Functions sont toujours chiffrés en transit lorsqu'ils sont copiés vers les points de présence périphériques (POP) et entre les autres emplacements de stockage utilisés par CloudFront.

Chiffrement au repos

Le code de fonction et la configuration dans CloudFront Functions sont toujours stockés dans un format crypté sur les POPs de l'emplacement périphérique et dans les autres emplacements de stockage utilisés par CloudFront.

Restreindre l'accès au contenu

De nombreuses entreprises qui distribuent du contenu via Internet veulent limiter l'accès aux documents, données professionnelles, flux multimédias ou contenus destinés à un sous-ensemble d'utilisateurs. Pour diffuser ce contenu en toute sécurité à l'aide d'Amazon CloudFront, vous pouvez effectuer une ou plusieurs des opérations suivantes :

Utiliser des cookies ou des URL signés

> Vous pouvez restreindre l'accès au contenu destiné à des utilisateurs sélectionnés, par exemple des utilisateurs payants, en diffusant ce contenu privé à l' CloudFront aide d'URL signées ou de cookies signés. Pour de plus amples informations, veuillez consulter Diffusez du contenu privé avec des URL signées et des cookies signés.

Restriction de l'accès au contenu dans les compartiments Amazon S3

Si vous limitez l'accès à votre contenu en utilisant, par exemple, des URL CloudFront signées ou des cookies signés, vous ne voudrez pas non plus que les utilisateurs puissent consulter les fichiers en utilisant l'URL directe du fichier. Au lieu de cela, vous souhaitez qu'ils accèdent aux fichiers uniquement en utilisant l'URL CloudFront , afin que vos protections fonctionnent.

Si vous utilisez un compartiment Amazon S3 comme origine pour une CloudFront distribution, vous pouvez configurer un contrôle d'accès à l'origine (OAC) qui permet de restreindre l'accès au compartiment S3. Pour de plus amples informations, veuillez consulter the section called “Restreindre l'accès à une origine Amazon Simple Storage Service”.

Restreindre l'accès au contenu diffusé par un Application Load Balancer

Lorsque vous utilisez CloudFront un Application Load Balancer dans Elastic Load Balancing comme origine, vous pouvez le configurer CloudFront pour empêcher les utilisateurs d'accéder directement à l'Application Load Balancer. Cela permet aux utilisateurs d'accéder à l'Application Load Balancer uniquement par le biais de celui-ci CloudFront, ce qui vous permet de bénéficier des avantages de son utilisation. CloudFront Pour de plus amples informations, veuillez consulter Restreindre l'accès aux équilibreurs de charge des applications.

Utiliser des listes ACL web AWS WAF

Vous pouvez utiliser AWS WAF, un service de pare-feu d'application web, pour créer une liste de contrôle d'accès web (liste ACL web) afin de restreindre l'accès à votre contenu. En fonction des conditions que vous spécifiez, telles que les adresses IP d'où proviennent les demandes ou les valeurs des chaînes de requête, CloudFront répond aux demandes soit avec le contenu demandé, soit avec un code d'état HTTP 403 (interdit). Pour de plus amples informations, veuillez consulter Utilisez des AWS WAF protections.

Utiliser une restriction géographique

Vous pouvez utiliser une restriction géographique, également appelée blocage géographique, pour empêcher les utilisateurs situés à des emplacements géographiques spécifiques d'accéder au contenu que vous desservez via une distribution CloudFront. Il existe plusieurs options au choix lorsque vous configurez des restrictions géographiques. Pour de plus amples informations, veuillez consulter Limitez la distribution géographique de votre contenu.

Identity and Access Management pour Amazon CloudFront

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. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser CloudFront les ressources. 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. CloudFront

Utilisateur du service : si vous utilisez le CloudFront service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles CloudFront fonctionnalités pour effectuer votre travail, vous aurez peut-être 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 CloudFront, consultezRésolution des problèmes d' CloudFront identité et d'accès à Amazon.

Administrateur du service — Si vous êtes responsable des CloudFront ressources de votre entreprise, vous avez probablement un accès complet à CloudFront. C'est à vous de déterminer les CloudFront fonctionnalités et les ressources 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 manière dont votre entreprise peut utiliser IAM avec CloudFront, voirComment Amazon CloudFront travaille avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à. CloudFront Pour consulter

des exemples de politiques CloudFront basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon CloudFront

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 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 en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources 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 au service apparaissent dans votre Compte AWS fichier 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 Amazon CloudFront travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à CloudFront, découvrez les fonctionnalités IAM disponibles. CloudFront

Fonctionnalités IAM que vous pouvez utiliser avec Amazon CloudFront

Fonction IAM	CloudFront soutien
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
Transfert des sessions d'accès (FAS)	Non
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont CloudFront 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 CloudFront

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 politiques basées sur l'identité pour CloudFront

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon CloudFront

Politiques basées sur les ressources au sein de CloudFront

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 Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour CloudFront

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 consulter la liste des CloudFront actions, consultez la section Actions définies par Amazon CloudFront dans le Service Authorization Reference.

Les actions de politique en CloudFront cours utilisent le préfixe suivant avant l'action :

```
cloudfront
```

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

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

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon CloudFront

Ressources politiques pour CloudFront

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 consulter la liste des types de CloudFront ressources et leurs ARN, consultez la section Ressources définies par Amazon CloudFront dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon CloudFront.

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon CloudFront

Clés de conditions de politique pour CloudFront

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 consulter la liste des clés de CloudFront condition, consultez la section Clés de condition pour Amazon CloudFront dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon CloudFront.

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon CloudFront

ACL dans CloudFront

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 CloudFront

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.

CloudFront supporte ABAC pour les distributions uniquement.

Utilisation d'informations d'identification temporaires avec CloudFront

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.

Transférer les sessions d'accès pour CloudFront

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

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 CloudFront

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 associées à un rôle de service peut perturber CloudFront les fonctionnalités. Modifiez les rôles de service uniquement lorsque CloudFront vous recevez des instructions à cet effet.

Rôles liés à un service pour CloudFront

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

Lambda @Edge utilise des rôles liés à un service pour effectuer des actions à votre place. Pour plus d'informations sur la création ou la gestion de rôles CloudFront liés à un service, consultez. Rôles liés à un service pour Lambda@Edge

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 Amazon CloudFront

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier CloudFront des ressources. 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 CloudFront, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon CloudFront dans le Service Authorization Reference.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer CloudFront des ressources 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 CloudFront

Pour accéder à la CloudFront console Amazon, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails CloudFront des ressources 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 CloudFront console, associez également la politique CloudFront *ConsoleAccess* ou la politique *ReadOnly* AWS gérée 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": "*"
        }
```

```
    ]
}
```

Autorisations d'accès CloudFront par programmation

Voici une politique d'autorisations. Le `Sid`, ou ID de l'instruction, est facultatif.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowAllCloudFrontPermissions",
         "Effect": "Allow",
         "Action": ["cloudfront:*"],
         "Resource": "*"
      }
   ]
}
```

La politique accorde des autorisations pour effectuer toutes les CloudFront opérations, ce qui est suffisant pour y accéder CloudFront par programmation. Si vous utilisez la console pour y accéder CloudFront, consultezAutorisations requises pour utiliser la CloudFront console.

Pour obtenir la liste des actions et l'ARN que vous spécifiez pour accorder ou refuser l'autorisation d'utiliser chaque action, consultez la section Actions, ressources et clés de condition pour Amazon CloudFront dans le Service Authorization Reference.

Autorisations requises pour utiliser la CloudFront console

Pour accorder un accès complet à la CloudFront console, vous devez accorder les autorisations conformément à la politique d'autorisation suivante :

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:*",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:PutMetricAlarm",
```

```
            "cloudwatch:GetMetricStatistics",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Voici pourquoi les autorisations sont obligatoires :

`acm:ListCertificates`

Lorsque vous créez et mettez à jour des distributions à l'aide de la CloudFront console et que vous CloudFront souhaitez configurer pour exiger le protocole HTTPS entre le lecteur CloudFront et CloudFront l'origine, cela vous permet de consulter la liste des certificats ACM.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`cloudfront:*`

Permet d'effectuer toutes les CloudFront actions.

`cloudwatch:DescribeAlarms` et **`cloudwatch:PutMetricAlarm`**

Permet de créer et de visualiser des CloudWatch alarmes dans la CloudFront console. Voir aussi `sns:ListSubscriptionsByTopic` et `sns:ListTopics`.

Ces autorisations ne sont pas requises si vous n'utilisez pas la CloudFront console.

`cloudwatch:GetMetricStatistics`

CloudFront Rendons CloudWatch les métriques dans la CloudFront console.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`elasticloadbalancing:DescribeLoadBalancers`

Lorsque vous créez et mettez à jour des distributions, vous permet d'afficher la liste des équilibreurs de charge Elastic Load Balancing dans la liste des origines disponibles.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`iam:ListServerCertificates`

Lorsque vous créez et mettez à jour des distributions à l'aide de la CloudFront console et que vous souhaitez configurer de manière CloudFront à exiger le protocole HTTPS entre le lecteur CloudFront et CloudFront l'origine, cela vous permet de consulter la liste des certificats dans le magasin de certificats IAM.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`s3:ListAllMyBuckets`

Lorsque vous créez et mettez à jour des distributions et RTMP, vous permet d'effectuer les opérations suivantes :

- Afficher une liste des compartiments S3 dans la liste des origines disponibles
- Afficher une liste de compartiments S3 dans lesquels vous pouvez enregistrer les journaux d'accès

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`S3:PutBucketPolicy`

Lorsque vous créez ou mettez à jour des distributions qui restreignent l'accès aux compartiments S3, permet à un utilisateur de mettre à jour la politique de compartiment pour accorder l'accès à l'identité CloudFront d'accès d'origine. Pour plus d’informations, consultez the section called “Utiliser une identité d'accès d'origine (ancienne, non recommandée)”.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`sns:ListSubscriptionsByTopic` et **`sns:ListTopics`**

Lorsque vous créez des CloudWatch alarmes dans la CloudFront console, cela vous permet de choisir un sujet SNS pour les notifications.

Ces autorisations ne sont pas requises si vous n'utilisez pas la CloudFront console.

`waf:GetWebACL` et **`waf:ListWebACLs`**

Permet d'afficher la liste des ACL AWS WAF Web dans la CloudFront console.

Ces autorisations ne sont pas requises si vous n'utilisez pas la CloudFront console.

AWS politiques gérées (prédéfinies) pour CloudFront

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par. AWS Ces politiques AWS gérées accordent les autorisations nécessaires pour les cas d'utilisation courants afin que vous puissiez éviter d'avoir à rechercher les autorisations nécessaires. Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM. En CloudFront effet, IAM fournit deux politiques gérées :

- CloudFrontFullAccess— Accorde un accès complet aux CloudFront ressources.

> **Important**
>
> Si vous souhaitez CloudFront créer et enregistrer des journaux d'accès, vous devez accorder des autorisations supplémentaires. Pour plus d'informations, consultez Autorisations requises pour configurer la journalisation standard et accéder à vos fichiers journaux.

- CloudFrontReadOnlyAccess— Accorde un accès en lecture seule aux ressources. CloudFront

Exemples de politiques gérées par le client

Vous pouvez créer vos propres politiques IAM personnalisées pour autoriser les actions d' CloudFront API. Vous pouvez attacher ces politiques personnalisées aux utilisateurs ou groupes IAM qui nécessitent les autorisations spécifiées. Ces politiques fonctionnent lorsque vous utilisez l' CloudFront API, les AWS SDK ou le AWS CLI. Les exemples suivants présentent des autorisations pour quelques cas d'utilisation courants. Pour connaître la politique qui accorde à un utilisateur un accès complet à CloudFront, voirAutorisations requises pour utiliser la CloudFront console.

Exemples

- Exemple 1 : Autoriser l'accès en lecture à toutes les distributions
- Exemple 2 : Créer, mettre à jour et supprimer des distributions
- Exemple 3 : Autoriser la création et l'inventaire des invalidations

- Exemple 4 : Autoriser la création d'une distribution

Exemple 1 : Autoriser l'accès en lecture à toutes les distributions

La politique d'autorisation suivante accorde à l'utilisateur l'autorisation d'afficher toutes les distributions dans la CloudFront console :

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Exemple 2 : Créer, mettre à jour et supprimer des distributions

La politique d'autorisation suivante permet aux utilisateurs de créer, de mettre à jour et de supprimer des distributions à l'aide de la CloudFront console :

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:CreateDistribution",
            "cloudfront:DeleteDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

L'autorisation `cloudfront:ListCloudFrontOriginAccessIdentities` permet aux utilisateurs d'accorder automatiquement à une identité d'accès à l'origine existante l'autorisation d'accès aux objets dans un compartiment Amazon S3. Si vous souhaitez également que les utilisateurs puissent créer des identités d'accès à l'origine, vous devez également accorder l'autorisation `cloudfront:CreateCloudFrontOriginAccessIdentity`.

Exemple 3 : Autoriser la création et l'inventaire des invalidations

La politique d'autorisations suivante permet aux utilisateurs de créer et de répertorier des invalidations. Cela inclut l'accès en lecture aux CloudFront distributions, car vous créez et visualisez les invalidations en affichant d'abord les paramètres d'une distribution :

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:GetDistribution",
            "cloudfront:GetStreamingDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "cloudfront:CreateInvalidation",
            "cloudfront:GetInvalidation",
            "cloudfront:ListInvalidations",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Exemple 4 : Autoriser la création d'une distribution

La politique d'autorisation suivante accorde à l'utilisateur l'autorisation de créer et de répertorier des distributions dans la CloudFront console. Pour l'`CreateDistribution`action, spécifiez le caractère générique (*) au `Resource` lieu d'un caractère générique pour l'ARN de distribution ()`arn:aws:cloudfront::123456789012:distribution/*`. Pour plus d'informations sur l'`Resource`élément, voir Éléments de politique IAM JSON : ressource dans le guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "cloudfront:CreateDistribution",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "cloudfront:ListDistributions",
            "Resource": "*"
        }
    ]
}
```

AWSpolitiques gérées pour Amazon CloudFront

Pour ajouter des autorisations à des utilisateurs, des groupes et des rôles, il est plus facile d'utiliser des politiques gérées AWS que d'écrire des politiques vous-même. Il faut du temps et de l'expertise pour Créer des politiques IAM gérées par le client qui fournissent aux utilisateurs uniquement les autorisations dont ils ont besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques gérées AWS. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques gérées par AWS, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Les services AWS assurent la maintenance et la mise à jour des politiques gérées AWS. Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées AWS. Les services

ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctions. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont les plus susceptibles de mettre à jour une politique gérée par AWS lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles autorisations deviennent disponibles. Les services ne supprimant pas les autorisations d'une politique gérée AWS, les mises à jour de politique n’interrompent vos autorisations existantes.

En outre, AWS prend en charge des politiques gérées pour des activités professionnelles couvrant plusieurs services. Par exemple, la politique ReadOnlyAccess gérée par AWS donne accès en lecture seule à l'ensemble des services et des ressources AWS. Quand un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l’utilisateur IAM.

Stratégie AWS gérée : CloudFrontReadOnlyAccess

Vous pouvez associer la politique CloudFrontReadOnlyAccess à vos identités IAM. Cette politique autorise les autorisations en lecture seule pour les ressources. CloudFront Il autorise également des autorisations en lecture seule pour d'autres ressources de AWS service associées à la CloudFront console et visibles dans celle-ci. CloudFront

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `cloudfront:Describe*`— Permet aux directeurs d'obtenir des informations sur les métadonnées relatives aux CloudFront ressources.
- `cloudfront:Get*`— Permet aux responsables d'obtenir des informations détaillées et des configurations pour les CloudFront ressources.
- `cloudfront:List*`— Permet aux directeurs d'obtenir des listes de CloudFront ressources.
- `cloudfront-keyvaluestore:Describe*`- Permet aux principaux d'obtenir des informations sur le magasin de valeurs clés.
- `cloudfront-keyvaluestore:Get*`- Permet aux donneurs d'ordre d'obtenir des informations détaillées et des configurations pour le magasin de valeurs clés.

- `cloudfront-keyvaluestore:List*`- Permet aux directeurs d'obtenir des listes des principales valeurs stockées.
- `acm:ListCertificates` – Permet aux entités principales d'obtenir une liste de certificats ACM.
- `iam:ListServerCertificates` – Permet aux entités principales d'obtenir une liste des certificats de serveur stockés dans IAM.
- `route53:List*` – Permet aux entités principales d'obtenir des listes de ressources Route 53.
- `waf:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `waf:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `wafv2:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `wafv2:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cfReadOnly",
      "Effect": "Allow",
      "Action": [
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Stratégie AWS gérée : CloudFrontFullAccess

Vous pouvez associer la politique CloudFrontFullAccess à vos identités IAM. Cette politique autorise les autorisations administratives sur les CloudFront ressources. Il autorise également des autorisations en lecture seule pour d'autres ressources de AWS service associées à la CloudFront console et visibles dans celle-ci. CloudFront

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `s3:ListAllMyBuckets` – Permet aux entités principales d'obtenir une liste de tous les compartiments Amazon S3.
- `acm:ListCertificates` – Permet aux entités principales d'obtenir une liste de certificats ACM.
- `cloudfront:*`— Permet aux principaux d'effectuer toutes les actions sur toutes les CloudFront ressources.
- `cloudfront-keyvaluestore:*`- Permet aux principaux d'effectuer toutes les actions sur le magasin de valeurs clés.
- `iam:ListServerCertificates` – Permet aux entités principales d'obtenir une liste des certificats de serveur stockés dans IAM.
- `waf:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `waf:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `wafv2:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `wafv2:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `kinesis:ListStreams` – Permet aux entités principales d'obtenir une liste des Amazon Kinesis streams.
- `kinesis:DescribeStream` – Permet aux entités principales d'obtenir des informations détaillées sur un flux Kinesis.
- `iam:ListRoles` – Permet aux entités principales d'obtenir une liste des rôles dans IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cfflistbuckets",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "cffullaccess",
      "Action": [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "cffdescribestream",
      "Action": [
        "kinesis:DescribeStream"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid": "cfflistroles",
      "Action": [
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:*"
    }
```

```
  ]
}
```

Stratégie AWS gérée : AWSCloudFrontLogger

Vous ne pouvez pas associer la AWSCloudFrontLoggerpolitique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet d' CloudFront effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter the section called “Rôles liés à un service pour Lambda@Edge”.

Cette politique permet CloudFront d'envoyer des fichiers journaux à Amazon CloudWatch. Pour obtenir des détails sur les autorisations incluses dans cette politique, consultez the section called “Autorisations de rôle liées au service pour l'enregistreur CloudFront”.

Stratégie AWS gérée : AWSLambdaReplicator

Vous ne pouvez pas associer la AWSLambdaReplicatorpolitique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet d' CloudFront effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter the section called “Rôles liés à un service pour Lambda@Edge”.

Cette politique permet CloudFront de créer, de supprimer et de désactiver des fonctions dans AWS Lambda pour répliquer les fonctions Lambda @Edge dans. Régions AWS Pour obtenir des détails sur les autorisations incluses dans cette politique, consultez the section called “Autorisations du rôle lié à un service pour Lambda Replicator”.

CloudFront mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées CloudFront depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du CloudFront document.

