aws

Guida per gli sviluppatori

Amazon CloudFront

Amazon CloudFront: Guida per gli sviluppatori

Table of Contents

Cos'è Amazon CloudFront?

Amazon CloudFront è un servizio Web che accelera la distribuzione di contenuto Web statico e dinamico, come file immagine, .html, .css e .js, agli utenti. CloudFront distribuisce i tuoi contenuti attraverso una rete mondiale di data center chiamati edge location. Quando un utente richiede contenuto che distribuisci tramite Amazon CloudFront, la richiesta viene instradata all'edge location che fornisce la latenza (ritardo) più bassa, affinché la distribuzione venga eseguita con le migliori prestazioni possibili.

- Se il contenuto si trova già nella edge location con la latenza più bassa, Amazon CloudFront lo distribuisce immediatamente.
- Se i contenuti non si trova un tale edge location, Amazon CloudFront li recupera da un'origine definita dall'utente, come un bucket di Amazon S3, un canale MediaPackage o un server HTTP (ad esempio, un server Web) che hai identificato come l'origine della versione definitiva dei contenuti.

Ad esempio, supponiamo tu stia distribuendo un'immagine da un server Web tradizionale, e non mediante CloudFront. Ad esempio, è possibile distribuire un'immagine, sunsetphoto.png, utilizzando l'URL `https://example.com/sunsetphoto.png`.

I tuoi utenti possono facilmente passare a questo URL e visualizzare l'immagine. Probabilmente ignorano che la loro richiesta è stata instradata da una rete all'altra, attraverso un complesso insieme di reti interconnesse che costituiscono Internet, fino a che è stata trovata l'immagine.

CloudFront accelera la distribuzione dei contenuti instradando ogni richiesta utente tramite la rete dorsale AWS alla edge location che può servire meglio i contenuti. Di solito si tratta di un edge server CloudFront che fornisce la distribuzione più veloce per il visualizzatore. L'uso della rete AWS riduce drasticamente il numero di reti attraverso le quali le richieste degli utenti devono transitare e di conseguenza migliora le prestazioni. Gli utenti usufruiscono di una latenza più bassa (il periodo di tempo necessario per caricare il primo byte del file) e velocità di trasferimento dati più elevate.

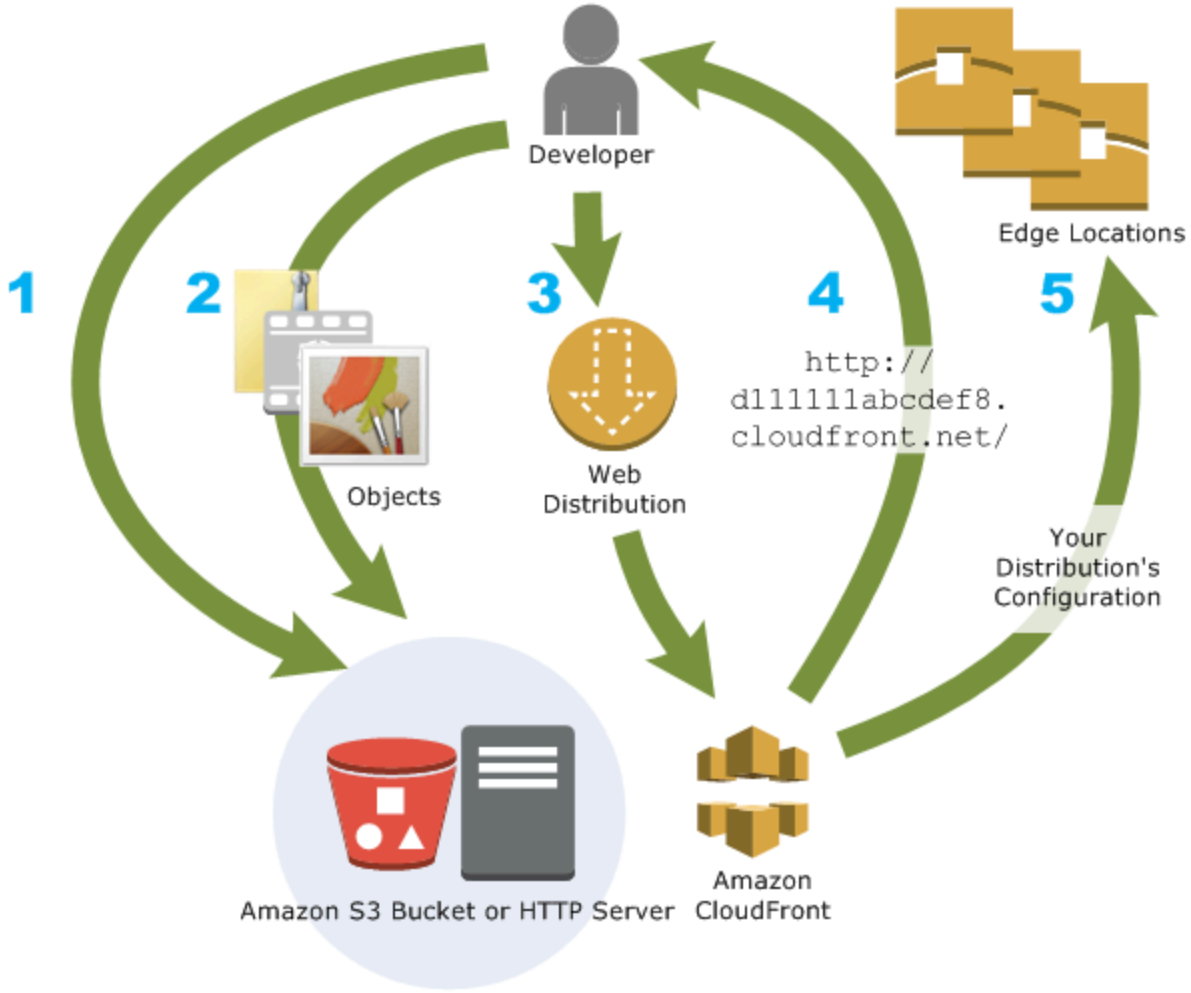
I vantaggi sono evidenti anche a livello di affidabilità e disponibilità, in quanto copie dei tuoi file (note anche come oggetti) si trovano (o sono memorizzate nella cache) in più edge location in tutto il mondo.