Modification	Description	Date
CloudFrontReadOnlyAccess et CloudFrontFullAccess :	CloudFront a ajouté de nouvelles autorisations pour les magasins à valeur clé.	19 décembre 2023

Modification	Description	Date
mise à jour de deux politiques existantes.	Les nouvelles autorisations permettent aux utilisateurs d'obtenir des informations sur les magasins à valeur clé et de prendre des mesures à leur sujet.	
CloudFrontReadOnlyAccess - mise à jour d'une politique existante	CloudFront a ajouté une nouvelle autorisation pour décrire CloudFront les fonctions. Cette autorisation permet à l'utilisateur, au groupe ou au rôle de lire les informations et les métadonnées relatives à une fonction, mais pas le code de la fonction.	8 septembre 2021
CloudFront a commencé à suivre les modifications	CloudFront a commencé à suivre les modifications apportées AWS à ses politique s gérées.	8 septembre 2021

Résolution des problèmes d' CloudFront identité et d'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec CloudFront IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans CloudFront
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes CloudFront ressources

Je ne suis pas autorisé à effectuer une action dans CloudFront

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 `cloudfront:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudfront: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 `cloudfront:`*`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 effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle CloudFront.

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 effectuer une action dans CloudFront. 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 permettre à des personnes extérieures Compte AWS à moi d'accéder à mes CloudFront ressources

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 ces fonctionnalités sont prises CloudFront en charge, consultezComment Amazon CloudFront travaille 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Journalisation et surveillance sur Amazon CloudFront

La surveillance est un élément important permettant d'assurer la disponibilité et les performances de CloudFront et de vos solutions AWS. 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. AWSfournit plusieurs outils pour surveiller vos CloudFront ressources et votre activité, et répondre aux incidents potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique Amazon SNS ou à une stratégie AWS Auto Scaling. CloudWatch les alarmes n'appellent aucune action lorsqu'une métrique est dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour de plus amples informations, veuillez consulter Surveillance CloudFront des métriques avec Amazon CloudWatch.

AWS CloudTrailJournaux

CloudTrail fournit un enregistrement des actions d'API effectuées par un utilisateur, un rôle ou un AWS service dans CloudFront. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande d'API qui a été faite CloudFront, 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 de plus amples informations, veuillez consulter Journalisation des appels d' CloudFront API Amazon à l'aide de AWS CloudTrail.

CloudFront journaux standard et journaux en temps réel

CloudFront les journaux fournissent des informations détaillées sur les demandes adressées à une distribution. Ces journaux sont utiles pour de nombreuses applications. Par exemple, les informations des journaux peuvent être importantes en cas d'audit de sécurité ou des accès. Pour de plus amples informations, veuillez consulter CloudFront et journalisation des fonctions Edge.

Journaux des fonctions de périphérie

Les journaux générés par les fonctions périphériques, CloudFront Functions et Lambda @Edge, sont envoyés directement à Amazon CloudWatch Logs et ne sont stockés nulle part par. CloudFront CloudFront Functions utilise un rôle lié à un service AWS Identity and Access Management (IAM) pour envoyer les journaux générés par les clients directement aux CloudWatch journaux de votre compte.

CloudFront rapports de console

La CloudFront console inclut divers rapports, notamment le rapport sur les statistiques du cache, le rapport sur les objets populaires et le rapport sur les principaux référents. La plupart des rapports de CloudFront console sont basés sur les données des journaux CloudFront d'accès, qui contiennent des informations détaillées sur chaque demande d'utilisateur CloudFront reçue. Toutefois, vous n'avez pas besoin d'activer les journaux d'accès pour consulter ces rapports. Pour de plus amples informations, veuillez consulter Afficher CloudFront les rapports dans la console.

Validation de conformité pour Amazon CloudFront

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon dans CloudFront le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, HIPAA.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Votre responsabilité en matière de conformité lors de l'utilisation CloudFront est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Architecting for HIPAA Security and Compliance on AWS — Ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  Le programme de conformité AWS HIPAA inclut CloudFront (à l'exception de la diffusion de contenu via des POP CloudFront intégrés) en tant que service éligible à la HIPAA. Si vous avez exécuté un addendum d'associé commercial (BAA) avec AWS, vous pouvez l'utiliser CloudFront (à l'exception de la diffusion de contenu via des POP CloudFront intégrés) pour diffuser du contenu contenant des informations de santé protégées (PHI). Pour de plus amples informations, consultez Conformité à la loi HIPAA.
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service utilise des contrôles de sécurité pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à vous conformer aux différents cadres de conformité. Pour plus d'informations sur l'utilisation de Security Hub pour évaluer les CloudFront ressources, consultez Amazon CloudFront Controls dans le guide de AWS Security Hub l'utilisateur.

CloudFront meilleures pratiques en matière de conformité

Cette section fournit les meilleures pratiques et des recommandations en matière de conformité lorsque vous utilisez Amazon CloudFront pour diffuser votre contenu.

Si vous exécutez des charges de travail conformes aux normes PCI ou HIPAA basées sur le modèle de responsabilitéAWS partagée, nous vous recommandons de consigner vos données CloudFront d'utilisation des 365 derniers jours à des fins d'audit futur. Pour journaliser les données d'utilisation, vous pouvez procéder comme suit :

- Activez les journaux d' CloudFront accès. Pour plus d'informations, consultez Configuration et utilisation des journaux standard (journaux d'accès).
- Capturez les demandes envoyées à l' CloudFront API. Pour plus d'informations, consultez Journalisation des appels d' CloudFront API Amazon à l'aide de AWS CloudTrail.

En outre, consultez ce qui suit pour plus de détails sur la manière dont CloudFront il est conforme aux normes PCI DSS et SOC.

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

CloudFront (à l'exception de la diffusion de contenu via des POP CloudFront intégrés) prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données (DSS) du secteur des cartes de paiement (PCI) a été validée. Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section PCI DSS niveau 1.

Pour des raisons de sécurité, nous vous recommandons de ne pas mettre en cache les informations de carte de crédit dans les caches CloudFront périphériques. Par exemple, vous pouvez configurer votre origine de manière à ce qu'elle inclue un en-tête `Cache-Control:no-cache="`*`nom-de-champ`*`"` dans les réponses qui contiennent des informations relatives aux cartes de crédit, telles que les quatre derniers chiffres d'un numéro de carte de crédit et les coordonnées du titulaire de la carte.

System and Organization Controls (SOC)

CloudFront (à l'exception de la diffusion de contenu via des POP CloudFront intégrés) est conforme aux mesures de contrôle du système et de l'organisation (SOC), notamment les normes SOC 1, SOC 2 et SOC 3. Les rapports SOC sont des rapports d'examen indépendants réalisés par des

tiers qui montrent comment AWS atteindre les principaux contrôles et objectifs de conformité. Ces audits garantissent que les protections et procédures adéquates sont établies pour protéger contre les risques susceptibles d'avoir une incidence sur la sécurité, la confidentialité et la disponibilité des données des clients et des entreprises. Les résultats de ces audits tiers sont disponibles sur le site Web de conformité du AWS SOC, où vous pouvez consulter les rapports publiés pour obtenir plus d'informations sur les contrôles qui soutiennent les AWS opérations et la conformité.

Résilience chez Amazon CloudFront

L'infrastructure mondiale AWS s'articule autours de régions et de zones de disponibilité AWS. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, 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 de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

CloudFront basculement d'origine

Outre la prise en charge de l'infrastructure AWS mondiale, Amazon CloudFront propose une fonctionnalité de basculement d'origine pour répondre à vos besoins en matière de résilience des données. CloudFront est un service mondial qui diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques ou points de présence (POPs). Si votre contenu n'est pas déjà mis en cache dans un emplacement périphérique, CloudFront l'extrait d'une origine que vous avez identifiée comme étant la source de la version définitive du contenu.

Vous pouvez améliorer la résilience et augmenter la disponibilité pour des scénarios spécifiques en configurant CloudFront avec le basculement d'origine. Pour commencer, vous créez un groupe d'origine dans lequel vous désignez une origine principale CloudFront plus une deuxième origine. CloudFront passe automatiquement à la deuxième origine lorsque l'origine principale renvoie des réponses d'échec de code d'état HTTP spécifiques. Pour de plus amples informations, veuillez consulter Optimisez la haute disponibilité grâce au basculement CloudFront d'origine.

Sécurité de l'infrastructure sur Amazon CloudFront

En tant que service géré, Amazon CloudFront est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez des appels d'API AWS publiés pour accéder CloudFront 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.

CloudFront Functions utilise une barrière d'isolation hautement sécurisée entre les AWS comptes, garantissant ainsi que les environnements des clients sont protégés contre les attaques par canaux secondaires telles que Spectre et Meltdown. Functions ne peut pas accéder aux données appartenant à d'autres clients ni les modifier. Functions s'exécute dans un processus monothread sur un processeur dédié sans hyper-threading. Quel que soit le point de présence de la CloudFront périphérie (POP), CloudFront Functions ne dessert qu'un seul client à la fois, et toutes les données spécifiques au client sont effacées entre les exécutions des fonctions.

Résolution des problèmes

Résolvez les problèmes courants que vous pouvez rencontrer lors de la configuration d'Amazon CloudFront pour diffuser votre contenu ou lors de l'utilisation de Lambda @Edge, et trouvez des solutions possibles.

Rubriques

Résolution des problèmes de distribution

Utilisez les informations fournies ici pour vous aider à diagnostiquer et à corriger les erreurs de certificat, les problèmes de refus d'accès ou les autres problèmes courants que vous pourriez rencontrer lors de la configuration de votre site Web ou de votre application avec les distributions Amazon CloudFront .

Rubriques

CloudFront renvoie une Access Denied erreur

Si vous utilisez un compartiment Amazon S3 comme origine de votre CloudFront distribution, un message d'erreur Access Denied (403) peut s'afficher dans les exemples suivants.

Table des matières

- Vous utilisez des informations d'identification non valides ou vous ne disposez pas des autorisations suffisantes

Vous avez indiqué un objet manquant dans l'origine d'Amazon S3

Vérifiez que l'objet demandé existe dans votre compartiment. Les noms d'objets distinguent les majuscules et minuscules. La saisie d'un nom d'objet non valide peut renvoyer un code d'erreur de refus d'accès.

Par exemple, si vous suivez le CloudFront didacticiel pour créer une distribution de base, vous créez un compartiment Amazon S3 comme origine et vous chargez un exemple de `index.html` fichier.

Dans votre navigateur Web, si vous entrez `https://d111111abcdef8.cloudfront.net/INDEX.HTML` au lieu de`https://d111111abcdef8.cloudfront.net/index.html`, vous verrez peut-être un message similaire, car le `index.html` fichier dans le chemin de l'URL distingue les majuscules et minuscules.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>22Q367AHT7Y1ABCD</RequestId>
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
</Error>
```

Les autorisations IAM de votre origine Amazon S3 sont manquantes

Vérifiez que vous avez sélectionné le bon compartiment Amazon S3 comme domaine et nom d'origine. L'origine (Amazon S3) doit disposer des autorisations appropriées.

Si vous ne spécifiez pas les autorisations appropriées, le message de refus d'accès suivant peut s'afficher pour vos spectateurs.

```
<Code>AccessDenied</Code>
<Message>User: arn:aws:sts::856369053181:assumed-role/OriginAccessControlRole/
EdgeCredentialsProxy+EdgeHostAuthenticationClient is not authorized to perform:
 kms:Decrypt on the resource associated with this ciphertext because the resource does
 not exist in this Region, no resource-based policies allow access, or a resource-based
 policy explicitly denies access</Message>
<RequestId>22Q367AHT7Y1ABCD/RequestId>
```

```
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
</Error>
```

> **Note**
>
> Dans ce message d'erreur, l'ID de compte 856369053181 est un compte géré. AWS

Lorsque vous distribuez du contenu depuis Amazon S3 et que vous utilisez également AWS Key Management Service (AWS KMS) le chiffrement côté service (SSE-KMS), vous devez spécifier des autorisations IAM supplémentaires pour la clé KMS et le compartiment Amazon S3. Votre CloudFront distribution a besoin de ces autorisations pour utiliser la clé KMS, qui est utilisée pour le chiffrement du compartiment Amazon S3 d'origine.

Les configurations de la politique de compartiment Amazon S3 permettent à la CloudFront distribution de récupérer les objets chiffrés pour la diffusion de contenu.

Pour vérifier les autorisations de votre compartiment Amazon S3 et de votre clé KMS

1. Vérifiez que la clé KMS que vous utilisez est la même que celle utilisée par votre compartiment Amazon S3 pour le chiffrement par défaut. Pour plus d'informations, consultez Spécifier le chiffrement côté serveur avec AWS KMS (SSE-KMS) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
2. Vérifiez que les objets du compartiment sont chiffrés avec la même clé KMS. Vous pouvez sélectionner n'importe quel objet dans le compartiment Amazon S3 et vérifier les paramètres de chiffrement côté serveur pour vérifier l'ARN de la clé KMS.
3. Modifiez la politique du compartiment Amazon S3 pour CloudFront autoriser l'appel de l'opération d'`GetObject`API depuis le compartiment Amazon S3. Pour un exemple de politique de compartiment Amazon S3 qui utilise le contrôle d'accès à l'origine, consultezDonnez à l'origine l'autorisation de contrôle d'accès d'accéder au compartiment S3.
4. Modifiez la politique des clés KMS pour accorder l' CloudFront autorisation d'effectuer les actions à `Encrypt`Decrypt, et`GenerateDataKey*`. Pour vous aligner sur l'autorisation du moindre privilège, spécifiez un `Condition` élément afin que seule la CloudFront distribution spécifiée puisse effectuer les actions répertoriées. Vous pouvez personnaliser la politique en fonction de votre AWS KMS politique existante. Pour un exemple de politique relative aux clés KMS, consultez leSSE-KMS.

Si vous utilisez l'identité d'accès d'origine (OAI) au lieu d'OAC, les autorisations d'accès au compartiment Amazon S3 sont légèrement différentes car vous accordez l'autorisation à une identité au lieu de. Service AWS Pour plus d’informations, consultez Autoriser une identité d'accès d'origine à lire des fichiers dans le compartiment Amazon S3.

Si vous ne parvenez toujours pas à afficher vos fichiers dans votre distribution, consultezJe ne peux pas afficher les fichiers de ma distribution.

Vous utilisez des informations d'identification non valides ou vous ne disposez pas des autorisations suffisantes

Un message d'erreur Accès refusé peut s'afficher si vous utilisez des AWS SCT informations d'identification incorrectes ou expirées (clé d'accès et clé secrète) ou si votre rôle ou utilisateur IAM ne dispose pas de l'autorisation requise pour effectuer une action sur une CloudFront ressource. Pour plus d'informations sur les messages d'erreur de refus d'accès, consultez la section Résolution des messages d'erreur liés au refus d'accès dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la façon dont IAM fonctionne avec CloudFront, consultezIdentity and Access Management pour Amazon CloudFront.

CloudFront renvoie une InvalidViewerCertificate erreur lorsque j'essaie d'ajouter un autre nom de domaine

Si CloudFront un `InvalidViewerCertificate` message d'erreur s'affiche lorsque vous essayez d'ajouter un autre nom de domaine (CNAME) à votre distribution, consultez les informations suivantes pour résoudre le problème. Cette erreur peut indiquer que l’un des problèmes suivants doit être résolu avant que vous puissiez correctement ajouter le nom de domaine alternatif.

Les erreurs suivantes sont répertoriées dans l'ordre dans lequel l' CloudFront autorisation d'ajouter un autre nom de domaine est vérifiée. Cela peut vous aider à résoudre les problèmes, car en fonction de l'erreur CloudFront renvoyée, vous pouvez savoir quelles vérifications ont été effectuées avec succès.

Il n’y a aucun certificat associé à votre distribution.

> Pour ajouter un nom de domaine alternatif (CNAME), vous devez attacher un certificat valide et approuvé à votre distribution. Consultez les exigences, obtenez un certificat valide qui répond à ces exigences, attachez celui-ci à votre distribution, puis réessayez. Pour de plus amples informations, veuillez consulter Exigences relatives à l’utilisation de noms de domaines alternatifs.

Il y a un trop grand nombre de certificats dans la chaîne de certificats pour le certificat que vous avez attaché.

Vous pouvez uniquement posséder jusqu'à cinq certificats dans une chaîne de certificats. Réduisez le nombre de certificats dans la chaîne, puis réessayez.

La chaîne de certificats inclut un ou plusieurs certificats qui ne sont pas valides pour la date du jour.

La chaîne de certificats pour un certificat que vous avez ajouté a un ou plusieurs certificats qui ne sont pas valides, soit parce que le certificat n'est pas encore valide ou parce qu'il a expiré. Vérifiez les champs Not Valid Before (Non valide avant) et Not Valid After (Non valide après) dans les certificats de votre chaîne de certificats pour vous assurer que tous les certificats sont valides en fonction des dates que vous avez répertoriées.

Le certificat que vous avez attaché n'est pas signé par une autorité de certification (CA) approuvée.

Le certificat que vous attachez CloudFront pour vérifier un autre nom de domaine ne peut pas être un certificat auto-signé. Il doit être signé par une autorité de certification approuvée. Pour de plus amples informations, veuillez consulter Exigences relatives à l'utilisation de noms de domaines alternatifs.

Le certificat que vous avez attaché n'est pas formaté correctement

Le nom de domaine et le format d'adresse IP qui sont inclus dans le certificat et le format du certificat lui-même, doivent respecter la norme pour les certificats.

Une erreur CloudFront interne s'est produite.

CloudFront a été bloqué en raison d'un problème interne et n'a pas pu effectuer de contrôles de validation pour les certificats. Dans ce scénario, CloudFront renvoie un code d'état HTTP 500 et indique qu'il existe un CloudFront problème interne lors de l'attachement du certificat. Attendez quelques minutes, puis réessayez pour ajouter le nom de domaine alternatif avec le certificat.

Le certificat que vous avez attaché ne couvre pas le nom de domaine alternatif que vous tentez d'ajouter.

Pour chaque nom de domaine alternatif que vous ajoutez, CloudFront vous devez joindre un certificat SSL/TLS valide provenant d'une autorité de certification (CA) fiable qui couvre le nom de domaine, afin de valider votre autorisation d'utilisation. Mettez à jour votre certificat pour inclure un nom de domaine qui couvre le CNAME que vous tentez d'ajouter. Pour de plus amples informations et pour obtenir des exemples d'utilisation de noms de domaines avec caractères génériques, veuillez consulter Exigences relatives à l'utilisation de noms de domaines alternatifs.

Je ne peux pas afficher les fichiers de ma distribution

Si vous ne parvenez pas à afficher les fichiers de votre CloudFront distribution, consultez les rubriques suivantes pour découvrir certaines solutions courantes.

Vous êtes-vous inscrit à la fois à Amazon S3 CloudFront et à Amazon S3 ?

Pour utiliser Amazon CloudFront avec une origine Amazon S3, vous devez vous inscrire séparément à Amazon S3 CloudFront et à Amazon S3. Pour plus d'informations sur l'inscription à Amazon S3 CloudFront et sur Amazon S3, consultezConfiguration.

Votre compartiment Amazon S3 et vos autorisations d’objet sont-elles définis correctement ?

Si vous l'utilisez CloudFront avec une origine Amazon S3, les versions originales de votre contenu sont stockées dans un compartiment S3. La méthode la plus simple à utiliser CloudFront avec Amazon S3 est de rendre tous vos objets lisibles publiquement dans Amazon S3. Pour faire ceci, vous devez activer les privilèges de lecture publique de manière explicite pour chaque objet que vous chargez sur Amazon S3.

Si votre contenu n'est pas lisible par le public, vous devez créer un contrôle CloudFront d'accès à l'origine (OAC) afin de CloudFront pouvoir y accéder. Pour plus d'informations sur le contrôle CloudFront d'accès à l'origine, consultezthe section called “Restreindre l'accès à une origine Amazon Simple Storage Service”.

Les propriétés d’objet et les propriétés de compartiment sont indépendantes. Vous devez accorder, de manière explicite, des privilèges à chaque objet dans Amazon S3. Les objets n’héritent pas des propriétés des compartiments et les propriétés d’objet doivent être définies indépendamment du compartiment.

Votre nom de domaine alternatif (CNAME) est-il configuré correctement ?

Si vous avez déjà un enregistrement CNAME pour votre nom de domaine, mettez-le à jour ou remplacez-le par un nouvel enregistrement qui pointe vers votre nom de domaine de distribution.

Veillez également à ce que votre archive CNAME dirige vers votre nom de domaine de distribution et non pas votre compartiment Amazon S3. Vous pouvez confirmer que l’archive CNAME dans votre système DNS dirige vers votre nom de domaine de distribution. À cette fin, utilisez un outil DNS tel que dig.

L'exemple suivant illustre une demande dig sur un nom de domaine appelé `images.example.com` et la partie appropriée de la réponse. Sous `ANSWER SECTION`, regardez la ligne qui contient `CNAME`. L'enregistrement CNAME de votre nom de domaine est correctement configuré si la valeur sur le côté droit de CNAME est le nom de domaine de votre CloudFront distribution. S'il s'agit de votre case de serveur d'origine Amazon S3 ou d'autre nom de domaine, alors l'archive CNAME est mal définie.