Argomenti

- Prezzi
- Modalità di utilizzo di CloudFront
- Come CloudFront distribuisce i contenuti
- Ubicazioni e intervalli di indirizzi IP dei server edge di CloudFront
- Utilizzo di CloudFront con un SDK AWS
- Risorse tecniche di CloudFront

Come configurare CloudFront per la distribuzione dei contenuti

È possibile creare una distribuzione CloudFront per dire a CloudFront da dove prendere i contenuti e fornire i dettagli su come tenere traccia e gestire la distribuzione di contenuti. Quindi CloudFront utilizza computer - edge server - che sono vicini ai visualizzatori per distribuire i contenuti in modo rapido quando un utente desidera visualizzare o utilizzare tali contenuti.



Configurazione di CloudFront per la distribuzione di contenuto

1. È possibile specificare i server di origine, ad esempio un bucket Amazon S3 o il tuo server HTTP, da cui CloudFront ottiene i file che verranno poi distribuiti da edge location CloudFront in tutto il mondo.

   Un server di origine archivia la versione originale e definitiva dei tuoi oggetti. Se distribuisci contenuto via HTTP, il server di origine è un bucket Amazon S3 o un server HTTP, ad esempio un server Web. Il server HTTP può essere eseguito su un'istanza di Amazon Elastic Compute Cloud (Amazon EC2) o su un server che gestisci; questi server sono anche noti come origini personalizzate.
2. Carica i file nei server di origine. I file, noti anche come oggetti, in genere includono pagine Web, immagini e file multimediali, ma possono essere tutti quelli forniti tramite HTTP.

   Se utilizzi un bucket Amazon S3 come server di origine, puoi rendere gli oggetti nel bucket leggibili pubblicamente e quindi consentire agli utenti che conoscono gli URL di CloudFront dei tuoi oggetti di accedervi. Hai anche la possibilità di conservare gli oggetti privati e di controllare chi accede agli stessi. Consulta Offri contenuti privati con cookie firmati URLs e firmati.
3. Crea una distribuzione CloudFront che indica a CloudFront i server di origine da cui ottenere i file quando gli utenti li richiedono tramite il tuo sito Web o applicazione. Specifica inoltre i dettagli, ad esempio se CloudFront deve registrare tutte le richieste e se la distribuzione deve essere attivata non appena viene creata.
4. CloudFront assegna un nome di dominio alla nuova distribuzione che puoi visualizzare nella console di CloudFront oppure lo restituisce nella risposta a una richiesta programmatica, ad esempio una richiesta API. Se lo si desidera, è possibile aggiungere un nome di dominio alternativo da utilizzare.
5. CloudFront invia la configurazione della distribuzione (ma non il contenuto) a tutte le relative edge location o points of presence (POP), ovvero gruppi di server in data center situati in differenti zone geografiche dove CloudFront memorizza nella cache le copie dei file.

Durante lo sviluppo del sito Web o dell'applicazione, utilizzi il nome di dominio che CloudFront fornisce per i tuoi URL. Ad esempio, se CloudFront restituisce `d111111abcdef8.cloudfront.net` come nome di dominio per la distribuzione, l'URL per logo.jpg nel tuo bucket Amazon S3 (o nella directory principale in un server HTTP) sarà `https://d111111abcdef8.cloudfront.net/logo.jpg`.

Oppure, è possibile configurare CloudFront affinché utilizzi il tuo nome di dominio con la distribuzione. In tal caso, l'URL potrebbe essere `https://www.example.com/logo.jpg`.

Eventualmente, puoi configurare il tuo server di origine per aggiungere intestazioni ai file, in modo da indicare il periodo di tempo durante il quale i file rimangono nella cache delle edge location di CloudFront. Per impostazione predefinita, ogni file rimane in una edge location per 24 ore prima della scadenza. La scadenza minima è 0 secondi e non esiste un tempo massimo. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Scelta tra distribuzione standard o distribuzione multi-tenant

CloudFront offre opzioni di distribuzione per singoli siti web o app e per scenari multi-tenant.

Distribuzione standard

Progettata per configurazioni univoche per sito web o applicazione. Scegli questa opzione nei seguenti casi d'uso:

- È necessaria una distribuzione CloudFront autonoma
- Ogni sito o applicazione richiede impostazioni personalizzate

La maggior parte delle persone inizia con una distribuzione standard.

Distribuzione multi-tenant e tenant di distribuzione (Gestore SaaS CloudFront)

Progettati specificamente per fornitori SaaS e scenari multi-tenant. Scegli questa opzione nei seguenti casi d'uso:

- Stai creando una piattaforma SaaS per servire più siti web o applicazioni di clienti
- Devi gestire più distribuzioni simili in modo efficiente
- Desideri un controllo centralizzato sulle configurazioni condivise

Per ulteriori informazioni, consulta Comprendere il funzionamento delle distribuzioni multi-tenant.

Prezzi

CloudFront addebita i costi per i trasferimenti di dati in uscita dalle posizioni edge, insieme alle richieste HTTP o HTTPS. I prezzi variano in base al tipo di utilizzo, all'area geografica e alla selezione di funzionalità.

Il trasferimento dei dati dall'origine a CloudFront è sempre gratuito quando si utilizzano origini AWS come Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing o Gateway Amazon API. Ti verrà addebitato solo il trasferimento dati in uscita da CloudFront al visualizzatore quando utilizzi origini AWS.

Per ulteriori informazioni, consulta Prezzi di CloudFront e Domande frequenti su Bundle fatturazione e risparmio.

Modalità di utilizzo di CloudFront

L'uso di CloudFront permette di raggiungere diversi obiettivi. In questa sezione ne vengono elencati alcuni, insieme a collegamenti a ulteriori informazioni, per darti un'idea delle possibilità.

Argomenti

- Accelerazione della distribuzione di contenuti di siti Web statici
- Esecuzione di video on-demand o in streaming live
- Crittografia di campi specifici durante l'elaborazione di sistema
- Personalizzazione sull'edge
- Esecuzione di contenuti privati utilizzando le personalizzazioni Lambda@Edge

Accelerazione della distribuzione di contenuti di siti Web statici

CloudFront può accelerare la distribuzione di contenuti statici (ad esempio, immagini, fogli di stile, JavaScript e così via) per visualizzatori in tutto il mondo. Utilizzando CloudFront, puoi sfruttare la rete dorsale AWS e i server edge CloudFront per offrire ai visualizzatori un'esperienza rapida, sicura e affidabile quando visitano il tuo sito Web.

Un approccio semplice per archiviare e distribuire contenuti statici è utilizzare un bucket Amazon S3. L'uso di S3 insieme a CloudFront ha diversi vantaggi, inclusa la possibilità di usare il controllo di accesso origine per limitare facilmente l'accesso ai contenuti S3.