```
[prompt]> dig images.example.com

; <<> DiG 9.3.3rc2 <<> images.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15917
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;images.example.com.   IN  A
;; ANSWER SECTION:
images.example.com. 10800 IN CNAME d111111abcdef8.cloudfront.net.
...
...
```

Pour plus d'informations sur les CNAME, consultez Utilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames).

Référencez-vous l'URL correcte pour votre CloudFront distribution ?

Assurez-vous que l'URL à laquelle vous faites référence utilise le nom de domaine (ou CNAME) de votre CloudFront distribution, et non votre compartiment Amazon S3 ou votre origine personnalisée.

Avez-vous besoin d'aide pour résoudre un problème lié à une origine personnalisée ?

Si vous avez besoin d'aide AWS pour résoudre un problème d'origine personnalisé, nous devrons probablement inspecter les entrées `X-Amz-Cf-Id` d'en-tête de vos demandes. Si vous n'enregistrez pas déjà ces entrées, il se peut que vous pensiez à le faire à l'avenir. Pour plus d'informations, consultez the section called "Utiliser Amazon EC2 (ou une autre origine personnalisée)". Pour obtenir plus d'aide, consultez le Centre de support AWS.

Message d'erreur : Certificat : <certificate-id>est utilisé par CloudFront

Problème : vous essayez de supprimer un certificat SSL/TLS du magasin de certificats IAM et le message « Certificat : <certificate-id>est utilisé par » s'affiche. CloudFront

Solution : Chaque CloudFront distribution doit être associée au CloudFront certificat par défaut ou à un certificat SSL/TLS personnalisé. Avant de pouvoir supprimer un certificat SSL/TLS, vous devez soit le faire pivoter (remplacer le certificat SSL/TLS personnalisé actuel par un autre certificat SSL/TLS personnalisé), soit passer du certificat SSL/TLS personnalisé au certificat par défaut. CloudFront Pour régler ce problème, effectuez les étapes de l'une des procédures suivantes :

- Rotation des certificats SSL/TLS
- Revenir d'un certificat SSL/TLS personnalisé au certificat par défaut CloudFront

Résolution des réponses d'erreur de votre origine

Si CloudFront vous demandez un objet à votre origine et que celle-ci renvoie un code d'état HTTP 4xx ou 5xx, cela signifie qu'il y a un problème de communication entre CloudFront et votre origine. Les rubriques suivantes décrivent les causes courantes de certains de ces codes d'état HTTP et fournissent des solutions possibles.

Rubriques

- Code d'état HTTP 400 (Requête incorrecte)
- Code d'état HTTP 502 (Passerelle incorrecte)
- Code d'état HTTP 503 (Service non disponible)
- Code d'état HTTP 504 (délai d'expiration de la passerelle)

Code d'état HTTP 400 (Requête incorrecte)

Votre CloudFront distribution peut envoyer des réponses d'erreur avec le code d'état HTTP 400 Bad Request et un message similaire au suivant :

L'en-tête d'autorisation est mal formé ; la région « *<AWS Region>* » est incorrecte ; on attend « *<AWS* Region> »

Par exemple :

The authorization header is malformed; the region 'us-east-1' is wrong; expecting 'us-west-2'

Ce problème peut se produire dans le scénario suivant :

1. L'origine de votre CloudFront distribution est un compartiment Amazon S3.

2. Vous avez déplacé le compartiment S3 d'une AWS région à une autre. En d'autres termes, vous avez supprimé le compartiment S3, puis vous avez créé un nouveau compartiment portant le même nom de compartiment, mais dans une AWS région différente de celle où se trouvait le compartiment S3 d'origine.

Pour corriger cette erreur, mettez à jour votre CloudFront distribution afin qu'elle trouve le compartiment S3 dans la AWS région actuelle du compartiment.

Pour mettre à jour votre CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution qui génère cette erreur.
3. Choisissez Origins and Origin Groups (Origines et groupes d'origine).
4. Recherchez l'origine du compartiment S3 que vous avez déplacé. Activez la case à cocher en regard de cette origine, puis choisissez Modifier.
5. Choisissez Oui, Modifier. Vous n'avez pas besoin de modifier les paramètres avant de choisir Oui, Modifier.

Lorsque vous avez terminé ces étapes, CloudFront redéploie votre distribution. Pendant le déploiement de la distribution, l'état du déploiement s'affiche dans la colonne Dernière modification. Quelque temps après la fin du déploiement, vous ne devriez plus recevoir les réponses `AuthorizationHeaderMalformed` d'erreur.

Code d'état HTTP 502 (Passerelle incorrecte)

Un code d'état HTTP 502 (Bad Gateway) indique que l'objet demandé CloudFront n'a pas pu être utilisé car il n'a pas pu se connecter au serveur d'origine.

Si vous utilisez Lambda @Edge, le problème est peut-être dû à une erreur de validation Lambda. Si vous recevez une erreur HTTP 502 avec le code `NonS3OriginDnsError` d'erreur, il est probable qu'un problème de configuration DNS CloudFront empêche la connexion à l'origine.

Rubriques

- Echec de négociation SSL/TLS entre CloudFront et un serveur d'origine personnalisé
- L'origine ne répond pas avec les chiffrements/protocoles pris en charge

- Le certificat SSL/TLS sur l'origine a expiré, n'est pas valide, est auto-signé ou la chaîne de certificats est dans l'ordre incorrect
- L'origine ne répond pas sur des ports spécifiés dans les paramètres de l'origine
- Erreur de validation Lambda
- Erreur DNS (NonS3OriginDnsError)

Echec de négociation SSL/TLS entre CloudFront et un serveur d'origine personnalisé

Si vous utilisez une origine personnalisée et que vous avez configuré CloudFront pour exiger le protocole HTTPS entre CloudFront et votre origine, le problème peut être dû à des noms de domaine incompatibles. Le certificat SSL/TLS installé sur votre origine inclut un nom de domaine dans le champ Common Name (Nom courant) et éventuellement plusieurs autres dans le champ Subject Alternative Names (Noms SAN). (CloudFront prend en charge les caractères génériques dans les noms de domaine des certificats.) L'un des noms de domaine du certificat doit correspondre à au moins une des valeurs suivantes :

- La valeur que vous avez spécifiée pour le domaine d'origine pour l'origine applicable dans votre distribution.
- La valeur de l'`Host`en-tête si vous l'avez configuré CloudFront pour le `Host` transmettre à votre origine. Pour plus d'informations sur le transfert des en-têtes `Host` à votre origine, consultez Contenu du cache basé sur les en-têtes des demandes.

Si les noms de domaine ne correspondent pas, le handshake SSL/TLS échoue et CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) et définit l'en-tête sur. `X-Cache Error from cloudfront`

Pour déterminer si les noms de domaine du certificat correspondent au domaine d'origine de la distribution ou de l'`Host`en-tête, vous pouvez utiliser un vérificateur SSL en ligne ou OpenSSL. Si les noms de domaine ne correspondent pas, vous avez deux options :

- La valeur que vous avez spécifiée pour Nom du domaine d'origine pour l'origine applicable de votre distribution.
- La valeur de l'`Host`en-tête si vous l'avez configuré CloudFront pour le `Host` transmettre à votre origine. Pour plus d'informations sur le transfert des en-têtes `Host` à votre origine, consultez Contenu du cache basé sur les en-têtes des demandes.

Si les noms de domaine ne correspondent pas, le handshake SSL/TLS échoue et CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) et définit l'en-tête sur. `X-Cache Error from cloudfront`

Pour déterminer si des noms de domaine du certificat correspondent à Origin Domain Name dans la distribution ou l'en-tête `Host`, vous pouvez utiliser un outil de vérification SSL en ligne ou OpenSSL. Si les noms de domaine ne correspondent pas, vous avez deux options :

- Demandez un nouveau certificat SSL/TLS qui inclut les noms de domaine applicables.

  Si vous utilisez AWS Certificate Manager (ACM), consultez la section Demande d'un certificat public dans le guide de AWS Certificate Manager l'utilisateur pour demander un nouveau certificat.
- Modifiez la configuration de distribution afin de CloudFront ne plus essayer d'utiliser le protocole SSL pour vous connecter à votre origine.

Outil de vérification SSL en ligne

Pour trouver un outil de test SSL, recherchez sur Internet « online ssl checker ». En règle générale, vous spécifiez le nom de votre domaine, et l'outil renvoie différentes informations sur votre certificat SSL/TLS. Vérifiez que le certificat contient votre nom de domaine dans les champs Common Names ou Subject Alternative Names.

OpenSSL

Pour résoudre les erreurs HTTP 502 CloudFront, vous pouvez utiliser OpenSSL pour essayer d'établir une connexion SSL/TLS avec votre serveur d'origine. Si OpenSSL n'est pas en mesure d'établir une connexion, il peut s'agir d'un problème avec la configuration SSL/TLS de votre serveur d'origine. Si OpenSSL est en mesure d'établir une connexion, il renvoie des informations sur le certificat du serveur d'origine, y compris le nom commun (champ `Subject CN`) et le nom alternatif d'objet (champ `Subject Alternative Name`) du certificat.

Utilisez la commande OpenSSL suivante pour tester la connexion à votre serveur d'origine (*`remplacez`* le domaine d'origine par le nom de domaine de votre serveur d'origine, tel que exemple.com) :

```
openssl s_client -connect origin domain name:443
```

Si les conditions suivantes sont réunies :

- Votre serveur d'origine prend en charge plusieurs noms de domaine avec plusieurs certificats SSL/TLS
- Votre distribution est configurée pour transférer l'en-tête `Host` vers l'origine

Ajoutez ensuite l'option `-servername` à la commande OpenSSL, comme dans l'exemple suivant (remplacez *CNAME* par le CNAME configuré dans votre distribution) :

```
openssl s_client -connect origin domain name:443 -servername CNAME
```

L'origine ne répond pas avec les chiffrements/protocoles pris en charge

CloudFront se connecte aux serveurs d'origine à l'aide de chiffrements et de protocoles. Pour obtenir la liste des chiffrements et des protocoles pris CloudFront en charge, consultez. the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine" Si votre origine ne répond pas avec l'un de ces chiffrements ou protocoles dans l'échange SSL/TLS, elle ne parvient pas à se connecter. CloudFront Vous pouvez vérifier que votre origine prend en charge les chiffrements et les protocoles à l'aide d'un outil en ligne tel que SSL Labs. Saisissez le nom de domaine de votre origine dans le champ Hostname, puis choisissez Submit. Consultez les champs Noms Communs et autres noms (SAN) du test pour savoir si ces noms correspondent au nom de domaine de votre origine. A la fin du test, consultez les sections Protocols et Cipher Suites des résultats pour connaître les chiffrements ou les protocoles pris en charge par votre origine. Comparez-les à la liste des the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine".

Le certificat SSL/TLS sur l'origine a expiré, n'est pas valide, est auto-signé ou la chaîne de certificats est dans l'ordre incorrect

Si le serveur d'origine renvoie ce qui suit, CloudFront abandonne la connexion TCP, renvoie le code d'état HTTP 502 (Bad Gateway) et définit l'`X-Cache`en-tête comme suit : `Error from cloudfront`

- Certificat expiré
- Certificat non valide
- Certificat auto-signé
- Chaîne de certificats dans le désordre

> **Note**
>
> Si la chaîne complète de certificats, y compris le certificat intermédiaire, n'est pas présente, CloudFront supprime la connexion TCP.

Pour obtenir des informations sur l'installation d'un certificat SSL/TLS sur votre serveur d'origine personnalisée, consultez the section called "Exiger le protocole HTTPS pour une origine personnalisée".

L'origine ne répond pas sur des ports spécifiés dans les paramètres de l'origine

Lorsque vous créez une origine sur votre CloudFront distribution, vous pouvez définir les ports qui CloudFront se connectent à l'origine pour le trafic HTTP et HTTPS. Par défaut, il s'agit des ports TCP 80/443. Vous avez la possibilité de modifier ces ports. Si votre point d'origine rejette le trafic sur ces ports pour quelque raison que ce soit, ou si votre serveur principal ne répond pas sur les ports, la connexion CloudFront échouera.

Pour résoudre ces problèmes, vérifiez les pare-feu qui s'exécutent dans votre infrastructure et vérifiez qu'ils ne bloquent pas les plages IP prises en charge. Pour plus d'informations, consultez AWS IP Address Ranges dans le manuel Référence générale d'Amazon Web Services. Vous pouvez également vérifier que votre serveur web s'exécute sur l'origine.

Erreur de validation Lambda

Si vous utilisez Lambda@Edge, un code de statut HTTP 502 peut indiquer que la réponse de votre fonction Lambda était mal formulée ou comprenait du contenu non valide. Pour de plus amples informations sur le dépannage des erreurs Lambda@Edge, veuillez consulter Tester et déboguer les fonctions Lambda @Edge.

Erreur DNS (`NonS3OriginDnsError`)

Une erreur HTTP 502 avec le code `NonS3OriginDnsError` d'erreur indique qu'un problème de configuration DNS CloudFront empêche la connexion à l'origine. Si cette erreur provient de CloudFront, assurez-vous que la configuration DNS de l'origine est correcte et fonctionne.

Lorsqu'il CloudFront reçoit une demande pour un objet expiré ou qui n'est pas dans son cache, il adresse une demande à l'origine pour obtenir l'objet. Pour envoyer une demande à l'origine avec

succès, CloudFront effectue une résolution DNS sur le domaine d'origine. Si le service DNS de votre domaine rencontre des problèmes, CloudFront vous ne parvenez pas à résoudre le nom de domaine pour obtenir l'adresse IP, ce qui entraîne une erreur HTTP 502 (`NonS3OriginDnsError`). Pour résoudre ce problème, contactez votre fournisseur DNS ou, si vous utilisez Amazon Route 53, consultez Pourquoi est-ce que je ne peux pas accéder à mon site Web qui utilise les services DNS Route 53 ?

Pour continuer à résoudre ce problème, vérifiez que les serveurs de noms faisant autorité du domaine racine ou de la zone apex (comme `example.com`) de votre origine fonctionne correctement. Vous pouvez utiliser les commandes suivantes pour trouver les serveurs de noms pour votre origine apex, à l'aide d'un outil tel que dig ou nslookup :

```
dig OriginAPEXDomainName NS +short
```

```
nslookup -query=NS OriginAPEXDomainName
```

Quand vous avez les noms de vos serveurs de noms, utilisez les commandes suivantes pour interroger le nom de domaine de votre origine sur ceux-ci afin de vous assurer qu'ils répondent :