Per ulteriori informazioni sull'utilizzo di Amazon S3 insieme a CloudFront, incluso un modello CloudFormation che aiuterà a iniziare rapidamente, consulta Nozioni di base sull'utilizzo di un sito web statico sicuro.

Esecuzione di video on-demand o in streaming live

CloudFront offre diverse opzioni per lo streaming di contenuti multimediali a visualizzatori globali, come file pre-registrati ed eventi live.

- Per streaming di video on-demand (VOD), puoi utilizzare CloudFront per eseguire lo streaming in formati comuni come MPEG DASH, Apple HLS, Microsoft Smooth Streaming e CMAF, verso qualsiasi dispositivo.
- Per la trasmissione di uno streaming live, puoi eseguire la memorizzazione nella cache di frammenti multimediali sull'edge, in modo da poter combinare più richieste per il file manifest che distribuisce i frammenti nell'ordine corretto, riducendo il carico sul server di origine.

Per ulteriori informazioni su come distribuire contenuti in streaming con CloudFront, consulta Video on demand e video in streaming live con CloudFront.

Crittografia di campi specifici durante l'elaborazione di sistema

Quando configuri HTTPS con CloudFront, disponi già di connessioni end-to-end sicure ai server di origine. Quando aggiungi crittografia a livello di campo, puoi proteggere dati specifici durante l'elaborazione del sistema oltre alla sicurezza HTTPS, in modo che i dati possano essere visti solo da alcune applicazioni a livello di origine.

Per configurare la crittografia a livello di campo, aggiungi una chiave pubblica a CloudFront, quindi specifica il set di campi che desideri crittografare con la chiave. Per ulteriori informazioni, consulta Utilizzo della crittografia a livello di campo per la protezione dei dati sensibili.

Personalizzazione sull'edge

L'esecuzione di codice serverless a livello di edge apre diverse possibilità do personalizzazione dei contenuti e dell'esperienza per visualizzatori, a latenza ridotta. Ad esempio, quando il server di origine è inattivo per manutenzione, puoi restituire un messaggio di errore personalizzato per evitare che i visualizzatori ricevano un messaggio di errore HTTP generico. Oppure puoi utilizzare una funzione per facilitare l'autorizzazione degli utenti e controllare l'accesso ai contenuti, prima che CloudFront inoltri una richiesta all'origine.

L'uso di Lambda@Edge con CloudFront offre diversi modi per personalizzare i contenuti distribuiti da CloudFront. Per ulteriori informazioni su Lambda@Edge e su come creare e distribuire funzioni con CloudFront, consulta Personalizzazione al livello di edge con Lambda@Edge. Per visualizzare

una serie di esempi di codice che puoi personalizzare per le tue soluzioni, consulta Esempi di funzioni Lambda@Edge.

Esecuzione di contenuti privati utilizzando le personalizzazioni Lambda@Edge

Grazie a Lambda@Edge è possibile semplificare la configurazione della distribuzione CloudFront per servire contenuti privati dalla propria origine personalizzata, oltre all'utilizzo di URL o cookie firmati.

Per distribuire in modo sicuro contenuti privati utilizzando CloudFront, procedere come segue:

- Richiedere agli utenti (visualizzatori) di accedere ai contenuti utilizzando URL o cookie firmati.
- Limitare l'accesso alla propria origine in modo che sia disponibile solo dai server originari di CloudFront. Questa operazione può essere eseguita in uno dei seguenti modi:
  - Per un'origine Amazon S3, è possibile usare un controllo di accesso origine (OAC).
  - Per un'origine personalizzata, è possibile eseguire le operazioni seguenti:
    - Se l'origine personalizzata è protetta da un gruppo di sicurezza Amazon VPC o AWS Firewall Manager, è possibile usare l'elenco di prefissi gestiti CloudFront per permettere il traffico in entrata verso la propria origine solo dagli indirizzi IP originari di CloudFront.
    - Usare un'intestazione HTTP personalizzata per limitare l'accesso alle sole richieste di CloudFront. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso ai file su origini personalizzate” e the section called “Aggiunta di intestazioni personalizzate alle richieste di origine”. Per un esempio che utilizza un'intestazione personalizzata per limitare l'accesso a un'origine Application Load Balancer, consulta the section called “Limitazione dell’accesso ad Application Load Balancer”.
    - Se l'origine personalizzata richiede una logica di controllo degli accessi personalizzata, è possibile utilizzare Lambda@Edge per implementare tale logica, come descritto in questo post del blog: Serving Private Content Using Amazon CloudFront & Lambda@Edge (Invio di contenuti privati con Amazon CloudFront e Lambda@Edge).

Come CloudFront distribuisce i contenuti

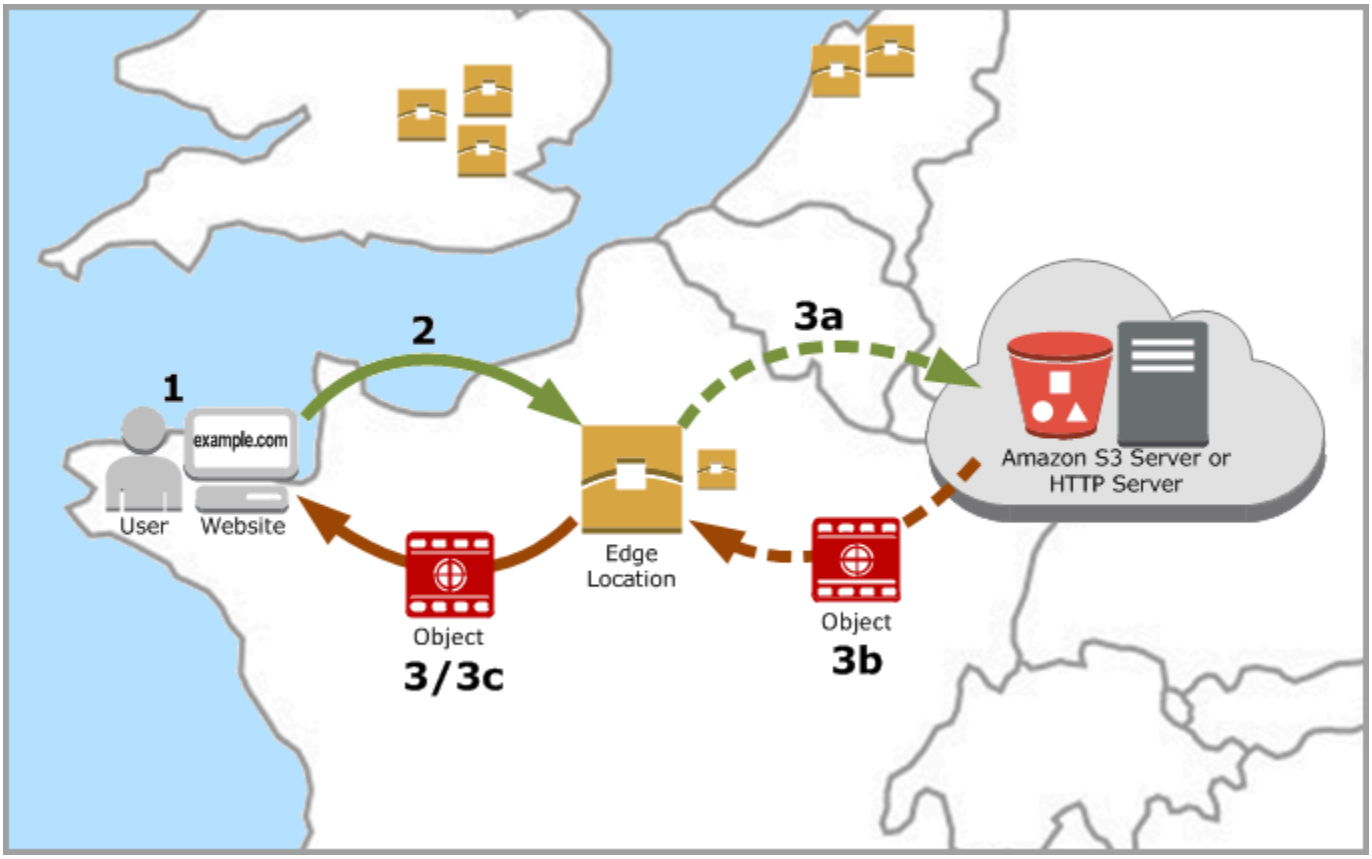
Dopo alcune operazioni di configurazione iniziali, CloudFront funziona insieme al sito Web o all'applicazione e velocizza la distribuzione di contenuti. In questa sezione viene descritto in che modo CloudFront serve i contenuti quando vengono richiesti dai visualizzatori.

Argomenti

Come CloudFront distribuisce i contenuti agli utenti

Dopo la configurazione di CloudFront per la distribuzione dei contenuti, ecco cosa avviene quando gli utenti richiedono gli oggetti:

1. Un utente accede al sito Web o applicazione e richiede un oggetto, ad esempio un file di immagine o un file HTML.
2. DNS instrada la richiesta al POP CloudFront (posizione edge) che può soddisfare al meglio la richiesta, in genere il POP CloudFront più vicino in termini di latenza.
3. CloudFront verifica la cache per l'oggetto richiesto. Se l'oggetto è nella cache, CloudFront lo restituisce all'utente. Se l'oggetto non è nella cache, CloudFront esegue le operazioni seguenti:
   a. CloudFront confronta la richiesta alle specifiche nella distribuzione e inoltra la richiesta al server di origine dell'oggetto corrispondente, ad esempio al bucket Simple Storage Service (Amazon S3) o al server HTTP.
   b. Il server di origine reinvia l'oggetto alla posizione edge.
   c. Subito dopo l'arrivo del primo byte dall'origine, CloudFront inizia a inoltrare l'oggetto all'utente. Inoltre, CloudFront aggiunge l'oggetto alla cache per le richieste successive.



Funzionamento di CloudFront con cache edge regionali

I punti di presenza (noti anche come POP o posizioni edge) di CloudFront fanno in modo che i contenuti popolari possano essere distribuiti rapidamente ai visualizzatori. CloudFront dispone inoltre di cache edge regionali, che rendono disponibile una maggiore quantità di contenuto in ubicazioni più vicine ai tuoi visualizzatori, anche quando il contenuto non è abbastanza popolare per rimanere in un POP, per aiutare a migliorare le prestazioni per il contenuto in questione.

Le cache edge regionali sono utili con tutti i tipi di contenuto, in particolare con il contenuto che tende a diventare meno popolare con il passare del tempo. Ad esempio, contenuto generato dagli utenti, come video, foto o illustrazioni; asset di e-commerce, come foto e video di prodotti; contenuto correlato a notizie ed eventi che potrebbero improvvisamente ritornare d'attualità.

Funzionamento delle cache regionali

Le cache edge regionali sono ubicazioni di CloudFront presenti in tutto il mondo, vicine ai visualizzatori. Si trovano tra il server di origine e i POP, le posizioni edge globali che distribuiscono il contenuto direttamente ai visualizzatori. Man mano che la popolarità degli oggetti diminuisce, singoli POP possono eliminarli per fare spazio a contenuto più popolare. Le cache edge regionali

dispongono di cache di maggiori dimensioni rispetto ai singoli POP, di conseguenza gli oggetti rimangono più a lungo nella cache edge regionale più vicina. In questo modo i contenuti rimarranno più vicini agli utenti finali, riducendo la necessità che CloudFront acceda costantemente al server di origine e migliorando le prestazioni complessive a beneficio degli utenti.

Quando un visualizzatore effettua una richiesta sul tuo sito Web o tramite la tua applicazione, DNS instrada la richiesta al POP che può servire al meglio la richiesta dell'utente. In genere, si tratta della edge location di CloudFront più vicina in termini di latenza. Nel POP, CloudFront verifica la cache per l'oggetto richiesto. Se l'oggetto è nella cache, CloudFront lo restituisce all'utente. Se l'oggetto non è nella cache, i POP in genere accedono alla cache edge regionale più vicina per recuperarlo. Per ulteriori informazioni su quando il POP ignora la cache edge regionale e passa direttamente all'origine, vedere la nota seguente.