```
dig OriginDomainName @NameServer
```

```
nslookup OriginDomainName NameServer
```

> **Important**
>
> Assurez-vous d'effectuer ce dépannage DNS à l'aide d'un ordinateur connecté à l'Internet public. CloudFront résout le domaine d'origine à l'aide du DNS public sur Internet. Il est donc important de résoudre le problème dans un contexte similaire.

Si votre origine est un sous-domaine dont l'autorité DNS est déléguée à un serveur de noms différent du domaine racine, assurez-vous que les enregistrements du serveur de noms (`NS`) et du début de l'autorité (`SOA`) sont correctement configurés pour le sous-domaine. Vous pouvez vérifier ces enregistrements à l'aide de commandes similaires aux exemples précédents.

Pour plus d'informations sur DNS, consultez les Concepts du système de noms de domaine (DNS) dans la documentation d'Amazon Route 53.

Code d’état HTTP 503 (Service non disponible)

Un code de statut HTTP 503 (Service non disponible) indique généralement un problème de performance sur le serveur d’origine. Dans de rares cas, cela indique qu'il est CloudFront temporairement impossible de satisfaire une demande en raison de contraintes de ressources à un emplacement périphérique.

Si vous utilisez Lambda @Edge ou CloudFront Functions, le problème peut être dû à une erreur d'exécution ou à une erreur de dépassement de la limite Lambda @Edge.

Rubriques

Le serveur d’origine n’a pas suffisamment de capacité pour prendre en charge le débit de requêtes

Lorsqu'un serveur d'origine n'est pas disponible ou ne peut pas traiter les demandes entrantes, il renvoie un code d'état HTTP 503 (Service Unavailable). CloudFront transmet ensuite l'erreur à l'utilisateur. Pour résoudre ce problème, essayez les solutions suivantes :

- Si vous utilisez Amazon S3 comme serveur d'origine :
  - Vous pouvez envoyer 3 500 requêtes PUT/COPY/POST/DELETE ou 5 500 requêtes GET/HEAD par seconde et par préfixe Amazon S3 partitionné. Lorsqu'Amazon S3 renvoie une réponse 503 Slow Down, cela indique généralement un taux de demandes excessif par rapport à un préfixe Amazon S3 spécifique.

    Étant donné que les taux de demandes s'appliquent par préfixe dans un compartiment S3, les objets doivent être répartis entre plusieurs préfixes. À mesure que le taux de demandes sur les préfixes augmente progressivement, Amazon S3 évolue pour traiter les demandes pour chacun des préfixes séparément. Par conséquent, le taux de demandes global traité par le bucket est un multiple du nombre de préfixes.
  - Pour plus d’informations, consultez Optimisation de la performance d’Amazon S3 dans le Guide de l’utilisateur Amazon Simple Storage Service.

- Si vous utilisez Elastic Load Balancing comme serveur d'origine :
  - Assurez-vous que vos instances de backend peuvent répondre aux tests de santé.
  - Assurez-vous que votre équilibreur de charge et vos instances de backend peuvent gérer la charge.

  Pour plus d’informations, consultez :
  - Comment résoudre les erreurs 503 renvoyées lors de l'utilisation de Classic Load Balancer ?
  - Comment résoudre les erreurs 503 (service non disponible) depuis mon Application Load Balancer ?
- Si vous utilisez une origine personnalisée :
  - Examinez les journaux de l'application pour vous assurer que votre ordinateur d'origine dispose de ressources suffisantes, telles que la mémoire, le processeur et la taille du disque.
  - Si vous utilisez Amazon EC2 comme backend, assurez-vous que le type d’instance dispose des ressources appropriées pour traiter les demandes entrantes. Pour plus d'informations, consultez Types d'instances dans le Guide de l'utilisateur Amazon EC2.
- Si vous utilisez API Gateway :
  - Cette erreur est liée à l'intégration du backend lorsque l'API API Gateway ne parvient pas à recevoir de réponse. Le serveur principal peut être :
    - Surchargé au-delà de sa capacité et incapable de traiter les nouvelles demandes des clients.
    - En maintenance temporaire.
  - Pour résoudre cette erreur, consultez les journaux de votre application API Gateway afin de déterminer s'il existe un problème lié à la capacité du backend, à l'intégration ou à autre chose.

CloudFront a provoqué l'erreur en raison de contraintes de ressources à l'emplacement périphérique

Vous recevrez cette erreur dans les rares cas où vous ne CloudFront pouvez pas acheminer les demandes vers le meilleur emplacement périphérique disponible suivant et ne pouvez donc pas satisfaire une demande. Cette erreur est courante lorsque vous effectuez des tests de charge sur votre CloudFront distribution. Pour essayer d’éviter ceci, suivez les conseils de the section called “Test de charge CloudFront” pour éviter les erreurs 503 (dépassement de capacité).

Si cela se produit dans votre environnement de production, contactez AWS Support.

Lambda @Edge ou erreur d'exécution de CloudFront la fonction

Si vous utilisez Lambda @Edge ou CloudFront Functions, un code d'état HTTP 503 peut indiquer que votre fonction a renvoyé une erreur d'exécution.

Pour plus de détails sur la façon d'identifier et de résoudre les erreurs Lambda @Edge, consultez. Tester et déboguer les fonctions Lambda @Edge

Pour plus d'informations sur le test CloudFront des fonctions, consultezFonctions de test.

Limite Lambda @Edge dépassée

Si vous utilisez Lambda @Edge, un code d'état HTTP 503 peut indiquer que Lambda a renvoyé une erreur. Cette erreur peut être due à l'une des raisons suivantes :

- Le nombre d'exécutions de fonctions a dépassé l'un des quotas définis par Lambda pour limiter les exécutions dans un Région AWS (exécutions simultanées ou fréquence d'invocation).
- La fonction a dépassé le quota d'expiration de la fonction Lambda.

Pour plus d'informations sur les quotas Lambda @Edge, consultez. Quotas sur Lambda@Edge Pour plus de détails sur la façon d'identifier et de résoudre les erreurs Lambda @Edge, consultez. the section called "Test et débogage" Vous pouvez également consulter les quotas du service Lambda dans le Guide du AWS Lambda développeur.

Code d'état HTTP 504 (délai d'expiration de la passerelle)

Un code d'état HTTP 504 (délai d'expiration de la passerelle) indique que lors du CloudFront transfert d'une demande à l'origine (parce que l'objet demandé ne se trouvait pas dans le cache périphérique), l'un des événements suivants s'est produit :

- L'origine a renvoyé un code d'état HTTP 504 à CloudFront.
- L'origine n'a pas répondu avant l'expiration de la demande.

CloudFront renverra un code d'état HTTP 504 si le trafic est bloqué vers l'origine par un pare-feu ou un groupe de sécurité, ou si l'origine n'est pas accessible sur Internet. Commencez par vérifier ces problèmes. Ensuite, si l'accès n'est pas le problème, explorez les retards de l'application et les délais d'attente du serveur pour mieux identifier et résoudre les problèmes.

Rubriques

- Configurez le pare-feu sur votre serveur d'origine pour autoriser CloudFront le trafic
- Configurez les groupes de sécurité sur votre serveur d'origine pour autoriser CloudFront le trafic
- Rendez accessible votre serveur d'origine personnalisée sur Internet
- Recherchez et corrigez des réponses retardées à partir des applications sur votre serveur d'origine

Configurez le pare-feu sur votre serveur d'origine pour autoriser CloudFront le trafic

Si le pare-feu de votre serveur d'origine bloque le CloudFront trafic et CloudFront renvoie un code d'état HTTP 504, il est donc conseillé de vous assurer que ce n'est pas le problème avant de vérifier s'il existe d'autres problèmes.

La méthode que vous utilisez pour déterminer s'il s'agit d'un problème avec votre pare-feu dépend du système que votre serveur d'origine utilise :

- Si vous utilisez un pare-feu IPTables sur un serveur Linux, vous pouvez rechercher des outils et des informations qui vous aideront à travailler avec IPTables.
- Si vous utilisez le pare-feu de Windows sur un serveur Windows, consultez Ajouter ou modifier la règle de pare-feu dans la documentation Microsoft.

Lorsque vous évaluez la configuration du pare-feu sur votre serveur d'origine, recherchez les pare-feux ou les règles de sécurité qui bloquent le trafic en provenance des emplacements CloudFront périphériques, en fonction de la plage d'adresses IP publiée. Pour plus d'informations, consultez Emplacements et plages d'adresses IP des serveurs CloudFront périphériques.

Si la plage d'adresses CloudFront IP est autorisée à se connecter à votre serveur d'origine, veillez à mettre à jour les règles de sécurité de votre serveur afin d'intégrer les modifications. Vous pouvez vous abonner à une rubrique Amazon SNS et recevoir des notifications lorsque le fichier de plage d'adresses IP est mis à jour. Après avoir reçu la notification, vous pouvez utiliser le code pour extraire le fichier, l'analyser et effectuer des ajustements pour votre environnement local. Pour plus d'informations, consultez la section S'abonner aux modifications d'adresse IP AWS publique via Amazon SNS sur le blog d' AWS actualités.

Configurez les groupes de sécurité sur votre serveur d'origine pour autoriser CloudFront le trafic

Si votre origine utilise Elastic Load Balancing, passez en revue les groupes de sécurité ELB et assurez-vous qu'ils autorisent le trafic entrant en provenance de. CloudFront

Vous pouvez également l'utiliser AWS Lambda pour mettre à jour automatiquement vos groupes de sécurité afin d'autoriser le trafic entrant en provenance de CloudFront.

Rendez accessible votre serveur d’origine personnalisée sur Internet

Si CloudFront vous ne parvenez pas à accéder à votre serveur d'origine personnalisé parce qu'il n'est pas accessible au public sur Internet, CloudFront renvoie une erreur HTTP 504.

CloudFront les emplacements périphériques se connectent aux serveurs d'origine via Internet. Si votre origine personnalisée se trouve sur un réseau privé, CloudFront vous ne pouvez pas y accéder. Pour cette raison, vous ne pouvez pas utiliser de serveurs privés, y compris les équilibreurs de charge classiques internes, comme serveurs d'origine avec CloudFront.

Pour vérifier que le trafic Internet peut se connecter à votre serveur d'origine, exécutez les commandes suivantes (où se *OriginDomainName*trouve le nom de domaine de votre serveur) :

Pour le trafic HTTPS :

- NC-ZV 443 *OriginDomainName*
- telnet 443 *OriginDomainName*

Pour le trafic HTTP :

- NC-ZV 80 *OriginDomainName*
- telnet 80 *OriginDomainName*

Recherchez et corrigez des réponses retardées à partir des applications sur votre serveur d’origine

Les délais d’attente du serveur sont souvent le résultat d’une application qui met beaucoup de temps à répondre ou de la définition d’une valeur de délai d’attente trop faible.

Une solution rapide pour éviter les erreurs HTTP 504 consiste simplement à définir une valeur de CloudFront délai d'expiration plus élevée pour votre distribution. Cependant, nous vous recommandons de commencer par vous assurer que vous traitez tous les problèmes de performances et de latence liés à l’application et au serveur d’origine. Ensuite, vous pouvez définir une valeur de délai d’attente raisonnable qui vise à empêcher les erreurs HTTP 504 et qui offre une bonne réactivité aux utilisateurs.

Voici une vue d'ensemble des étapes que vous pouvez suivre pour rechercher des problèmes de performances et les corriger :

1. Mesurez la latence standard et à charge élevée (réactivité) de votre application web.
2. Ajoutez d'autres ressources, telles que l'UC ou la mémoire, si nécessaire. Prenez d'autres mesures pour résoudre les problèmes, telles que le réglage des requêtes de base de données pour prendre en charge les scénarios à charge élevée.
3. Si nécessaire, ajustez la valeur du délai d'expiration pour votre CloudFront distribution.

Vous trouverez ci-après des détails relatifs à chaque étape.

Mesure de la latence standard et à charge élevée

Pour déterminer si un ou plusieurs serveurs d'application web backend présentent une latence élevée, exécutez la commande curl Linux suivante sur chaque serveur :

```
curl -w "Connect time: %{time_connect} Time to first byte: %{time_starttransfer} Total
 time: %{time_total} \n" -o /dev/null https://www.example.com/yourobject
```

> **Note**
>
> Si vous exécutez Windows sur vos serveurs, vous pouvez rechercher et télécharger curl pour Windows afin d'exécuter une commande similaire.

Lorsque vous mesurez et évaluez la latence d'une application qui s'exécute sur votre serveur, gardez à l'esprit les points suivants :

- Les valeurs de latence sont relatives à chaque application. Toutefois, un délai jusqu'au premier octet en millisecondes plutôt qu'en secondes ou plus est raisonnable.
- Si vous mesurez la latence de l'application sous une charge normale et qu'elle est satisfaisante, sachez que les utilisateurs peuvent tout de même connaître des dépassements de délais d'attente sous une charge élevée. Lorsqu'il y a une forte demande, les serveurs peuvent avoir des réponses différées ou aucune réponse du tout. Pour essayer d'éviter les problèmes de latence en cas de charge élevée, vérifiez les ressources de vos serveurs telles que l'UC, la mémoire et les lectures et écritures sur disque pour vous assurer que vos serveurs ont la capacité d'évoluer suffisamment pour traiter une charge élevée.

Vous pouvez exécuter la commande Linux suivante pour vérifier la mémoire utilisée par les processus Apache :

```
watch -n 1 "echo -n 'Apache Processes: ' && ps -C apache2 --no-headers | wc -l && free -m"
```

- Une utilisation intensive de l'UC sur le serveur peut réduire considérablement les performances d'une application. Si vous utilisez une instance Amazon EC2 pour votre serveur principal, passez en revue les CloudWatch métriques du serveur afin de vérifier l'utilisation du processeur. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon. Ou, si vous utilisez votre propre serveur, reportez-vous à la documentation d'aide du serveur pour obtenir des instructions sur la manière de vérifier l'utilisation de l'UC.
- Recherchez d'autres problèmes potentiels sous des charges élevées, telles que les requêtes de base de données qui s'exécutent lentement dans le cas d'un grand volume de demandes.

Ajout de ressources et réglage des serveurs et des bases de données

Une fois que vous avez évalué la réactivité de vos applications et serveurs, assurez-vous d'avoir les ressources suffisantes en place pour gérer des situations à trafic standard et à charge élevée :

- Si vous possédez votre propre serveur, assurez-vous qu'il a suffisamment d'UC, de mémoire et d'espace disque pour gérer les demandes des utilisateurs, en fonction de votre évaluation.
- Si vous utilisez une instance Amazon EC2 comme serveur backend, assurez-vous que le type d'instance dispose des ressources appropriées pour traiter les demandes entrantes. Pour plus d'informations, consultez Types d'instances dans le Guide de l'utilisateur Amazon EC2.

En outre, prenez en compte les étapes de réglage suivantes pour essayer d'éviter le dépassement des délais d'attente :

- Si la valeur du délai jusqu'au premier octet qui est renvoyée par la commande curl semble élevée, prenez des mesures pour améliorer les performances de votre application. L'amélioration de la réactivité de l'application aidera à son tour à réduire les erreurs de dépassement de délai.
- Réglez les requêtes de base de données pour vous assurer que de grands volumes de requêtes peuvent être gérés sans ralentir les performances.
- Configurez des connexions keep-alive (persistantes) sur votre serveur backend. Cette option permet d'éviter les latences qui se produisent lorsque les connexions doivent être rétablies pour des demandes ou des utilisateurs suivants.

- Si vous utilisez ELB comme origine, découvrez comment vous pouvez réduire la latence en passant en revue les suggestions présentées dans l'article suivant du Centre de connaissances : Comment résoudre les problèmes de latence élevée liés à ELB Classic Load Balancer ?

Si nécessaire, ajustez la valeur du CloudFront délai d'attente

Si vous avez évalué et traité le problème de la lenteur de la performance de l'application, de la capacité du serveur d'origine et d'autres problèmes, mais que les utilisateurs connaissent encore des erreurs HTTP 504, vous devez envisager de modifier le temps spécifié dans votre distribution comme délai d'attente de réponse de l'origine. Pour plus d'informations, consultez the section called "Délai de réponse (origines personnalisées uniquement)".

Test de charge CloudFront

Les méthodes traditionnelles de test de charge ne fonctionnent pas bien, CloudFront car elles CloudFront utilisent le DNS pour équilibrer les charges entre des emplacements périphériques géographiquement dispersés et au sein de chaque emplacement périphérique. Lorsqu'un client demande du contenu à CloudFront, il reçoit une réponse DNS qui inclut un ensemble d'adresses IP. Si vous effectuez un test en envoyant des requêtes à une seule des adresses IP renvoyées par le DNS, vous ne testez qu'un petit sous-ensemble de ressources dans un emplacement CloudFront périphérique, ce qui ne représente pas exactement les modèles de trafic réels. Selon le volume de données demandé, les tests effectués de cette manière peuvent surcharger et dégrader les performances de ce petit sous-ensemble de CloudFront serveurs.

CloudFront est conçu pour s'adapter aux utilisateurs qui ont des adresses IP clients différentes et des résolveurs DNS différents dans plusieurs régions géographiques. Pour effectuer des tests de charge permettant d'évaluer avec précision les CloudFront performances, nous vous recommandons d'effectuer toutes les opérations suivantes :

- Envoyez les demandes des clients depuis plusieurs régions géographiques.
- Configurez votre test de manière à ce que chaque client fasse une demande DNS indépendante. Chaque client recevra alors un ensemble d'adresses IP différent de la part du DNS.
- Pour chaque client qui fait des demandes, répartissez les demandes de vos clients sur l'ensemble des adresses IP renvoyées par le DNS. Cela garantit que la charge est répartie sur plusieurs serveurs situés dans un emplacement CloudFront périphérique.

Remarques

- Les tests de charge ne sont pas autorisés sur les comportements de cache dotés de déclencheurs de demande ou de réponse de lecteur Lambda @Edge.
- Les tests de charge ne sont pas autorisés sur les origines sur lesquelles Origin Shield est activé.

Quotas

CloudFront est soumis aux quotas suivants.

Rubriques

Quotas généraux

Entité	Quota par défaut
Débit de transfert des données par distribution	150 Gb/s Demander une augmentation du quota

Entité	Quota par défaut
Demandes par seconde par distribution	250 000 Demander une augmentation du quota
Balises pouvant être ajoutées à une distribution	50 Demander une augmentation du quota
Fichiers que vous pouvez servir par distribution	Pas de quota
Longueur maximale d'une demande ou d'une réponse d'origine, y compris les en-têtes et les chaînes de requête, à l'exclusion du corps du contenu	20 480 octets
Longueur maximale d'une URL	8 192 octets

Quotas généraux sur les distributions

Entité	Quota par défaut
Noms de domaine alternatifs (CNAME) par distribution Pour de plus amples informations, veuillez consulter Utilisez des URL personnalisées en ajoutant des noms de domaine alternatifs (CNames).	100 Demander une augmentation du quota
Comportements de cache par distribution	25 Demander une augmentation du quota
Tentatives de connexion par origine	1 à 3

Entité	Quota par défaut
Pour de plus amples informations, veuillez consulter Tentatives de connexion.	
Délai de connexion par origine Pour de plus amples informations, veuillez consulter Délai de connexion.	1 à 10 secondes
Distributions par Compte AWS Pour plus d'informations, consultez Créer une distribution.	200 Demander une augmentation du quota
Contrôle d'accès aux distributions par origine	100 Demander une augmentation du quota
Compression de fichiers : plage de tailles de fichiers qui CloudFront compresse Pour plus d'informations, consultez Servir des fichiers compressés.	1 000 à 10 000 000 octets
Délai de maintien en vie par origine Pour plus d'informations, consultez Délai d'attente des connexions actives (origines personnalisées uniquement).	1 à 60 secondes Demander une augmentation du quota
Taille de fichier maximale pouvant être mise en cache par réponse HTTP GET. Seules les réponses pour HTTP GET sont mises en cache. Les réponses pour POST et PUT ne sont pas mises en cache.	50 Go
Contrôles d'accès à Origin par Compte AWS	100

Entité	Quota par défaut
Identités d'accès à l'origine par Compte AWS	100 Demander une augmentation du quota
Origines par distribution	25 Demander une augmentation du quota
Groupes d'origine par distribution	10 Demander une augmentation du quota
Délai de réponse par origine Pour de plus amples informations, veuillez consulter Délai de réponse (origines personnalisées uniquement).	1 à 60 secondes Demander une augmentation du quota
Répartition des distributions par Compte AWS Pour plus d'informations, consultez the section called "Utilisez le déploiement continu pour tester les modifications en toute sécurité".	20 Demander une augmentation du quota

Quotas généraux sur les politiques

Entité	Quota par défaut
Politiques de cache par Compte AWS	20

Entité	Quota par défaut
	Demander une augmentation du quota
Distributions associées à la même politique de cache	100
Chaînes de requête par politique de cache	10 Demander une augmentation du quota
En-têtes par politique de cache	10 Demander une augmentation du quota
Cookies par politique de cache	10 Demander une augmentation du quota
Longueur totale combinée de tous les noms de chaîne de requête, d'en-tête et de cookie dans une politique de cache	1 024
Politiques de demande d'origine par Compte AWS	20 Demander une augmentation du quota
Distributions associées à la même politique de demande d'origine	100

Entité	Quota par défaut
Chaînes de requête par politique de demande d'origine	10 Demander une augmentation du quota
En-têtes par politique de demande d'origine	10 Demander une augmentation du quota
Politique de demande de cookies par origine	10 Demander une augmentation du quota
Longueur totale combinée de tous les noms de chaîne de requête, d'en-tête et de cookie dans une stratégie de demande d'origine	1 024
Politiques relatives aux en-têtes de réponse par Compte AWS	20 Demander une augmentation du quota
Distributions associées à la même politique d’en-têtes de réponses	100 Demander une augmentation du quota
En-têtes personnalisés par politique d’en-têtes de réponses	10 Demander une augmentation du quota

Entité	Quota par défaut
Politiques de déploiement continu par Compte AWS	20 Demander une augmentation du quota

Quotas relatifs aux CloudFront fonctions

Entité	Quota par défaut
Fonctions par Compte AWS	100
Taille de fonction maximale	10 Ko Demander une augmentation du quota
Mémoire de fonction maximale	2 Mo
Distributions associées à la même politique de fonction	100

Outre ces quotas, il existe d'autres restrictions lors de l'utilisation de CloudFront Functions. Pour plus d'informations, consultez Restrictions relatives aux CloudFront fonctions.

Quotas sur les magasins de clés-valeurs

Entité	Quota par défaut
Taille maximale d'une clé dans une paire clé-valeur	512 octets
Taille maximale de la valeur dans une paire clé-valeur	1 Ko
Nombre maximal de paires clé-valeur que vous pouvez mettre à jour dans une seule demande d'API	50 clés ou 3 Mo de charge utile, selon

Entité	Quota par défaut
	la première valeur atteinte
Taille maximale d'un magasin de clés-valeurs individuel	5 Mo
Nombre maximal de fonctions auxquelles un magasin de clés-valeurs unique peut être associé	10
Nombre maximal de magasins de clés-valeurs par fonction	1
Nombre maximal de magasins de clés-valeurs par compte	50 Demander une augmentation du quota

Quotas sur Lambda@Edge

Les quotas de cette section s'appliquent à Lambda@Edge. Ces quotas s'ajoutent aux AWS Lambda quotas par défaut, qui s'appliquent également. Pour les quotas Lambda, consultez Quotas dans le Guide du développeur AWS Lambda .

> **Note**
>
> Lambda met à l'échelle de façon dynamique la capacité pour répondre à une augmentation du trafic, dans les quotas associés à votre Compte AWS. Pour plus d'informations, consultez Scalabilité d'une fonction dans le Guide du développeur AWS Lambda .

Quotas généraux

Entité	Quota par défaut
Distributions par Compte AWS lesquelles des fonctions Lambda @Edge peuvent être utilisées	500 Demander l'augmentation du quota

Entité	Quota par défaut
Fonctions Lambda@Edge par distribution	100 Demander l'augmentation du quota
Demandes par seconde	10 000 (dans chaque Région AWS) Demander l'augmentation du quota
Exécutions simultanées Pour plus d'informations, consultez Scalabilité d'une fonction dans le Guide du développeur AWS Lambda .	1 000 (dans chaque Région AWS) Demander l'augmentation du quota
Distributions associées à la même fonction	500

Quotas selon le type d'événement

Entité	Événements de demande de l'utilisateur et de réponse à l'utilisateur	Événements de demande de l'origine et de réponse à l'origine
Taille de la mémoire de la fonction	128 Mo	Identique aux quotas Lambda.
Fonction timeout. Cette fonction peut effectuer des appels réseau vers des ressources telles que des compartiments Amazon S3, des tables DynamoDB ou des instances Amazon EC2 dans Régions AWS.	5 secondes	30 secondes
Taille d'une réponse qui est générée par une fonction Lambda, en-têtes et corps compris	40 Ko	1 Mo

Entité	Événements de demande de l'utilisateur et de réponse à l'utilisateur	Événements de demande de l'origine et de réponse à l'origine
Taille compressée maximale de votre fonction Lambda et des bibliothèques associées	1 Mo	50 Mo

Outre ces quotas, d'autres restrictions s'appliquent lors de l'utilisation des fonctions Lambda@Edge. Pour de plus amples informations, veuillez consulter Restrictions sur Lambda@Edge.

Quotas sur les certificats SSL

Entité	Quota par défaut
Certificats SSL utilisés Compte AWS lors de l'envoi de requêtes HTTPS à l'aide d'adresses IP dédiées (aucun quota lors du traitement de requêtes HTTPS via SNI) Pour plus d'informations, consultez Utilisez le protocole HTTPS avec CloudFront.	2 Demander une augmentation du quota
Certificats SSL pouvant être associés à une CloudFront distribution	1

Si votre certificat SSL est spécifiquement destiné à la communication HTTPS entre les utilisateurs et CloudFront que vous avez utilisé AWS Certificate Manager (ACM) ou le magasin de certificats IAM pour approvisionner ou importer votre certificat, des quotas supplémentaires s'appliquent. Pour plus d'informations, consultez Quotas d'utilisation des certificats SSL/TLS avec CloudFront (HTTPS entre utilisateurs et uniquement) CloudFront .

Il existe également des quotas sur le nombre de certificats SSL que vous pouvez importer dans AWS Certificate Manager (ACM) ou télécharger vers AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Augmenter les quotas pour les certificats SSL/TLS.

Quotas sur les invalidations

Entité	Quota par défaut
Invalidation de fichier : nombre maximal de fichiers autorisés dans les requêtes d'invalidation actives, à l'exclusion des invalidations de caractère générique Pour de plus amples informations, veuillez consulter Invalider des fichiers pour supprimer du contenu.	3 000
Invalidation de fichier : nombre maximal d'invalidations de caractère générique actives autorisées	15
Invalidation de fichier : nombre maximal de fichiers qu'une invalidation de caractère générique peut traiter	Pas de quota

Quotas sur les groupes clés

Entité	Quota par défaut
Clés publiques dans un seul groupe clé	5 Demander une augmentation du quota
Groupes clés associés à un seul comportement du cache	4 Demander une augmentation du quota
Groupes clés par Compte AWS	10 Demander une augmentation du quota

Entité	Quota par défaut
Répartitions associées à un seul groupe clé	100 Demander une augmentation du quota

Quotas sur WebSocket les connexions

Entité	Quota par défaut
Délai de réponse de l'origine (délai d'inactivité)	10 minutes Si aucun octet CloudFront n'a été détecté depuis l'origine vers le client au cours des 10 dernières minutes, la connexion est considérée comme inactive et est fermée.

Quotas sur le chiffrement au niveau du champ

Entité	Quota par défaut
Longueur maximale d'un champ à chiffrer Pour de plus amples informations, veuillez consulter Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.	16 Ko
Nombre maximal de champs dans le corps d'une requête lorsque le chiffrement au niveau du champ est configuré	10

Entité	Quota par défaut
Longueur maximale du corps d'une demande lorsque le chiffrement au niveau du champ est configuré	1 Mo
Nombre maximal de configurations de chiffrement au niveau du champ pouvant être associées à une Compte AWS	10
Nombre maximal de profils de chiffrement au niveau du champ pouvant être associés à un Compte AWS	10
Nombre maximal de clés publiques qui peuvent être ajoutées à un Compte AWS	10
Nombre maximum de champs à chiffrer qui peuvent être spécifiés dans un profil	10
Nombre maximal de CloudFront distributions pouvant être associées à une configuration de chiffrement au niveau du champ	20
Nombre maximum de mappages de profil d'argument de requête qui peuvent être inclus dans une configuration de chiffrement au niveau du champ	5

Quotas sur les cookies (paramètres de cache hérités)

Ces quotas s'appliquent aux CloudFront anciens paramètres de cache. Nous recommandons d'utiliser une politique de cache ou une politique de demande d'origine au lieu des anciens paramètres.

Entité	Quota par défaut
Cookies par comportement du cache Pour de plus amples informations, veuillez consulter Contenu du cache basé sur les cookies.	10 Demander une augmentation du quota

Entité	Quota par défaut
Nombre total d'octets dans les noms des cookies (ne s'applique pas si vous configurez CloudFront pour transférer tous les cookies à l'origine)	512 moins le nombre de cookies

Quotas sur les chaînes de requêtes (paramètres de cache hérités)

Ces quotas s'appliquent aux CloudFront anciens paramètres de cache. Nous recommandons d'utiliser une politique de cache ou une politique de demande d'origine au lieu des anciens paramètres.

Entité	Quota par défaut
Nombre maximal de caractères dans une chaîne de requêtes	128 caractères
Le nombre maximal de caractères au total pour toutes les chaînes de requêtes dans le même paramètre	512 caractères
Chaînes de requêtes par comportement du cache Pour de plus amples informations, veuillez consulter Contenu du cache basé sur les paramètres de chaîne de requête.	10 Demander une augmentation du quota

Quotas sur les en-têtes

Entité	Quota par défaut
En-têtes par comportement du cache (paramètres de cache hérités) Pour plus d’informations, consultez the section called “Contenu du cache basé sur les en-têtes des demandes”.	10 Demander une augmentation du quota
En-têtes personnalisés : nombre maximum d'en-têtes personnalisés que vous pouvez configurer CloudFront pour ajouter aux demandes d'origine	10

Entité	Quota par défaut
Pour plus d'informations, consultez the section called "Ajouter des en-têtes personnalisés aux demandes d'origine".	Demander une augmentation du quota
En-têtes personnalisés : nombre maximal d'en-têtes personnalisés que vous pouvez ajouter à une politique d'en-têtes de réponses	10 Demander une augmentation du quota
En-têtes personnalisés : longueur maximale d'un nom d'en-tête	256 caractères
En-têtes personnalisés : longueur maximale d'une valeur d'en-tête	1,783 caractères
En-têtes personnalisés : longueur maximale de tous les noms et valeurs d'en-tête combinés	10 240 caractères
Longueur maximale de la valeur de l'en-tête `Content-Security-Policy`	1 783 caractères Demander une augmentation du quota

Exemples de code pour CloudFront l'utilisation des AWS SDK

Les exemples de code suivants montrent comment utiliser CloudFront un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Les Scénarios sont des exemples de code qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Actions relatives à CloudFront l'utilisation des AWS SDK
  - Utilisation CreateDistribution avec un AWS SDK ou une CLI
  - Utilisation CreateFunction avec un AWS SDK ou une CLI
  - Utilisation CreateInvalidation avec un AWS SDK ou une CLI
  - Utilisation CreateKeyGroup avec un AWS SDK ou une CLI
  - Utilisation CreatePublicKey avec un AWS SDK ou une CLI
  - Utilisation DeleteDistribution avec un AWS SDK ou une CLI
  - Utilisation GetCloudFrontOriginAccessIdentity avec un AWS SDK ou une CLI
  - Utilisation GetCloudFrontOriginAccessIdentityConfig avec un AWS SDK ou une CLI
  - Utilisation GetDistribution avec un AWS SDK ou une CLI
  - Utilisation GetDistributionConfig avec un AWS SDK ou une CLI
  - Utilisation ListCloudFrontOriginAccessIdentities avec un AWS SDK ou une CLI
  - Utilisation ListDistributions avec un AWS SDK ou une CLI
  - Utilisation UpdateDistribution avec un AWS SDK ou une CLI

Actions relatives à CloudFront l'utilisation des AWS SDK

Les exemples de code suivants montrent comment effectuer des CloudFront actions individuelles avec AWS les SDK. Ces extraits appellent l' CloudFront API et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une liste complète, consultez le Amazon CloudFront API Reference.

Exemples

- Utilisation CreateDistribution avec un AWS SDK ou une CLI
- Utilisation CreateFunction avec un AWS SDK ou une CLI
- Utilisation CreateInvalidation avec un AWS SDK ou une CLI
- Utilisation CreateKeyGroup avec un AWS SDK ou une CLI
- Utilisation CreatePublicKey avec un AWS SDK ou une CLI
- Utilisation DeleteDistribution avec un AWS SDK ou une CLI
- Utilisation GetCloudFrontOriginAccessIdentity avec un AWS SDK ou une CLI
- Utilisation GetCloudFrontOriginAccessIdentityConfig avec un AWS SDK ou une CLI
- Utilisation GetDistribution avec un AWS SDK ou une CLI
- Utilisation GetDistributionConfig avec un AWS SDK ou une CLI
- Utilisation ListCloudFrontOriginAccessIdentities avec un AWS SDK ou une CLI
- Utilisation ListDistributions avec un AWS SDK ou une CLI
- Utilisation UpdateDistribution avec un AWS SDK ou une CLI

Utilisation **`CreateDistribution`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateDistribution`.

CLI

AWS CLI

Pour créer une CloudFront distribution

L'exemple suivant crée une distribution pour un compartiment S3 nomméawsexamplebucket, et le spécifie également `index.html` comme objet racine par défaut, à l'aide d'arguments de ligne de commande :

```
aws cloudfront create-distribution \
    --origin-domain-name awsexamplebucket.s3.amazonaws.com \
    --default-root-object index.html
```

Au lieu d'utiliser des arguments de ligne de commande, vous pouvez fournir la configuration de distribution dans un fichier JSON, comme illustré dans l'exemple suivant :

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Le fichier `dist-config.json` est un document JSON dans le dossier actuel qui contient les éléments suivants :

```
{
    "CallerReference": "cli-example",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                "DomainName": "awsexamplebucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
```

```
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-example",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
```

```
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": true,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Que vous fournissiez les informations de distribution avec un argument de ligne de commande ou un fichier JSON, le résultat est le même :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EMLARXS9EXAMPLE",
    "ETag": "E9LHASXEXAMPLE",
```

```
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-11-22T00:55:15.705Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
```

```
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
```

```
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Pour plus de détails sur l'API, voir CreateDistributionla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple suivant utilise un bucket Amazon Simple Storage Service (Amazon S3) comme origine de contenu.

Après avoir créé la distribution, le code crée un CloudFrontWaiterpour attendre que la distribution soit déployée avant de renvoyer la distribution.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.ItemSelection;
import software.amazon.awssdk.services.cloudfront.model.Method;
import software.amazon.awssdk.services.cloudfront.model.ViewerProtocolPolicy;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;
import software.amazon.awssdk.services.s3.S3Client;

import java.time.Instant;

public class CreateDistribution {

        private static final Logger logger =
 LoggerFactory.getLogger(CreateDistribution.class);

        public static Distribution createDistribution(CloudFrontClient
 cloudFrontClient, S3Client s3Client,
                        final String bucketName, final String keyGroupId, final
 String originAccessControlId) {

                final String region = s3Client.headBucket(b ->
 b.bucket(bucketName)).sdkHttpResponse().headers()
                                .get("x-amz-bucket-region").get(0);
                final String originDomain = bucketName + ".s3." + region +
 ".amazonaws.com";
                String originId = originDomain; // Use the originDomain value for
 the originId.

                // The service API requires some deprecated methods, such as
                // DefaultCacheBehavior.Builder#minTTL and #forwardedValue.
                CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                                .distributionConfig(b1 -> b1
```

```
                                                .origins(b2 -> b2
                                                                .quantity(1)
                                                                .items(b3 -> b3

.domainName(originDomain)

.id(originId)

.s3OriginConfig(builder4 -> builder4

              .originAccessIdentity(

                                 ""))

.originAccessControlId(

              originAccessControlId)))
                                                .defaultCacheBehavior(b2 -> b2

.viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)

.targetOriginId(originId)
                                                                .minTTL(200L)

.forwardedValues(b5 -> b5

.cookies(cp -> cp

              .forward(ItemSelection.NONE))

.queryString(true))

.trustedKeyGroups(b3 -> b3

.quantity(1)

.items(keyGroupId)

.enabled(true))

.allowedMethods(b4 -> b4

.quantity(2)
```

```
.items(Method.HEAD, Method.GET)

.cachedMethods(b5 -> b5

              .quantity(2)

              .items(Method.HEAD,

                            Method.GET))))
                                          .cacheBehaviors(b -> b
                                                         .quantity(1)
                                                         .items(b2 -> b2

.pathPattern("/index.html")

.viewerProtocolPolicy(

              ViewerProtocolPolicy.ALLOW_ALL)

.targetOriginId(originId)

.trustedKeyGroups(b3 -> b3

              .quantity(1)

              .items(keyGroupId)

              .enabled(true))

.minTTL(200L)

.forwardedValues(b4 -> b4

              .cookies(cp -> cp

                            .forward(ItemSelection.NONE))

              .queryString(true))

.allowedMethods(b5 -> b5.quantity(2)

              .items(Method.HEAD,
```

```
                                Method.GET)

                .cachedMethods(b6 -> b6

                                .quantity(2)

                                .items(Method.HEAD,

                                                Method.GET)))))
                                 .enabled(true)
                                 .comment("Distribution built with
 java")

 .callerReference(Instant.now().toString())));

                final Distribution distribution =
 createDistResponse.distribution();
                logger.info("Distribution created. DomainName: [{}]  Id: [{}]",
 distribution.domainName(),
                                 distribution.id());
                logger.info("Waiting for distribution to be deployed ...");
                try (CloudFrontWaiter cfWaiter =
 CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
                        ResponseOrException<GetDistributionResponse>
 responseOrException = cfWaiter
                                        .waitUntilDistributionDeployed(builder ->
 builder.id(distribution.id()))
                                        .matched();
                        responseOrException.response()
                                        .orElseThrow(() -> new
 RuntimeException("Distribution not created"));
                        logger.info("Distribution deployed. DomainName: [{}]  Id:
 [{}]", distribution.domainName(),
                                        distribution.id());
                }
                return distribution;
        }
}
```

- Pour plus de détails sur l'API, voir CreateDistributionla section Référence des AWS SDK for Java 2.x API.

PowerShell

Outils pour PowerShell

Exemple 1 : crée une CloudFront distribution de base, configurée avec la journalisation et la mise en cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "ps-cmdlet-sample.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
      -Logging_Bucket ps-cmdlet-sample-logging.s3.amazonaws.com `
      -Logging_Prefix "help/" `
      -DistributionConfig_CallerReference Client1 `
      -DistributionConfig_DefaultRootObject index.html `
      -DefaultCacheBehavior_TargetOriginId $origin.Id `
      -ForwardedValues_QueryString $true `
      -Cookies_Forward all `
      -WhitelistedNames_Quantity 0 `
      -TrustedSigners_Enabled $false `
      -TrustedSigners_Quantity 0 `
      -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
      -DefaultCacheBehavior_MinTTL 1000 `
      -DistributionConfig_PriceClass "PriceClass_All" `
      -CacheBehaviors_Quantity 0 `
      -Aliases_Quantity 0
```

- Pour plus de détails sur l'API, consultez la section CreateDistributionRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateFunction`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`CreateFunction`.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.CloudFrontException;
import software.amazon.awssdk.services.cloudfront.model.CreateFunctionRequest;
import software.amazon.awssdk.services.cloudfront.model.CreateFunctionResponse;
import software.amazon.awssdk.services.cloudfront.model.FunctionConfig;
import software.amazon.awssdk.services.cloudfront.model.FunctionRuntime;
import java.io.InputStream;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateFunction {

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <functionName> <filePath>

                Where:
```

```
                    functionName - The name of the function to create.\s
                    filePath - The path to a file that contains the application
logic for the function.\s
                 """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        String filePath = args[1];
        CloudFrontClient cloudFrontClient = CloudFrontClient.builder()
                .region(Region.AWS_GLOBAL)
                .build();

        String funArn = createNewFunction(cloudFrontClient, functionName,
filePath);
        System.out.println("The function ARN is " + funArn);
        cloudFrontClient.close();
    }

    public static String createNewFunction(CloudFrontClient cloudFrontClient,
String functionName, String filePath) {
        try {
            InputStream fileIs =
CreateFunction.class.getClassLoader().getResourceAsStream(filePath);
            SdkBytes functionCode = SdkBytes.fromInputStream(fileIs);

            FunctionConfig config = FunctionConfig.builder()
                    .comment("Created by using the CloudFront Java API")
                    .runtime(FunctionRuntime.CLOUDFRONT_JS_1_0)
                    .build();

            CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
                    .name(functionName)
                    .functionCode(functionCode)
                    .functionConfig(config)
                    .build();

            CreateFunctionResponse response =
cloudFrontClient.createFunction(functionRequest);
            return response.functionSummary().functionMetadata().functionARN();
```

```
        } catch (CloudFrontException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Pour plus de détails sur l'API, voir CreateFunctionla section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateInvalidation`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateInvalidation`.