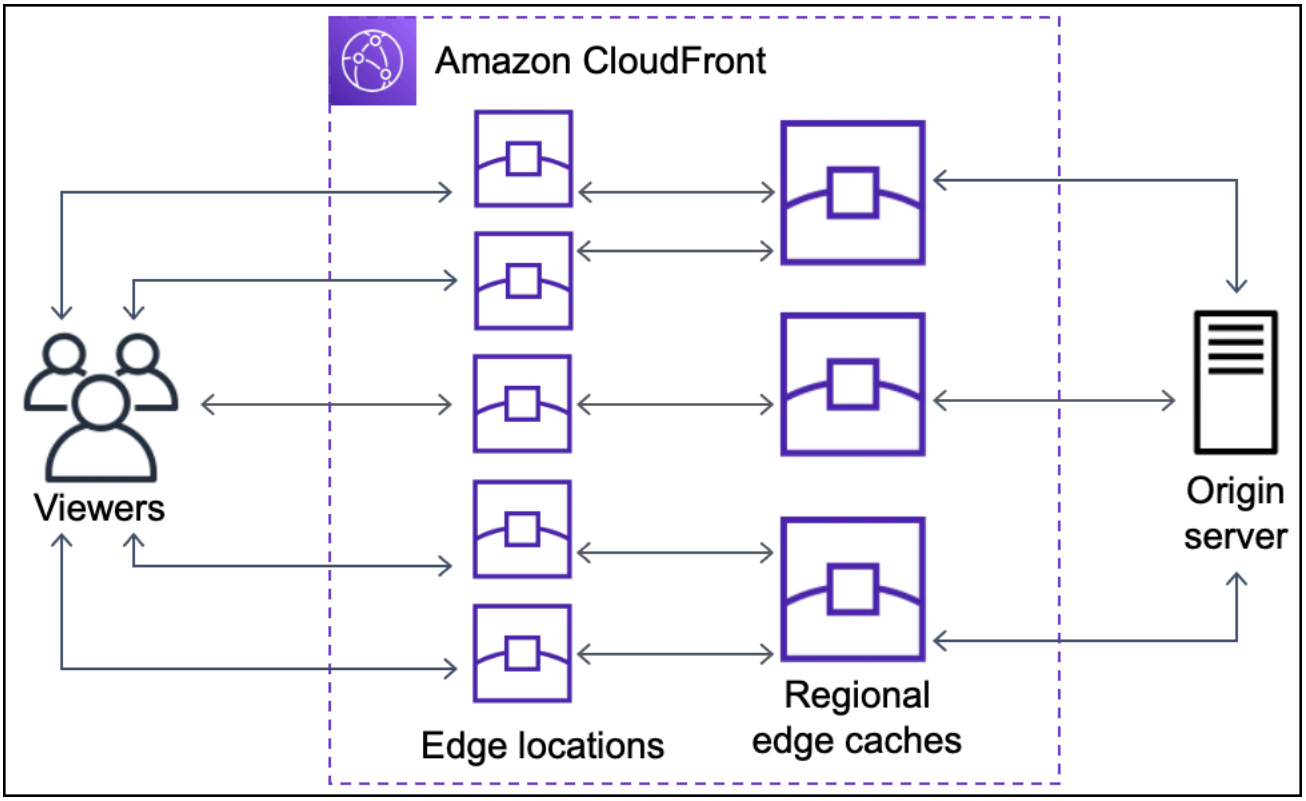
Nella cache edge regionale, CloudFront verifica di nuovo nella cache per l'oggetto richiesto. Se l'oggetto è nella cache, CloudFront lo inoltra al POP che lo ha richiesto. Subito dopo l'arrivo del primo byte dalla posizione della cache edge regionale, CloudFront inizia a inoltrare l'oggetto all'utente. Inoltre, CloudFront aggiunge inoltre l'oggetto alla cache per le richieste successive.

Per gli oggetti non memorizzati nella cache del POP o nella posizione della cache edge regionale, CloudFront confronta la richiesta con le specifiche nelle distribuzioni e inoltra la richiesta dei file al server di origine. Dopo che il server di origine ha inviato gli oggetti alla posizione della cache edge regionale, questi vengono inoltrati al POP e CloudFront li inoltra all'utente. In tal caso, CloudFront aggiunge l'oggetto anche alla cache nella posizione della cache edge regionale oltre che al POP, in modo che sia disponibile alla successiva richiesta di un visualizzatore. In questo modo tutti i POP di una regione condividono una cache locale, evitando l'invio di molteplici richieste ai server di origine. Inoltre, CloudFront mantiene connessioni permanenti con i server di origine, consentendo il recupero più rapido possibile degli oggetti dalle origini.

> **Note**
>
> - A livello di caratteristiche, le cache edge regionali presentano una condizione di parità di funzioni con i POP. Ad esempio, una richiesta di invalidamento della cache consente di rimuovere un oggetto dalle cache dei POP e dalle cache edge regionali prima che scada. La volta successiva che un visualizzatore richiede l'oggetto, CloudFront ritorna all'origine per recuperare la versione più recente dell'oggetto.
> - I metodi proxy HTTP (`PUT`, `POST`, `PATCH`, `OPTIONS` e `DELETE`) vanno direttamente all'origine dai POP senza passare per le cache edge regionali.

- Le richieste dinamiche, come determinate al momento della richiesta, non passano attraverso le cache edge regionali, ma passano direttamente all'origine.
- Quando l'origine è un bucket Simple Storage Service (Amazon S3) e la cache edge regionale ottimale della richiesta è nella stessa Regione AWSdel bucket S3, il POP ignora la cache edge regionale e passa direttamente al bucket S3.

Il diagramma seguente illustra il flusso di richieste e risposte attraverso le posizioni edge di CloudFront e le cache edge regionali.



Ubicazioni e intervalli di indirizzi IP dei server edge di CloudFront

Per un elenco delle posizioni dei server edge CloudFront, consulta la pagina di Amazon CloudFront Global Edge Network.

Amazon Web Services (AWS) pubblica i propri intervalli di indirizzi IP correnti in formato JSON. Per vedere gli intervalli correnti, scarica ip-ranges.json. Per ulteriori informazioni, consulta Intervalli di indirizzi IP di AWS nella Riferimenti generali di Amazon Web Services.

Per trovare intervalli di indirizzi IP associati a server edge di CloudFront cerca la seguente stringa in ip-ranges.json:

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

In alternativa, puoi visualizzare solo gli intervalli IP di CloudFront qui https://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips.

Utilizza l'elenco di prefissi gestiti CloudFront

L'elenco dei prefissi gestiti di CloudFront contiene gli intervalli di indirizzi IP di tutti i server originali distribuiti a livello globale di CloudFront. Se l'origine è ospitata su AWS e protetta da un gruppo di sicurezza di Amazon VPC, puoi utilizzare l'elenco dei prefissi gestiti di CloudFront per consentire il traffico in entrata alla tua origine solo dai server di CloudFront rivolti all'origine, impedendo a qualsiasi traffico non CloudFront di raggiungerla. CloudFront mantiene l'elenco dei prefissi gestiti, quindi è sempre aggiornato con gli indirizzi IP di tutti i server globali di CloudFront rivolti all'origine. Con l'elenco dei prefissi gestiti CloudFront, non è necessario leggere o mantenere autonomamente un elenco di intervalli di indirizzi IP.