CLI

AWS CLI

Pour créer une invalidation pour une distribution CloudFront

L'`create-invalidation`exemple suivant crée une invalidation pour les fichiers spécifiés dans la CloudFront distribution spécifiée :

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --paths "/example-path/example-file.jpg" "/example-path/example-file2.png"
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I1JLWSDAP8FU89",
    "Invalidation": {
        "Id": "I1JLWSDAP8FU89",
        "Status": "InProgress",
```

```
        "CreateTime": "2019-12-05T18:24:51.407Z",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file2.png",
                    "/example-path/example-file.jpg"
                ]
            },
            "CallerReference": "cli-1575570291-670203"
        }
    }
}
```

Dans l'exemple précédent, la AWS CLI a automatiquement généré un résultat aléatoire`CallerReference`. Pour spécifier les vôtres `CallerReference` ou pour éviter de transmettre les paramètres d'invalidation en tant qu'arguments de ligne de commande, vous pouvez utiliser un fichier JSON. L'exemple suivant crée une invalidation pour deux fichiers, en fournissant les paramètres d'invalidation dans un fichier JSON nommé : `inv-batch.json`

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --invalidation-batch file://inv-batch.json
```

Contenu de `inv-batch.json` :

```
{
    "Paths": {
        "Quantity": 2,
        "Items": [
            "/example-path/example-file.jpg",
            "/example-path/example-file2.png"
        ]
    },
    "CallerReference": "cli-example"
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I2J0I21PCUYOIK",
```

```
    "Invalidation": {
        "Id": "I2J0I21PCUYOIK",
        "Status": "InProgress",
        "CreateTime": "2019-12-05T18:40:49.413Z",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file.jpg",
                    "/example-path/example-file2.png"
                ]
            },
            "CallerReference": "cli-example"
        }
    }
}
```

- Pour plus de détails sur l'API, voir CreateInvalidationla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple crée une nouvelle invalidation sur une distribution dont l'ID est EXAMPLENSTXAXE. CallerReference Il s'agit d'un identifiant unique choisi par l'utilisateur ; dans ce cas, un horodatage représentant le 15 mai 2019 à 9 h 00 est utilisé. La variable $Paths stocke trois chemins d'accès aux fichiers image et multimédia que l'utilisateur ne souhaite pas inclure dans le cache de la distribution. La valeur du paramètre -Paths_Quantity est le nombre total de chemins spécifiés dans le paramètre -Paths_Item.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Sortie :

```
Invalidation                          Location

```

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

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Pour plus de détails sur l'API, consultez la section CreateInvalidationRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateKeyGroup`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`CreateKeyGroup`.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Un groupe de clés nécessite au moins une clé publique utilisée pour vérifier les URL signées ou les cookies.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;

import java.util.UUID;

public class CreateKeyGroup {
    private static final Logger logger =
 LoggerFactory.getLogger(CreateKeyGroup.class);

    public static String createKeyGroup(CloudFrontClient cloudFrontClient, String
 publicKeyId) {
```

```
        String keyGroupId = cloudFrontClient.createKeyGroup(b ->
 b.keyGroupConfig(c -> c
                .items(publicKeyId)
                .name("JavaKeyGroup" + UUID.randomUUID()))
                .keyGroup().id();
        logger.info("KeyGroup created with ID: [{}]", keyGroupId);
        return keyGroupId;
    }
}
```

- Pour plus de détails sur l'API, voir CreateKeyGroupla section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreatePublicKey`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreatePublicKey`.

CLI

AWS CLI

Pour créer une clé CloudFront publique

L'exemple suivant crée une clé CloudFront publique en fournissant les paramètres dans un fichier JSON nommépub-key-config.json. Avant de pouvoir utiliser cette commande, vous devez disposer d'une clé publique codée PEM. Pour plus d'informations, consultez la section Créer une paire de clés RSA dans le manuel Amazon CloudFront Developer Guide.

```
aws cloudfront create-public-key \
    --public-key-config file://pub-key-config.json
```

Le fichier pub-key-config.json est un document JSON dans le dossier actuel qui contient les éléments suivants. Notez que la clé publique est codée au format PEM.

```
{
```

```
    "CallerReference": "cli-example",
    "Name": "ExampleKey",
    "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----
END PUBLIC KEY-----\n",
    "Comment": "example public key"
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/public-key/
KDFB19YGCR002",
    "ETag": "E2QWRUHEXAMPLE",
    "PublicKey": {
        "Id": "KDFB19YGCR002",
        "CreatedTime": "2019-12-05T18:51:43.781Z",
        "PublicKeyConfig": {
            "CallerReference": "cli-example",
            "Name": "ExampleKey",
            "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----
END PUBLIC KEY-----\n",
            "Comment": "example public key"
        }
    }
}
```

- Pour plus de détails sur l'API, voir CreatePublicKeyla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple de code suivant lit une clé publique et la télécharge sur Amazon CloudFront.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.CreatePublicKeyResponse;
import software.amazon.awssdk.utils.IoUtils;

import java.io.IOException;
import java.io.InputStream;
import java.util.UUID;

public class CreatePublicKey {
    private static final Logger logger =
 LoggerFactory.getLogger(CreatePublicKey.class);

    public static String createPublicKey(CloudFrontClient cloudFrontClient,
 String publicKeyFileName) {
        try (InputStream is =
 CreatePublicKey.class.getClassLoader().getResourceAsStream(publicKeyFileName)) {
            String publicKeyString = IoUtils.toUtf8String(is);
            CreatePublicKeyResponse createPublicKeyResponse = cloudFrontClient
                    .createPublicKey(b -> b.publicKeyConfig(c -> c
                            .name("JavaCreatedPublicKey" + UUID.randomUUID())
                            .encodedKey(publicKeyString)
                            .callerReference(UUID.randomUUID().toString())));
            String createdPublicKeyId = createPublicKeyResponse.publicKey().id();
            logger.info("Public key created with id: [{}]", createdPublicKeyId);
            return createdPublicKeyId;

        } catch (IOException e) {
            throw new RuntimeException(e);
        }
```

```
    }
}
```

- Pour plus de détails sur l'API, voir CreatePublicKeyla section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteDistribution`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteDistribution`.

CLI

AWS CLI

Pour supprimer une CloudFront distribution

L'exemple suivant supprime la CloudFront distribution avec l'ID. `EDFDVBD6EXAMPLE` Avant de pouvoir supprimer une distribution, vous devez la désactiver. Pour désactiver une distribution, utilisez la commande update-distribution. Pour plus d'informations, consultez les exemples de distribution de mises à jour.

Lorsqu'une distribution est désactivée, vous pouvez la supprimer. Pour supprimer une distribution, vous devez utiliser l'`--if-match`option permettant de fournir les informations de la distribution`ETag`. Pour obtenir le`ETag`, utilisez la commande get-distribution orget-distribution-config .

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

En cas de réussite, cette commande n'a aucune sortie.

- Pour plus de détails sur l'API, voir DeleteDistributionla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple de code suivant met une distribution à Disabled, utilise un serveur qui attend que la modification soit déployée, puis supprime la distribution.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.DeleteDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionConfig;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;

public class DeleteDistribution {
        private static final Logger logger =
 LoggerFactory.getLogger(DeleteDistribution.class);

        public static void deleteDistribution(final CloudFrontClient
 cloudFrontClient, final String distributionId) {
                // First, disable the distribution by updating it.
                GetDistributionResponse response =
 cloudFrontClient.getDistribution(b -> b
                                .id(distributionId));
                String etag = response.eTag();
                DistributionConfig distConfig =
 response.distribution().distributionConfig();

                cloudFrontClient.updateDistribution(builder -> builder
                                .id(distributionId)
                                .distributionConfig(builder1 -> builder1

 .cacheBehaviors(distConfig.cacheBehaviors())
```

```
.defaultCacheBehavior(distConfig.defaultCacheBehavior())
                                                .enabled(false)
                                                .origins(distConfig.origins())
                                                .comment(distConfig.comment())

.callerReference(distConfig.callerReference())

.defaultCacheBehavior(distConfig.defaultCacheBehavior())

.priceClass(distConfig.priceClass())
                                                .aliases(distConfig.aliases())
                                                .logging(distConfig.logging())

.defaultRootObject(distConfig.defaultRootObject())

.customErrorResponses(distConfig.customErrorResponses())

.httpVersion(distConfig.httpVersion())

.isIPV6Enabled(distConfig.isIPV6Enabled())

.restrictions(distConfig.restrictions())

.viewerCertificate(distConfig.viewerCertificate())
                                                .webACLId(distConfig.webACLId())

.originGroups(distConfig.originGroups()))
                                .ifMatch(etag));

                logger.info("Distribution [{}] is DISABLED, waiting for
deployment before deleting ...",
                                distributionId);
                GetDistributionResponse distributionResponse;
                try (CloudFrontWaiter cfWaiter =
CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
                        ResponseOrException<GetDistributionResponse>
responseOrException = cfWaiter
                                        .waitUntilDistributionDeployed(builder ->
builder.id(distributionId)).matched();
                        distributionResponse = responseOrException.response()
                                        .orElseThrow(() -> new
RuntimeException("Could not disable distribution"));
                }
```

```
                DeleteDistributionResponse deleteDistributionResponse =
 cloudFrontClient
                                .deleteDistribution(builder -> builder
                                                .id(distributionId)

 .ifMatch(distributionResponse.eTag()));
                if (deleteDistributionResponse.sdkHttpResponse().isSuccessful())
 {
                        logger.info("Distribution [{}] DELETED", distributionId);
                }
        }
}
```

- Pour plus de détails sur l'API, voir DeleteDistributionla section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetCloudFrontOriginAccessIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetCloudFrontOriginAccessIdentity`.

CLI

AWS CLI

Pour obtenir une identité CloudFront d'accès à l'origine

L'exemple suivant obtient l'identité CloudFront d'accès à l'origine (OAI) avec l'IDE74FTE3AEXAMPLE, y compris son identifiant canonique S3 ETag et l'identifiant canonique S3 associé. L'ID OAI est renvoyé dans la sortie des commandes -access-identity et create-cloud-front-origin -access-identity. list-cloud-front-origin

```
aws cloudfront get-cloud-front-origin-access-identity --id E74FTE3AEXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
    }
}
```

- Pour plus de détails sur l'API, voir GetCloudFrontOriginAccessIdentityla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie une identité d'accès Amazon CloudFront Origin spécifique, spécifiée par le paramètre -Id. Bien que le paramètre -Id ne soit pas obligatoire, aucun résultat n'est renvoyé si vous ne le spécifiez pas.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Sortie :

```
     CloudFrontOriginAccessIdentityConfig    Id
    S3CanonicalUserId
     ------------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Pour plus de détails sur l'API, consultez la section GetCloudFrontOriginAccessIdentityRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetCloudFrontOriginAccessIdentityConfig`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetCloudFrontOriginAccessIdentityConfig`.

CLI

AWS CLI

Pour obtenir une configuration d'identité CloudFront d'accès à l'origine

L'exemple suivant obtient des métadonnées relatives à l'identité CloudFront d'accès à l'origine (OAI) avec l'ID`E74FTE3AEXAMPLE`, y compris son`ETag`. L'ID OAI est renvoyé dans la sortie des commandes -access-identity et create-cloud-front-origin -access-identity. list-cloud-front-origin

```
aws cloudfront get-cloud-front-origin-access-identity-config --id E74FTE3AEXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentityConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example OAI"
    }
}
```

- Pour plus de détails sur l'API, voir GetCloudFrontOriginAccessIdentityConfigla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie des informations de configuration concernant une seule identité CloudFront d'accès à Amazon Origin, spécifiée par le paramètre -Id. Des erreurs se produisent si aucun paramètre -Id n'est spécifié.

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Sortie :

```
     CallerReference                                                Comment
     ---------------                                                -------
     mycallerreference: 2/1/2011 1:16:32 PM                         Caller
reference: 2/1/2011 1:16:32 PM
```

- Pour plus de détails sur l'API, consultez la section GetCloudFrontOriginAccessIdentityConfigRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetDistribution`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetDistribution`.

CLI

AWS CLI

Pour obtenir une CloudFront distribution

L'exemple suivant obtient la CloudFront distribution avec l'ID`EDFDVBD6EXAMPLE`, y compris son`ETag`. L'ID de distribution est renvoyé dans les commandes create-distribution et list-distributions.

```
aws cloudfront get-distribution --id EDFDVBD6EXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "Deployed",
        "LastModifiedTime": "2019-12-04T23:35:41.433Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
```

```
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
```

```
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Pour plus de détails sur l'API, voir GetDistributionla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : récupère les informations relatives à une distribution spécifique.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, consultez la section GetDistributionRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetDistributionConfig`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetDistributionConfig`.

CLI

AWS CLI

Pour obtenir une configuration CloudFront de distribution

L'exemple suivant obtient les métadonnées relatives à la CloudFront distribution avec l'ID`EDFDVBD6EXAMPLE`, y compris son`ETag`. L'ID de distribution est renvoyé dans les commandes create-distribution et list-distributions.

```
aws cloudfront get-distribution-config --id EDFDVBD6EXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "DistributionConfig": {
        "CallerReference": "cli-example",
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                    "DomainName": "awsexamplebucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
```

```
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
```

```
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

- Pour plus de détails sur l'API, voir GetDistributionConfigla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : récupère la configuration d'une distribution spécifique.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, consultez la section GetDistributionConfigRéférence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""

    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client


    def update_distribution(self):
        distribution_id = input(
            "This script updates the comment for a CloudFront distribution.\n"
            "Enter a CloudFront distribution ID: "
        )

        distribution_config_response =
 self.cloudfront_client.get_distribution_config(
            Id=distribution_id
        )
```

```
        distribution_config = distribution_config_response["DistributionConfig"]
        distribution_etag = distribution_config_response["ETag"]

        distribution_config["Comment"] = input(
            f"\nThe current comment for distribution {distribution_id} is "
            f"'{distribution_config['Comment']}'.\n"
            f"Enter a new comment: "
        )
        self.cloudfront_client.update_distribution(
            DistributionConfig=distribution_config,
            Id=distribution_id,
            IfMatch=distribution_etag,
        )
        print("Done!")
```

- Pour plus de détails sur l'API, consultez GetDistributionConfigle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListCloudFrontOriginAccessIdentities`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListCloudFrontOriginAccessIdentities`.

CLI

AWS CLI

Pour répertorier les identités CloudFront d'accès à l'origine

L'exemple suivant permet d'obtenir une liste des identités CloudFront d'accès à l'origine (OAI) de votre AWS compte :

```
aws cloudfront list-cloud-front-origin-access-identities
```

Sortie :

```
{
    "CloudFrontOriginAccessIdentityList": {
        "Items": [
            {
                "Id": "E74FTE3AEXAMPLE",
                "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
                "Comment": "Example OAI"
            },
            {
                "Id": "EH1HDMBEXAMPLE",
                "S3CanonicalUserId":
 "1489f6f2e6faacaae7ff64c4c3e6956c24f78788abfc1718c3527c263bf7a17EXAMPLE",
                "Comment": "Test OAI"
            },
            {
                "Id": "E2X2C9TEXAMPLE",
                "S3CanonicalUserId":
 "cbfeebb915a64749f9be546a45b3fcfd3a31c779673c13c4dd460911ae402c2EXAMPLE",
                "Comment": "Example OAI #2"
            }
        ]
    }
}
```

- Pour plus de détails sur l'API, voir ListCloudFrontOriginAccessIdentitiesla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie une liste des identités CloudFront d'accès d'origine Amazon. Comme le MaxItem paramètre - spécifie une valeur de 2, les résultats incluent deux identités.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Sortie :

```
IsTruncated : True
```

```
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Pour plus de détails sur l'API, consultez la section ListCloudFrontOriginAccessIdentitiesRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListDistributions`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListDistributions`.

CLI

AWS CLI

Pour répertorier CloudFront les distributions

L'exemple suivant permet d'obtenir la liste des CloudFront distributions de votre AWS compte :

```
aws cloudfront list-distributions
```

Sortie :

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "EMLARXS9EXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
EMLARXS9EXAMPLE",
                "Status": "InProgress",
                "LastModifiedTime": "2019-11-22T00:55:15.705Z",
                "InProgressInvalidationBatches": 0,
                "DomainName": "d111111abcdef8.cloudfront.net",
                "ActiveTrustedSigners": {
```

```
                    "Enabled": false,
                    "Quantity": 0
                },
                "DistributionConfig": {
                    "CallerReference": "cli-example",
                    "Aliases": {
                        "Quantity": 0
                    },
                    "DefaultRootObject": "index.html",
                    "Origins": {
                        "Quantity": 1,
                        "Items": [
                            {
                                "Id": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                                "DomainName":
 "awsexamplebucket.s3.amazonaws.com",
                                "OriginPath": "",
                                "CustomHeaders": {
                                    "Quantity": 0
                                },
                                "S3OriginConfig": {
                                    "OriginAccessIdentity": ""
                                }
                            }
                        ]
                    },
                    "OriginGroups": {
                        "Quantity": 0
                    },
                    "DefaultCacheBehavior": {
                        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                        "ForwardedValues": {
                            "QueryString": false,
                            "Cookies": {
                                "Forward": "none"
                            },
                            "Headers": {
                                "Quantity": 0
                            },
                            "QueryStringCacheKeys": {
                                "Quantity": 0
                            }
```

```
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
```

```
                    "Enabled": true,
                    "ViewerCertificate": {
                        "CloudFrontDefaultCertificate": true,
                        "MinimumProtocolVersion": "TLSv1",
                        "CertificateSource": "cloudfront"
                    },
                    "Restrictions": {
                        "GeoRestriction": {
                            "RestrictionType": "none",
                            "Quantity": 0
                        }
                    },
                    "WebACLId": "",
                    "HttpVersion": "http2",
                    "IsIPV6Enabled": true
                }
            },
            {
                "Id": "EDFDVBD6EXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
EDFDVBD6EXAMPLE",
                "Status": "InProgress",
                "LastModifiedTime": "2019-12-04T23:35:41.433Z",
                "InProgressInvalidationBatches": 0,
                "DomainName": "d930174dauwrn8.cloudfront.net",
                "ActiveTrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "DistributionConfig": {
                    "CallerReference": "cli-example",
                    "Aliases": {
                        "Quantity": 0
                    },
                    "DefaultRootObject": "index.html",
                    "Origins": {
                        "Quantity": 1,
                        "Items": [
                            {
                                "Id": "awsexamplebucket1.s3.amazonaws.com-cli-
example",
                                "DomainName":
 "awsexamplebucket1.s3.amazonaws.com",
                                "OriginPath": "",
```

```
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            }
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "awsexamplebucket1.s3.amazonaws.com-
cli-example",
                    "ForwardedValues": {
                        "QueryString": false,
                        "Cookies": {
                            "Forward": "none"
                        },
                        "Headers": {
                            "Quantity": 0
                        },
                        "QueryStringCacheKeys": {
                            "Quantity": 0
                        }
                    },
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "MinTTL": 0,
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
```

```
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "DefaultTTL": 86400,
                    "MaxTTL": 31536000,
                    "Compress": false,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": ""
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "Logging": {
                    "Enabled": false,
                    "IncludeCookies": false,
                    "Bucket": "",
                    "Prefix": ""
                },
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": true,
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "http2",
                "IsIPV6Enabled": true
            }
        },
        {
```

```
                "Id": "E1X5IZQEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E1X5IZQEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2019-11-06T21:31:48.864Z",
                "DomainName": "d2e04y12345678.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Id": "awsexamplebucket2",
                            "DomainName": "awsexamplebucket2.s3.us-
west-2.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            }
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "awsexamplebucket2",
                    "ForwardedValues": {
                        "QueryString": false,
                        "Cookies": {
                            "Forward": "none"
                        },
                        "Headers": {
                            "Quantity": 0
                        },
                        "QueryStringCacheKeys": {
                            "Quantity": 0
                        }
                    },
                    "TrustedSigners": {
```

```
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "MinTTL": 0,
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "DefaultTTL": 86400,
                    "MaxTTL": 31536000,
                    "Compress": false,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": ""
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": true,
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
```

```
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "HTTP1_1",
                "IsIPV6Enabled": true
            }
        ]
    }
}
```

- Pour plus de détails sur l'API, voir ListDistributionsla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : renvoie les distributions.

```
Get-CFDistributionList
```

- Pour plus de détails sur l'API, consultez la section ListDistributionsRéférence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""
```

```
    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client


    def list_distributions(self):
        print("CloudFront distributions:\n")
        distributions = self.cloudfront_client.list_distributions()
        if distributions["DistributionList"]["Quantity"] > 0:
            for distribution in distributions["DistributionList"]["Items"]:
                print(f"Domain: {distribution['DomainName']}")
                print(f"Distribution Id: {distribution['Id']}")
                print(
                    f"Certificate Source: "
                    f"{distribution['ViewerCertificate']['CertificateSource']}"
                )
                if distribution["ViewerCertificate"]["CertificateSource"] ==
 "acm":
                    print(
                        f"Certificate: {distribution['ViewerCertificate']
['Certificate']}"
                    )
                print("")
        else:
            print("No CloudFront distributions detected.")
```

- Pour plus de détails sur l'API, consultez ListDistributionsle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`UpdateDistribution`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`UpdateDistribution`.

CLI

AWS CLI

Pour mettre à jour l'objet racine par défaut d'une CloudFront distribution

L'exemple suivant met à jour l'objet racine par défaut `index.html` pour la CloudFront distribution avec l'ID `EDFDVBD6EXAMPLE` :

```
aws cloudfront update-distribution --id EDFDVBD6EXAMPLE \
    --default-root-object index.html
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:55:39.870Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "6b10378d-49be-4c4b-a642-419ccaf8f3b5",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "example-website",
                        "DomainName": "www.example.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
```

```
                    "CustomOriginConfig": {
                        "HTTPPort": 80,
                        "HTTPSPort": 443,
                        "OriginProtocolPolicy": "match-viewer",
                        "OriginSslProtocols": {
                            "Quantity": 2,
                            "Items": [
                                "SSLv3",
                                "TLSv1"
                            ]
                        },
                        "OriginReadTimeout": 30,
                        "OriginKeepaliveTimeout": 5
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "example-website",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 1,
                    "Items": [
                        "*"
                    ]
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
```

```
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
```

```
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http1.1",
            "IsIPV6Enabled": true
        }
    }
}
```

Pour mettre à jour une CloudFront distribution

L'exemple suivant désactive la CloudFront distribution avec l'ID `EMLARXS9EXAMPLE` en fournissant la configuration de distribution dans un fichier JSON nommé`dist-config-disable.json`. Pour mettre à jour une distribution, vous devez utiliser l'`--if-match`option permettant de fournir les informations de la distribution`ETag`. Pour obtenir le`ETag`, utilisez la commande get-distribution orget-distribution-config .

Après avoir utilisé l'exemple suivant pour désactiver une distribution, vous pouvez utiliser la commande delete-distribution pour la supprimer.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Le fichier `dist-config-disable.json` est un document JSON dans le dossier actuel qui contient les éléments suivants. Notez que le `Enabled` champ est défini sur `false` :

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
                "DomainName": "awsexamplebucket.s3.amazonaws.com",
```

```
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
```

```
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": false,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Sortie :

```
{
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:32:35.553Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-1574382155-496510",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id":
 "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId":
 "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
```

```
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
```

```
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": false,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Pour plus de détails sur l'API, voir UpdateDistributionla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionRequest;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.DistributionConfig;
import
 software.amazon.awssdk.services.cloudfront.model.UpdateDistributionRequest;
import software.amazon.awssdk.services.cloudfront.model.CloudFrontException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ModifyDistribution {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <id>\s

                Where:
                    id - the id value of the distribution.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String id = args[0];
        CloudFrontClient cloudFrontClient = CloudFrontClient.builder()
                .region(Region.AWS_GLOBAL)
                .build();

        modDistribution(cloudFrontClient, id);
        cloudFrontClient.close();
    }
```

```
   public static void modDistribution(CloudFrontClient cloudFrontClient, String
idVal) {
       try {
           // Get the Distribution to modify.
           GetDistributionRequest disRequest = GetDistributionRequest.builder()
                   .id(idVal)
                   .build();

           GetDistributionResponse response =
cloudFrontClient.getDistribution(disRequest);
           Distribution disObject = response.distribution();
           DistributionConfig config = disObject.distributionConfig();

           // Create a new DistributionConfig object and add new values to
comment and
           // aliases
           DistributionConfig config1 = DistributionConfig.builder()
                   .aliases(config.aliases()) // You can pass in new values here
                   .comment("New Comment")
                   .cacheBehaviors(config.cacheBehaviors())
                   .priceClass(config.priceClass())
                   .defaultCacheBehavior(config.defaultCacheBehavior())
                   .enabled(config.enabled())
                   .callerReference(config.callerReference())
                   .logging(config.logging())
                   .originGroups(config.originGroups())
                   .origins(config.origins())
                   .restrictions(config.restrictions())
                   .defaultRootObject(config.defaultRootObject())
                   .webACLId(config.webACLId())
                   .httpVersion(config.httpVersion())
                   .viewerCertificate(config.viewerCertificate())
                   .customErrorResponses(config.customErrorResponses())
                   .build();

           UpdateDistributionRequest updateDistributionRequest =
UpdateDistributionRequest.builder()
                   .distributionConfig(config1)
                   .id(disObject.id())
                   .ifMatch(response.eTag())
                   .build();

           cloudFrontClient.updateDistribution(updateDistributionRequest);
```

```
        } catch (CloudFrontException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, voir UpdateDistributionla section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""

    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client


    def update_distribution(self):
        distribution_id = input(
            "This script updates the comment for a CloudFront distribution.\n"
            "Enter a CloudFront distribution ID: "
        )

        distribution_config_response =
 self.cloudfront_client.get_distribution_config(
            Id=distribution_id
```

```
        )
        distribution_config = distribution_config_response["DistributionConfig"]
        distribution_etag = distribution_config_response["ETag"]

        distribution_config["Comment"] = input(
            f"\nThe current comment for distribution {distribution_id} is "
            f"'{distribution_config['Comment']}'.\n"
            f"Enter a new comment: "
        )
        self.cloudfront_client.update_distribution(
            DistributionConfig=distribution_config,
            Id=distribution_id,
            IfMatch=distribution_etag,
        )
        print("Done!")
```

- Pour plus de détails sur l'API, consultez UpdateDistributionle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Scénarios d' CloudFront utilisation des AWS SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants CloudFront avec AWS les SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions CloudFront. Chaque scénario inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter le code.

Exemples

- Supprimer les ressources CloudFront de signature à l'aide du AWS SDK
- Créez des URL signées et des cookies à l'aide d'un SDK AWS

Supprimer les ressources CloudFront de signature à l'aide du AWS SDK

L'exemple de code suivant montre comment supprimer des ressources utilisées pour accéder à du contenu restreint dans un compartiment Amazon Simple Storage Service (Amazon S3).

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.DeleteKeyGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.DeleteOriginAccessControlResponse;
import software.amazon.awssdk.services.cloudfront.model.DeletePublicKeyResponse;
import software.amazon.awssdk.services.cloudfront.model.GetKeyGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.GetOriginAccessControlResponse;
import software.amazon.awssdk.services.cloudfront.model.GetPublicKeyResponse;

public class DeleteSigningResources {
    private static final Logger logger =
 LoggerFactory.getLogger(DeleteSigningResources.class);

    public static void deleteOriginAccessControl(final CloudFrontClient
 cloudFrontClient,
            final String originAccessControlId) {
        GetOriginAccessControlResponse getResponse = cloudFrontClient
                .getOriginAccessControl(b -> b.id(originAccessControlId));
        DeleteOriginAccessControlResponse deleteResponse =
 cloudFrontClient.deleteOriginAccessControl(builder -> builder
                .id(originAccessControlId)
                .ifMatch(getResponse.eTag()));
        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
```

```
            logger.info("Successfully deleted Origin Access Control [{}]",
 originAccessControlId);
        }
    }

    public static void deleteKeyGroup(final CloudFrontClient cloudFrontClient,
 final String keyGroupId) {

        GetKeyGroupResponse getResponse = cloudFrontClient.getKeyGroup(b ->
 b.id(keyGroupId));
        DeleteKeyGroupResponse deleteResponse =
 cloudFrontClient.deleteKeyGroup(builder -> builder
                .id(keyGroupId)
                .ifMatch(getResponse.eTag()));
        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
            logger.info("Successfully deleted Key Group [{}]", keyGroupId);
        }
    }

    public static void deletePublicKey(final CloudFrontClient cloudFrontClient,
 final String publicKeyId) {
        GetPublicKeyResponse getResponse = cloudFrontClient.getPublicKey(b ->
 b.id(publicKeyId));

        DeletePublicKeyResponse deleteResponse =
 cloudFrontClient.deletePublicKey(builder -> builder
                .id(publicKeyId)
                .ifMatch(getResponse.eTag()));

        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
            logger.info("Successfully deleted Public Key [{}]", publicKeyId);
        }
    }
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK for Java 2.x .
  - DeleteKeyGroup
  - DeleteOriginAccessControl
  - DeletePublicKey

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Créez des URL signées et des cookies à l'aide d'un SDK AWS

L'exemple de code suivant montre comment créer des URL signées et des cookies qui permettent d'accéder à des ressources restreintes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Utilisez la CannedSignerRequestclasse pour signer des URL ou des cookies avec une politique prédéfinie.

```
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;

public class CreateCannedPolicyRequest {

    public static CannedSignerRequest createRequestForCannedPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expirationDate = Instant.now().plus(7, ChronoUnit.DAYS);
```

```
        Path path = Paths.get(privateKeyFullPath);

        return CannedSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expirationDate)
                .build();
    }
}
```

Utilisez la CustomSignerRequestclasse pour signer des URL ou des cookies avec une politique personnalisée. Les méthodes `activeDate` et `ipRange` sont facultatives.

```
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;

public class CreateCustomPolicyRequest {

    public static CustomSignerRequest createRequestForCustomPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expireDate = Instant.now().plus(7, ChronoUnit.DAYS);
        // URL will be accessible tomorrow using the signed URL.
        Instant activeDate = Instant.now().plus(1, ChronoUnit.DAYS);
        Path path = Paths.get(privateKeyFullPath);

        return CustomSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                .privateKey(path)
                .keyPairId(publicKeyId)
```

```
                .expirationDate(expireDate)
                .activeDate(activeDate) // Optional.
                // .ipRange("192.168.0.1/24") // Optional.
                .build();
    }
}
```

L'exemple suivant illustre l'utilisation de la CloudFrontUtilitiesclasse pour produire des cookies et des URL signés. Consultez cet exemple de code sur GitHub.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontUtilities;
import software.amazon.awssdk.services.cloudfront.cookie.CookiesForCannedPolicy;
import software.amazon.awssdk.services.cloudfront.cookie.CookiesForCustomPolicy;
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;
import software.amazon.awssdk.services.cloudfront.url.SignedUrl;

public class SigningUtilities {
    private static final Logger logger =
 LoggerFactory.getLogger(SigningUtilities.class);
    private static final CloudFrontUtilities cloudFrontUtilities =
 CloudFrontUtilities.create();

    public static SignedUrl signUrlForCannedPolicy(CannedSignerRequest
 cannedSignerRequest) {
        SignedUrl signedUrl =
 cloudFrontUtilities.getSignedUrlWithCannedPolicy(cannedSignerRequest);
        logger.info("Signed URL: [{}]", signedUrl.url());
        return signedUrl;
    }

    public static SignedUrl signUrlForCustomPolicy(CustomSignerRequest
 customSignerRequest) {
        SignedUrl signedUrl =
 cloudFrontUtilities.getSignedUrlWithCustomPolicy(customSignerRequest);
        logger.info("Signed URL: [{}]", signedUrl.url());
        return signedUrl;
    }
```

```
    public static CookiesForCannedPolicy
 getCookiesForCannedPolicy(CannedSignerRequest cannedSignerRequest) {
        CookiesForCannedPolicy cookiesForCannedPolicy = cloudFrontUtilities
                .getCookiesForCannedPolicy(cannedSignerRequest);
        logger.info("Cookie EXPIRES header [{}]",
 cookiesForCannedPolicy.expiresHeaderValue());
        logger.info("Cookie KEYPAIR header [{}]",
 cookiesForCannedPolicy.keyPairIdHeaderValue());
        logger.info("Cookie SIGNATURE header [{}]",
 cookiesForCannedPolicy.signatureHeaderValue());
        return cookiesForCannedPolicy;
    }