Ad esempio, immagina che la tua origine sia un'istanza Amazon EC2 nella regione Europa (Londra) (`eu-west-2`). Se l'istanza si trova in un VPC, è possibile creare una regola del gruppo di sicurezza che consente l'accesso HTTPS in entrata dall'elenco dei prefissi gestiti CloudFront. Ciò consente a tutti i server globali rivolti all'origine di CloudFront di raggiungere l'istanza. Se rimuovi tutte le altre regole in entrata dal gruppo di sicurezza, impedisci a qualsiasi traffico non CloudFront di raggiungere l'istanza.

Gli elenchi di prefissi gestiti da CloudFront sono i seguenti:

- `com.amazonaws.global.cloudfront.origin-facing` (IPv4)
- `com.amazonaws.global.ipv6.cloudfront.origin-facing` (IPv6)

Per maggiori informazioni, consulta Utilizza di un elenco di prefissi gestiti da AWS nella Guida dell'utente di Amazon VPC.

> **Important**
>
> L'elenco dei prefissi gestiti di CloudFront è unico nel modo in cui si applica alle quote Amazon VPC. Per maggiori informazioni, consulta Peso dell'elenco di prefissi gestiti da AWS nella uida dell'utente di Amazon VPC.

Utilizzo di CloudFront con un SDK AWS

AWSI Software Development Kit (SDK) di sono disponibili per molti dei linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK per C++	AWS SDK per C++ Esempi di codice
AWS CLI	AWS CLI Esempi di codice
AWS SDK per Go	AWS SDK per Go Esempi di codice
AWS SDK per Java	AWS SDK per Java Esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript Esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin Esempi di codice
AWS SDK per .NET	AWS SDK per .NET Esempi di codice
AWS SDK per PHP	AWS SDK per PHP Esempi di codice
AWS Strumenti per PowerShell	AWS Strumenti per PowerShell Esempi di codice
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) Esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby Esempi di codice
AWS SDK per Rust	AWS SDK per Rust Esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK per SAP ABAP	AWS SDK per SAP ABAP Esempi di codice
AWS SDK per Swift	AWS SDK per Swift Esempi di codice

> **Esempio di disponibilità**
>
> Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Risorse tecniche di CloudFront

Utilizza le seguenti risorse per ottenere risposte a domande tecniche su CloudFront:

- AWS re:Post - sito dedicato a domande e risposte basate sulla community per sviluppatori utile alla discussione di domande tecniche correlate a CloudFront.
- Supporto Center: questo sito include informazioni sui recenti casi di assistenza e sui risultati di AWS Trusted Advisor e dei controlli dell'integrità. Fornisce inoltre collegamenti a forum di discussione, domande frequenti tecniche, pannello di controllo dell'integrità dei servizi e informazioni sui piani Supporto.
- Supporto AWS Premium: informazioni sul Supporto AWS Premium, un canale di supporto personale a rapida risposta per aiutare nella creazione e l'esecuzione di applicazioni su AWS.
- AWS IQ: ottieni assistenza da professionisti ed esperti certificati AWS.

Inizia con CloudFront

Gli argomenti di questa sezione mostrano come iniziare a distribuire i tuoi contenuti con Amazon CloudFront.

L'Configura il tuo Account AWSargomento descrive i prerequisiti per i seguenti tutorial, come la creazione di un utente Account AWS e la creazione di un utente con accesso amministrativo.

Il tutorial sulla distribuzione di base mostra come configurare il controllo di accesso origine (OAC) per inviare richieste autenticate a un'origine Amazon S3.

Il tutorial sul sito web statico sicuro mostra come creare un sito web statico sicuro per il nome di dominio utilizzando OAC con un'origine Amazon S3. Il tutorial utilizza un modello Amazon CloudFront (CloudFront) per la configurazione e la distribuzione.

Argomenti

Configura il tuo Account AWS

Questo argomento descrive i passaggi preliminari, come la creazione di un Account AWS file, per prepararti a utilizzare Amazon CloudFront.

Argomenti

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

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

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

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

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

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

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

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

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

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

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

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

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

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

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

Scegli come accedere CloudFront

Puoi accedere ad Amazon CloudFront nei seguenti modi:

- Console di gestione AWS— Le procedure riportate in questa guida spiegano come utilizzarlo Console di gestione AWS per eseguire attività.
- AWS SDKs— Se utilizzi un linguaggio di programmazione che AWS fornisce un SDK per, puoi utilizzare un SDK per accedere. CloudFront SDKs semplifica l'autenticazione, si integra facilmente con il tuo ambiente di sviluppo e fornisci l'accesso ai CloudFront comandi. Per ulteriori informazioni, consulta Utilizzo di CloudFront con un SDK AWS.

- CloudFront API: se utilizzi un linguaggio di programmazione per il quale non è disponibile un SDK, consulta Amazon CloudFront API Reference per informazioni sulle azioni API e su come effettuare richieste API.
- AWS CLI— Il AWS Command Line Interface (AWS CLI) è uno strumento unificato per la gestione. Servizi AWS Per informazioni su come installare e configurare la AWS CLI, consulta Installazione o aggiornamento alla versione più recente di AWS CLI nella Guida per l'utente di AWS Command Line Interface .
- Strumenti per Windows PowerShell: se hai esperienza con Windows PowerShell, potresti preferire AWS Tools for Windows PowerShell utilizzarli. Per ulteriori informazioni, consulta Installazione dell' AWS Tools for Windows PowerShell nella Guida per l'utente dell'AWS Strumenti per PowerShell .

Inizia con una distribuzione CloudFront standard

Le procedure in questa sezione mostrano come CloudFront impostare una distribuzione standard che esegua le seguenti operazioni:

- Crea un bucket Amazon S3 da utilizzare come origine della distribuzione.
- Archivia le versioni originali degli oggetti in un bucket Amazon Simple Storage Service (Amazon S3).
- Utilizza il controllo di accesso origine (OAC) per inviare richieste autenticate all'origine Amazon S3. OAC invia richieste CloudFront per impedire agli spettatori di accedere direttamente al bucket S3. Per ulteriori informazioni su OAC, consulta Limitazione dell'accesso a un'origine Amazon S3.
- Utilizza il nome di CloudFront dominio URLs per i tuoi oggetti (ad esempio,). `https://d111111abcdef8.cloudfront.net/index.html`
- Mantiene gli oggetti in posizioni CloudFront periferiche per la durata predefinita di 24 ore (la durata minima è 0 secondi).

La maggior parte di questo viene configurata automaticamente quando crei una CloudFront distribuzione.

Argomenti

- Crea una CloudFront distribuzione che utilizzi un'origine Amazon S3 con OAC
- Accedi ai tuoi contenuti tramite CloudFront
- Eliminazione
- Miglioramento della distribuzione di base

Prerequisiti

Prima di iniziare, assicurati di aver completato le fasi in Configura il tuo Account AWS.

Crea un bucket Amazon S3

Un bucket Amazon S3 è un contenitore per file (oggetti) o cartelle. CloudFront può distribuire quasi tutti i tipi di file per te quando la fonte è un bucket S3. Ad esempio, CloudFront può distribuire testo, immagini e video. Non c'è un massimo per la quantità di dati che è possibile memorizzare in Amazon S3.

Per questo tutorial, viene creato un bucket S3 con i file di esempio `hello world` forniti, che verranno utilizzati per creare una pagina web di base.

Per creare un bucket

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Ti consigliamo di utilizzare il nostro esempio Hello world per questa Guida introduttiva. Scarica la pagina web di Hello World: hello-world-html .zip. Decomprimila e salva la cartella `css` e il file `index` in una posizione conveniente, ad esempio sul desktop su cui stai eseguendo il browser.
3. Seleziona Crea bucket.
4. Inserisci un Nome bucket univoco conforme alle Regole di denominazione dei bucket per uso generale nella Guida per l'utente di Amazon Simple Storage Service.
5. Per Regione, ti consigliamo di scegliere una Regione AWS che sia geograficamente vicina a te. Questo riduce la latenza e i costi.
   - Anche la scelta di una regione diversa funziona. Ad esempio, per soddisfare i requisiti normativi.
6. Lascia tutte le altre impostazioni con i valori predefiniti, quindi seleziona Crea bucket.

Caricamento dei contenuti nel bucket

Dopo aver creato il bucket Amazon S3, carica il contenuto del file `hello world` decompresso. Hai scaricato e decompresso questo file in Crea un bucket Amazon S3.

Per caricare i contenuti su Amazon S3

1. Nella sezione Bucket per uso generico, scegli il nome del nuovo bucket.
2. Scegli Carica.
3. Nella pagina Carica, trascina la cartella `css` e il file `index` nell'area di rilascio.
4. Lascia tutte le altre impostazioni con i valori predefiniti, quindi seleziona Carica.

Crea una CloudFront distribuzione che utilizzi un'origine Amazon S3 con OAC

In questo tutorial, creerai una CloudFront distribuzione che utilizza un'origine Amazon S3 con controllo dell'accesso all'origine (OAC). OAC consente di inviare in modo sicuro richieste autenticate all'origine Amazon S3. Per ulteriori informazioni su OAC, consulta Limitazione dell'accesso a un'origine Amazon S3.

Per creare una CloudFront distribuzione con un'origine Amazon S3 che utilizza OAC

1. Apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Scegli Create Distribution (Crea distribuzione).
3. Immetti un Nome della distribuzione per la distribuzione standard. Il nome verrà visualizzato come valore per la chiave `Name` come un tag. Puoi modificare questo valore in un secondo momento. Puoi aggiungere fino a 50 tag per la distribuzione standard. Per ulteriori informazioni, consulta Tagging di una distribuzione.
4. Scegli Singolo sito web o app, Avanti.
5. Scegli Next (Successivo).
6. Per la pagina Tipo di origine, seleziona Amazon S3.
7. Per Origine S3, scegli Sfoglia S3 e seleziona il bucket S3 creato per questo tutorial.
8. Per Impostazioni, scegli Usa le impostazioni di origine consigliate. CloudFront utilizzerà le impostazioni predefinite di cache e origine consigliate per l'origine Amazon S3, inclusa la

configurazione di Origin Access Control (OAC). Per ulteriori informazioni sulle impostazioni consigliate, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

9. Scegli Next (Successivo).
10. Nella pagina Abilita le protezioni di sicurezza, scegli se abilitare AWS WAF le protezioni di sicurezza.
11. Scegli Next (Successivo).
12. Scegli Crea distribuzione. CloudFront aggiorna la policy sui bucket S3 per te.
13. Esamina la sezione Dettagli per la nuova distribuzione. Quando la distribuzione è stata completata, il campo Ultima modifica cambia da Implementazione in corso a una data e un'ora.
14. Registra il nome di dominio CloudFront assegnato alla tua distribuzione. Avrà un aspetto simile al seguente: `d111111abcdef8.cloudfront.net`.

Prima di utilizzare la distribuzione e il bucket S3 di questo tutorial in un ambiente di produzione, assicurati di configurarli per soddisfare le esigenze specifiche. Per informazioni sulla configurazione dell'accesso in un ambiente di produzione, consulta Configurazione dell'accesso sicuro e restrizione dell'accesso ai contenuti.

Accedi ai tuoi contenuti tramite CloudFront

Per accedere ai tuoi contenuti CloudFront, combina il nome di dominio utilizzato per la CloudFront distribuzione con la pagina principale dei tuoi contenuti. Hai registrato il nome del dominio di distribuzione in Crea una CloudFront distribuzione che utilizzi un'origine Amazon S3 con OAC.

- Il nome di dominio di distribuzione potrebbe essere simile al seguente: `d111111abcdef8.cloudfront.net`.
- Il percorso verso la pagina principale di un sito Web è in genere `/index.html`.

Pertanto, l'URL tramite cui accedere ai tuoi contenuti CloudFront potrebbe essere simile al seguente:

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

Se hai seguito i passaggi precedenti e hai utilizzato la pagina web hello world, dovresti vedere una pagina web con la scritta Hello world!.

Quando carichi più contenuti in questo bucket S3, puoi accedervi CloudFront combinando il nome del dominio di CloudFront distribuzione con il percorso dell'oggetto nel bucket S3. Ad esempio, se carichi un nuovo file denominato `new-page.html` nella root del bucket S3, l'URL è simile al seguente:

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

Eliminazione

Se hai creato la distribuzione e il bucket S3 solo a scopo didattico, eliminali in modo da non incorrere in ulteriori costi. Elimina prima la distribuzione. Per ulteriori informazioni, consulta i collegamenti seguenti:

- Eliminazione di una distribuzione
- Eliminazione di un bucket

Miglioramento della distribuzione di base

Questo tutorial introduttivo fornisce un framework minimale per la creazione di una distribuzione. Consigliamo di esplorare i seguenti miglioramenti:

- Puoi utilizzare la funzionalità dei contenuti CloudFront privati per limitare l'accesso ai contenuti nei bucket Amazon S3. Per ulteriori informazioni su come distribuire contenuti privati, consulta Offri contenuti privati con cookie firmati URLs e firmati.
- Puoi configurare la tua CloudFront distribuzione per utilizzare un nome di dominio personalizzato (ad esempio, `www.example.com` anzichéd`111111abcdef8.cloudfront.net`). Per ulteriori informazioni, consulta Usa personalizzato URLs.
- Questo tutorial utilizza un'origine Amazon S3 con controllo di accesso origine (OAC). Tuttavia, non è possibile utilizzare OAC se l'origine è un bucket S3 configurato come endpoint di un sito web. In tal caso, devi configurare il bucket CloudFront come origine personalizzata. Per ulteriori informazioni, consulta Utilizzo di un bucket Amazon S3 configurato come un endpoint del sito web. Per ulteriori informazioni su OAC, consulta Limitazione dell'accesso a un'origine Amazon S3.