    public static CookiesForCustomPolicy
 getCookiesForCustomPolicy(CustomSignerRequest customSignerRequest) {
        CookiesForCustomPolicy cookiesForCustomPolicy = cloudFrontUtilities
                .getCookiesForCustomPolicy(customSignerRequest);
        logger.info("Cookie POLICY header [{}]",
 cookiesForCustomPolicy.policyHeaderValue());
        logger.info("Cookie KEYPAIR header [{}]",
 cookiesForCustomPolicy.keyPairIdHeaderValue());
        logger.info("Cookie SIGNATURE header [{}]",
 cookiesForCustomPolicy.signatureHeaderValue());
        return cookiesForCustomPolicy;
    }
}
```

- Pour plus de détails sur l'API, voir CloudFrontUtilitiesla section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à CloudFront la documentation. Pour recevoir des notifications sur les mises à jour, vous pouvez vous abonner au flux RSS.

Modification	Description	Date
Ajout de nouvelles politiques de cache géré	Ajout de nouvelles politique s de cache géré `UseOrigin CacheControlHeaders` et`UseOriginCacheCont rolHeaders-QuerySt rings` .	24 mai 2024
Support de contrôle d'accès à l'origine ajouté	Vous pouvez désormais créer un contrôle d'accès à l'origine (OAC) pour la AWS Elemental MediaPackage V2 et une URL de AWS Lambda fonction.	11 avril 2024
Champs de journal en temps réel pour CMCD	Ajout de 18 champs de données client multimédia communes (CMCD) pour la journalisation en temps réel.	9 avril 2024
Commencer avec une CloudFront distribution de base	Tutoriel mis à jour pour une distribution de base utilisant une origine Amazon S3 avec contrôle d'accès à l'origine (OAC).	18 mars 2024
Exemples de code pour CloudFront l'utilisation des AWS SDK	Ajout d'exemples de code qui montrent comment utiliser CloudFront un kit de développement AWS logiciel (SDK). Les exemples sont divisés en extraits de code	16 février 2024

	qui vous montrent comment appeler des fonctions de service individuelles et en exemples qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.	
AWS mise à jour des politiques gérée	Les politiques IAM `CloudFrontReadOnlyAccess` et `CloudFrontFullAccess` prennent désormais en charge les opérations `KeyValueStore` .	19 décembre 2023
JavaScript environnement d'exécution 2.0	Ajout de fonctionnalités JavaScript d'exécution 2.0 pour CloudFront Functions.	21 novembre 2023
CloudFront KeyValueStore	Amazon prend CloudFront désormais en charge CloudFront KeyValueStore. Cette fonctionnalité est une banque de données de valeurs clés sécurisée, globale et à faible latence qui permet un accès en lecture depuis CloudFront Functions, permettant ainsi une logique personnalisable avancée aux emplacements CloudFront périphériques.	21 novembre 2023

Lambda@Edge prend en charge la version d'environnement d'exécution la plus récente	Lambda@Edge prend désormais en charge les fonctions Lambda avec l'environnement d'exécution Node.js 20.	15 novembre 2023
Tableau de bord de sécurité	CloudFront crée un tableau de bord de sécurité lorsque vous créez une distribution. Activez AWS WAF, gérez les restrictions géographiques et visualisez des données de haut niveau pour les demandes, les robots et les journaux.	8 novembre 2023
Tri des chaînes de requête dans les fonctions	CloudFront prend désormais en charge le tri des chaînes de requête à l'aide de CloudFront Functions.	3 octobre 2023
AWS WAF recommandations en matière de sécurité	Amazon affiche CloudFront désormais les recommandations AWS WAF de sécurité sur la CloudFront console.	26 septembre 2023
Prise en charge de la diffusion de contenu de cache obsolète (expiré)	CloudFront prend en charge `Stale-While-Revalidate` les directives de contrôle du `Stale-If-Error` cache et.	15 mai 2023
Activez AWS WAF les protections en un seul clic	Une méthode simplifiée pour ajouter des protections AWS WAF de sécurité aux CloudFront distributions.	10 mai 2023

Activer les listes ACL pour les nouveaux compartiments S3 utilisés pour les journaux standard	Ajout d'une note et de liens pour traiter le paramètre de liste ACL par défaut pour les nouveaux compartiments S3.	11 avril 2023
Création d'une origine à l'aide d'Amazon S3 Object Lambda	Vous pouvez utiliser un alias de point d'accès Amazon S3 Object Lambda comme origine pour votre distribution.	31 mars 2023
Personnalisez le statut et le corps du HTTP à l'aide de CloudFront Functions	Vous pouvez utiliser CloudFront Functions pour mettre à jour le code d'état de la réponse du lecteur et remplacer ou supprimer le corps de la réponse.	29 mars 2023
Ajout d'options de caractères génériques pour les en-têtes CORS pour les ports	Vous pouvez désormais inclure des configurations de caractères génériques pour les ports dans les en-têtes de contrôle d'accès CORS.	20 mars 2023
Ajout d'un nouveau lien pour le guide de AWS Security Hub l'utilisateur	Langue mise à jour et ajout d'un lien vers les CloudFront contrôles Amazon réorganis és dans le guide de l'AWS Security Hub utilisateur.	9 mars 2023

CloudFront prend désormais en charge les listes de blocage (« toutes sauf ») dans les politiques de demande d'origine	Utilisez des listes de blocage dans les politiques de demande d'origine pour inclure toutes les chaînes de requête, les en-têtes HTTP ou les cookies, à l'exception de ceux spécifiés, dans les demandes CloudFront envoyées à l'origine.	22 février 2023
CloudFront ajoute une nouvelle politique de demande d'origine gérée pour transférer tous les en-têtes du visualiseur à l'exception de l'en-tête Host	CloudFrontLa nouvelle politique de gestion des demandes d'origine d'Use consiste à inclure tous les en-têtes de la demande du lecteur, à l'exception de l'`Host`en-tête, dans les demandes CloudFront envoyées à l'origine.	22 février 2023
Mise à jour des restrictions sur Lambda@Edge	Lambda@Edge prend en charge les configurations de gestion de l'environnement d'exécution Lambda définies sur Auto.	16 février 2023
Mise à jour des directives IAM pour CloudFront	Mise à jour du guide s’aligner sur les bonnes pratiques IAM. Pour plus d’informations, consultez Bonnes pratiques de sécurité dans IAM.	15 février 2023
Renforcement de la sécurité avec contrôle d’accès à l’origine	Vous pouvez désormais sécuriser les MediaStore origines en autorisant l'accès uniquement aux CloudFront distributions désignées.	9 février 2023

Nouveaux en-têtes pour déterminer la structure de l'en-tête d'un utilisateur	Vous pouvez désormais ajouter un ordre d'en-tête et un nombre d'en-têtes pour identifier l'utilisateur en fonction des en-têtes qu'il envoie.	13 janvier 2023
Lambda@Edge prend en charge la version d'environnement d'exécution la plus récente	Lambda@Edge prend désormais en charge les fonctions Lambda avec l'environnement d'exécution Node.js 18.	12 janvier 2023
Suppression des en-têtes de réponse à l'aide d'une politique d'en-têtes de réponse	Vous pouvez désormais utiliser une politique d'en-têtes de CloudFront réponse pour supprimer de l'origine les en-têtes CloudFront reçus dans la réponse. Les en-têtes spécifiés ne sont pas inclus dans la réponse envoyée CloudFront aux spectateurs.	3 janvier 2023
Déploiement continu pour tester en toute sécurité les changements de configuration	Vous pouvez désormais déployer les changements apportés à la configuration de votre CDN en effectuant des tests sur un sous-ensemble du trafic de production.	18 novembre 2022
Publication de l'en-tête `CloudFront-Viewer-JA3-Fingerprint`	Vous pouvez désormais utiliser l'empreinte JA3 pour déterminer si la demande provient d'un client connu.	16 novembre 2022

Ajout d'options génériques pour les en-têtes CORS	Vous pouvez désormais utiliser différentes configurations de caractères génériques dans certains en-têtes de contrôle d'accès CORS.	11 novembre 2022
Mesures supplémentaires pour les CloudFront distributions	Support pour `MonitoringSubscription` l'CloudFront API et AWS CloudFormation.	3 octobre 2022
Renforcement de la sécurité avec contrôle d’accès à l’origine	Vous pouvez désormais sécuriser les origines d'Amazon S3 en autorisant l'accès uniquement aux CloudFront distributions désignées.	24 août 2022
Support HTTP/3 pour les distributions CloudFront	Vous pouvez désormais choisir HTTP/3 pour votre CloudFront distribution.	15 août 2022
Ajouter les détails de la poignée de main à l'en-tête CloudFront -Viewer-TLS	Vous pouvez désormais visualiser les informations relatives à la liaison SSL/TLS utilisée.	27 juin 2022
Nouvelle métrique dans l’en-tête Server-Timing	Ajout de la nouvelle métrique `cdn-downstream-fbl` aux en-têtes `Server-Timing` .	13 juin 2022

Nouvel en-tête pour obtenir des informations sur la version de TLS et le chiffrement TLS	Vous pouvez désormais utiliser l'`CloudFront-Viewer-TLS` en-tête pour obtenir des informations sur la version de TLS (ou SSL) et le chiffrement utilisé pour la connexion entre le lecteur et. CloudFront	23 mai 2022
Nouvelle FunctionThrottles métrique pour les CloudFront fonctions	Avec Amazon CloudWatch, vous pouvez désormais contrôler le nombre de fois qu'une CloudFront fonction a été limitée au cours d'une période donnée.	4 mai 2022
CloudFront prend en charge les URL des fonctions Lambda	Si vous créez une application Web sans serveur en utilisant des fonctions Lambda avec des URL de fonctions, vous pouvez désormais en CloudFront ajouter pour bénéficier de nombreux avantages.	6 avril 2022
En-tête Server-Timing dans les réponses HTTP	Vous pouvez désormais activer l'`Server-Timing` en-tête dans les réponses HTTP envoyées depuis CloudFront pour afficher les métriques qui peuvent vous aider à mieux comprendre le comportement et les performances de CloudFront.	30 mars 2022

Utiliser une liste de préfixes AWS gérée pour limiter le trafic entrant	Vous pouvez désormais limiter le trafic HTTP et HTTPS entrant vers vos origines uniquement à partir des adresses IP appartenant aux serveurs orientés vers CloudFront l'origine.	7 février 2022
Nouvelle fonction	CloudFront ajoute la prise en charge des politiques relatives aux en-têtes de réponse, qui vous permetten t de spécifier les en-têtes HTTP à CloudFront ajouter aux réponses HTTP envoyées aux utilisateurs (navigateurs Web ou autres clients). Vous pouvez spécifier les en-têtes souhaités (et leurs valeurs) sans modifier l'origine ni écrire de code. Pour plus d'informa tions, consultez la section Ajout ou suppression d'en-tête s HTTP dans les CloudFront réponses.	2 novembre 2021
Nouvel en-tête `CloudFron t-Viewer-Address` de demande	CloudFront ajoute la prise en charge d'un nouvel en-tête contenant l'adresse IP du lecteur à qui la requête HTTP a été envoyée CloudFront. `CloudFront-Viewer-Address` Pour plus d'informa tions, consultez la section Ajout d'en-têtes de CloudFront demande.	25 octobre 2021

Lambda @Edge prend en charge la nouvelle version d'exécution	Lambda@Edge prend désormais en charge les fonctions Lambda avec l'environnement d'exécution Python 3.9. Pour plus d'informations, consultez Runtimes pris en charge.	22 septembre 2021
AWS mise à jour des politiques gérée	CloudFront a mis à jour la CloudFrontReadOnly Accesspolitique. Pour plus d'informations, voir les CloudFront mises à jour des politiques AWS gérées.	8 septembre 2021
Nouvelle fonction	CloudFront prend désormais en charge les certificats ECDSA pour les connexions HTTPS destinées aux spectateurs. Pour plus d'informations, consultez Protocoles et chiffrements pris en charge entre les lecteurs CloudFront et Exigences relatives à l'utilisation de certificats SSL/TLS avec. CloudFront	14 juillet 2021

Nouvelle fonction	CloudFront prend désormais en charge davantage de moyens de déplacer un nom de domaine alternatif d'une distribution à une autre, sans contact AWS Support. Pour plus d'informations, voir Déplacer un autre nom de domaine vers une autre distribution.	7 juillet 2021
Nouvelle politique de sécurité	CloudFront prend désormais en charge une nouvelle politique de sécurité, TLSv1.2_2021, avec un ensemble plus restreint de chiffrements pris en charge. Pour plus d'informations, voir Protocoles et chiffrements pris en charge entre les utilisateurs et. CloudFront	23 Juin 2021
Nouvelle fonction	Amazon prend CloudFront désormais en charge CloudFront Functions, une fonctionnalité native CloudFront qui vous permet d'écrire des fonctions légères JavaScript pour des personnalisations de CDN à grande échelle et sensibles à la latence. Pour plus d'informations, consultez la section Personnalisation en périphérie à l'aide de CloudFront fonctions.	3 mai 2021

Lambda @Edge prend en charge les nouvelles versions d'exécution	Lambda@Edge prend désormais en charge les fonctions Lambda avec le runtime Node.js 14. Pour plus d'informations, consultez Runtimes pris en charge.	29 avril 2021
Supprimer la documentation pour les distributions RTMP	Amazon CloudFront a déconseillé les distributions du protocole de messageri e en temps réel (RTMP) le 31 décembre 2020. La documentation relative aux distributions RTMP est désormais supprimée du Amazon CloudFront Developer Guide.	10 février 2021
Nouvelle option de tarification	Amazon CloudFront lance le pack d'économies de CloudFront sécurité, un moyen simple d'économiser jusqu'à 30 % sur les CloudFront frais figurant sur votre AWS factu re. Pour plus d'informations, consultez les FAQ sur les offres groupées d'épargne.	5 février 2021

Nouveau tutoriel	L'Amazon CloudFront Developer Guide inclut désormais un didacticiel expliquant comment utiliser Amazon CloudFront pour restreindre l'accès à un Application Load Balancer dans Elastic Load Balancing . Pour plus d'informations, voir Restreindre l'accès aux équilibreurs de charge des applications.	18 décembre 2020
Nouvelle option pour la gestion des clés publiques	CloudFront prend désormais en charge la gestion des clés publiques pour les URL signées et les cookies signés via la CloudFront console et l'API, sans nécessiter l'accès de l'utilisateur Compte AWS root. Pour plus d'informations, voir Spécifier les signataires autorisés à créer des URL signées et des cookies signés.	22 octobre 2020

Nouvelle fonctionnalité — Origin Shield	CloudFront prend désormais en charge CloudFront Origin Shield, une couche supplémentaire de l'infrastructure de mise en CloudFront cache qui permet de minimiser la charge de votre origine, d'améliorer sa disponibilité et de réduire ses coûts d'exploitation. Pour plus d'informations, consultez la section Utilisation CloudFront d'Amazon Origin Shield.	20 octobre 2020
Nouveau format de compression	CloudFront prend désormais en charge la formation de compression Brotli lorsque vous configurez CloudFront pour compresser des objets aux emplacements des CloudFront bords. Vous pouvez également configurer la mise CloudFront en cache des objets Brotli à l'aide d'un en-tête normalisé`Accept-Encoding` . Pour plus d'informations, consultez les sections Service de fichiers compressés et Support de compression.	14 septembre 2020

Nouveau protocole TLS	CloudFront supporte désormais le protocole TLS 1.3 pour les connexions HTTPS entre les utilisateurs et les CloudFront distributions. Le protocole TLS 1.3 est activé par défaut dans toutes les politiques CloudFront de sécurité. Pour plus d'informations, voir Protocoles et chiffrements pris en charge entre les utilisateurs et. CloudFront	3 septembre 2020
Nouveaux journaux en temps réel	CloudFront prend désormais en charge les journaux en temps réel configurables. Avec les journaux en temps réel, vous pouvez obtenir des informations sur les demandes faites à une distribution en temps réel. Vous pouvez utiliser des journaux en temps réel pour surveiller, analyser et prendre des mesures en fonction de la performance de diffusion de contenu. Pour plus d'informations, consultez la section Journaux en temps réel.	31 août 2020

Support de l'API pour des métriques supplémentaires	CloudFront prend désormais en charge l'activation de huit métriques supplémentaires en temps réel avec l' CloudFront API. Pour plus d'informations, consultez la section Activation de mesures supplémentaires.	28 août 2020
Nouveaux en-têtes CloudFront HTTP	CloudFront a ajouté des en-têtes HTTP supplémentaires pour déterminer les informations sur le spectateur, telles que le type d'appareil, l'emplacement géographique, etc. Pour plus d'informations, consultez la section Ajout d'en-têtes de CloudFront demande.	23 juillet 2020
Nouvelle fonction	CloudFront prend désormais en charge les politiques de cache et les politiques de demande d'origine, qui vous permettent de contrôler plus précisément la clé de cache et les demandes d'origine pour vos CloudFront distributions. Pour plus d'informations, consultez les sections Contrôler la clé de cache et Contrôler les demandes d'origine.	22 juillet 2020

Nouvelle politique de sécurité	CloudFront prend désormais en charge une nouvelle politique de sécurité, TLSv1.2_2019, avec un ensemble plus restreint de chiffrements pris en charge. Pour plus d'informations, voir Protocoles et chiffrements pris en charge entre les utilisateurs et. CloudFront	8 juillet 2020
Nouveaux paramètres pour contrôler les délais d'origine et les tentatives	CloudFront a ajouté de nouveaux paramètres qui contrôlent les délais d'expiration et les tentatives d'origine . Pour plus d'informations, consultez la section Contrôle des délais d'origine et des tentatives.	5 juin 2020
Nouvelle documentation pour commencer à CloudFront créer un site Web statique sécurisé	Commencez CloudFront par créer un site Web statique sécurisé à l'aide d'Amazon S3 CloudFront, Lambda @Edge, etc., tous déployés avec. AWS CloudFormation Pour plus d'informations, consultez Démarrer avec un site web statique sécurisé.	2 juin 2020
Lambda @Edge prend en charge les nouvelles versions d'exécution	Lambda@Edge prend désormais en charge les fonctions Lambda avec les runtimes Node.js 12 et Python 3.8. Pour plus d'informations, consultez Runtimes pris en charge.	27 février 2020

Nouvelles mesures en temps réel dans CloudWatch	Amazon CloudFrontnow propose huit statistiques supplémentaires en temps réel sur Amazon CloudWatch. Pour plus d'informations, consultez la section Activation de mesures CloudFront de distribution supplémentaires.	19 décembre 2019
Nouveaux champs dans les journaux d'accès	CloudFront ajoute sept nouveaux champs aux journaux d'accès. Pour plus d'informations, consultez la section Champs de fichier journal standard.	12 décembre 2019
AWS WordPress plugin	Vous pouvez utiliser le AWS WordPress plugin pour offrir aux visiteurs de votre WordPress site Web une expérience de visionnage accélérée en utilisant CloudFront. (Mise à jour : depuis le 30 septembre 2022, le WordPress plugin AWS for est obsolète.)	30 octobre 2019

Politiques d'autorisations IAM basées sur les balises et au niveau des ressources	CloudFront prend désormais en charge deux méthodes supplémentaires pour spécifier les politiques d'autorisation IAM : les autorisations basées sur les balises et les autorisations de politique au niveau des ressources. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux ressources.	8 août 2019
Support du langage de programmation Python	Vous pouvez désormais utiliser le langage de programmation Python pour développer des fonctions dans Lambda@Edge, en plus de Node.js. Pour obtenir des exemples de fonctions qui couvrent divers scénarios, veuillez consulter Exemples de fonctions Lambda@Edge.	1 août 2019
Graphiques de surveillance mis à jour	Mises à jour du contenu pour décrire de nouvelles méthodes de surveillance des fonctions Lambda associées à vos CloudFront distributions directement depuis la CloudFront console afin de suivre et de déboguer plus facilement les erreurs. Pour plus d'informations, consultez la section Surveillance CloudFront.	20 juin 2019

Contenu de sécurité consolidé	Un nouveau chapitre sur la sécurité regroupe les informations relatives aux CloudFront fonctionnalités et à la mise en œuvre de la protection des données, de l'IAM, de la journalisation, de la conformité, etc. Pour de plus amples informations, veuillez consulter Sécurité.	24 mai 2019
La validation du domaine est désormais requise	CloudFront exige désormais que vous utilisiez un certificat SSL pour vérifier que vous êtes autorisé à utiliser un autre nom de domaine avec une distribution. Pour de plus amples informations, veuillez consulter Utilisation de noms de domaines alternatifs et de HTTPS.	9 avril 2019
Nom de fichier PDF mis à jour	Le nouveau nom de fichier pour le Amazon CloudFront Developer Guide est : AmazonCloudFront_DevGuide. Le nom précédent était : cf-dg.	7 janvier 2019

Nouvelles fonctionnalités	CloudFront prend désormais en charge WebSocket un protocole basé sur le protocole TCP qui est utile lorsque vous avez besoin de connexion s de longue durée entre les clients et les serveurs. Vous pouvez également désormais configurer le basculement CloudFront d'origine pour les scénarios nécessitant une haute disponibilité. Pour plus d'informations, consultez les sections Utilisation WebSocket avec les CloudFront distribut ions et Optimisation de la haute disponibilité avec CloudFront Origin Failover.	20 novembre 2018
Nouvelle fonction	CloudFront prend désormais en charge la journalisation détaillée des erreurs pour les requêtes HTTP qui exécutent des fonctions Lambda. Vous pouvez enregistrer les connexions CloudWatch et les utiliser pour résoudre les erreurs HTTP 5xx lorsque votre fonction renvoie une réponse non valide. Pour plus d'informations, consultez la section CloudWatch Métriques et CloudWatch journaux pour les fonctions Lambda.	8 octobre 2018

Nouvelle fonction	Vous pouvez désormais décider que Lambda@Edge expose le corps dans une requête pour des méthodes HTTP accessibles en écriture (POST, PUT, DELETE, etc.) afin que vous puissiez y accéder dans vos fonctions Lambda. Vous pouvez choisir un accès en lecture seule ou vous pouvez préciser que vous remplacerez le corps. Pour de plus amples informations, veuillez consulter Accès au corps de la requête en choisissant l'option Inclure le corps.	14 août 2018
Nouvelle fonction	CloudFront permet désormais de diffuser du contenu compressé à l'aide de brotli ou d'autres algorithmes de compression, en plus ou à la place de gzip. Pour de plus amples informations, veuillez consulter Service de fichiers compressés.	25 juillet 2018
Réorganisation	Le guide du CloudFront développeur Amazon a été réorganisé afin de simplifier la recherche de contenus connexes et d'améliorer la lisibilité et la navigation.	28 juin 2018

Nouvelle fonctionnalité	Lambda@Edge vous permet désormais de personnaliser davantage la diffusion du contenu stocké dans un compartiment Amazon S3, en vous donnant accès à des en-têtes supplémentaires, y compris des en-têtes personnalisés, dans les événements orientés vers l'origine. Pour de plus amples informations, veuillez consulter les exemples suivants illustrant la personnalisation de contenu selon l'emplacement de l'utilisateur et le type d'appareil de l'utilisateur.	20 mars 2018
Nouvelle fonctionnalité	Vous pouvez désormais utiliser Amazon CloudFront pour négocier des connexions HTTPS aux origines à l'aide de l'algorithme de signature numérique Elliptic Curve (ECDSA). ECDSA utilise des clés plus petites donc plus rapides, mais tout aussi sécurisées que l'ancien algorithme RSA. Pour plus d'informations, voir Protocoles et chiffrements SSL/TLS pris en charge pour la communication entre et votre origine CloudFront et À propos des chiffrements RSA et ECDSA.	15 mars 2018

Nouvelle fonctionnalité	Lambda @Edge vous permet de personnaliser les réponses aux erreurs depuis votre origine, en vous permettant d'exécuter des fonctions Lambda en réponse aux erreurs HTTP émises par Amazon CloudFrontreceives depuis votre origine. Pour de plus amples informations, veuillez consulter les exemples suivants illustrant des redirections vers un autre emplacement et la génération d'une réponse avec un code de statut 200 (OK).	21 décembre 2017
Nouvelle fonctionnalité	Une nouvelle CloudFront fonctionnalité, le chiffrement au niveau du champ, vous aide à renforcer encore la sécurité des données sensibles, telles que les numéros de carte de crédit ou les informations personnelles identifiables (PII) telles que les numéros de sécurité sociale. Pour plus d'informations, consultez la section Utilisation du chiffrement au niveau des champs pour protéger les données sensibles.	14 décembre 2017
Historique du document archivé	Les anciens historiques du document a été archivé.	1er décembre 2017

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.