Nozioni di base su una distribuzione standard (AWS CLI)

Le procedure in questa sezione mostrano come utilizzare AWS CLI with CloudFront per impostare una configurazione di base che prevede quanto segue:

- Creazione di un bucket Amazon S3 da utilizzare come origine della distribuzione.
- Archiviazione delle versioni originali degli oggetti nel bucket S3.

- Utilizzo del controllo di accesso origine (OAC) per inviare richieste autenticate all'origine Amazon S3. OAC invia richieste CloudFront per impedire agli utenti di accedere direttamente al bucket S3. Per ulteriori informazioni su OAC, consulta Limitazione dell'accesso a un'origine Amazon S3.
- Utilizzo del nome di CloudFront dominio URLs per gli oggetti (ad esempio,). `https://d111111abcdef8.cloudfront.net/index.html`
- Mantenete gli oggetti in posizioni CloudFront periferiche per la durata predefinita di 24 ore (la durata minima è 0 secondi).

La maggior parte delle opzioni è personalizzabile. Per informazioni su come personalizzare le opzioni di distribuzione CloudFront , consulta Creazione di una distribuzione.

Prerequisiti

Prima di iniziare, assicurati di aver completato le fasi in Configura il tuo Account AWS.

Installalo AWS CLI e configuralo con le tue credenziali. Per ulteriori informazioni, consulta Nozioni di base su AWS CLI nella Guida per l'utente di AWS CLI .

Crea un bucket Amazon S3

Un bucket Amazon S3 è un contenitore per file (oggetti) o cartelle. CloudFront può distribuire quasi tutti i tipi di file per te quando la fonte è un bucket S3. Ad esempio, CloudFront può distribuire testo, immagini e video. Non c'è un massimo per la quantità di dati che è possibile memorizzare in Amazon S3.

Per questo tutorial, verrà creato un bucket S3 e caricato un file HTML da utilizzare per creare una pagina web di base.

```
aws s3 mb s3://amzn-s3-demo-bucket/ --region us-east-1
```

*amzn-s3-demo-bucket*Sostituiscilo con un nome di bucket univoco a livello globale. Per questo Regione AWS, ti consigliamo di scegliere una regione geograficamente vicina a te. In questo modo si riducono la latenza e i costi, ma anche la scelta di una Regione diversa funziona. Ad esempio, puoi eseguire questa operazione per soddisfare i requisiti normativi.

Caricamento dei contenuti nel bucket

Per questo tutorial, scarica ed estrai i file di contenuto di esempio per una pagina web di base “Hello World”.

```
# Create a temporary directory
mkdir -p ~/cloudfront-demo

# Download the sample Hello World files
curl -o ~/cloudfront-demo/hello-world-html.zip https://docs.aws.amazon.com/
AmazonCloudFront/latest/DeveloperGuide/samples/hello-world-html.zip

# Extract the zip file
unzip ~/cloudfront-demo/hello-world-html.zip -d ~/cloudfront-demo/hello-world
```

Viene creata una directory con un file `index.html` e una cartella `css`. Carica questi file nel bucket S3.

```
aws s3 cp ~/cloudfront-demo/hello-world/ s3://amzn-s3-demo-bucket/ --recursive
```

Creazione di un controllo di accesso origine (OAC)

Per questo tutorial, verrà creato un controllo di accesso origine (OAC). OAC consente di inviare in modo sicuro richieste autenticate all’origine Amazon S3. Per ulteriori informazioni su OAC, consulta Limitazione dell’accesso a un’origine Amazon S3.

```
aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
s3",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=s3
```

Salva l’ID OAC dall’output come una variabile di ambiente. Sostituisci i valori di esempio con l’ID OAC. Verrà utilizzato nella fase successiva.

```
OAC_ID="E1ABCD2EFGHIJ"
```

Creazione di una distribuzione standard

Crea un file di configurazione della distribuzione denominato `distribution-config.json`. Sostituisci il nome del bucket di esempio con il nome del bucket per i valori `Id`, `DomainName`, e `TargetOriginId`.

```
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-example-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-amzn-s3-demo-bucket",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-amzn-s3-demo-bucket",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for S3 bucket",
    "Enabled": true
}
EOF
```

Crea una distribuzione standard.

```
aws cloudfront create-distribution --distribution-config file://distribution-
config.json
```

Salva l'ID distribuzione e il nome di dominio dell'output come variabili di ambiente. Sostituire i valori di esempio con i propri valori. Verranno utilizzati più avanti in questo tutorial.

```
DISTRIBUTION_ID="EABCD1234XMPL"
DOMAIN_NAME="d111111abcdef8.cloudfront.net"
```

Prima di utilizzare la distribuzione e il bucket S3 di questo tutorial in un ambiente di produzione, assicurati di configurarli per soddisfare le esigenze specifiche. Per informazioni sulla configurazione dell'accesso in un ambiente di produzione, consulta Configurazione dell'accesso sicuro e restrizione dell'accesso ai contenuti.

Aggiornamento della policy di bucket S3

Aggiorna la policy del bucket S3 per consentire l'accesso CloudFront agli oggetti. Sostituisci il nome bucket di esempio con il nome bucket.

```
# Get your AWS account ID
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create the bucket policy
cat > bucket-policy.json << EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::$ACCOUNT_ID:distribution/
$DISTRIBUTION_ID"
```

```
                }
            }
        }
    ]
}
EOF

# Apply the bucket policy
aws s3api put-bucket-policy \
    --bucket amzn-s3-demo-bucket \
    --policy file://bucket-policy.json
```

Conferma dell'implementazione della distribuzione

Dopo aver creato la distribuzione, occorrerà un po' di tempo per completarne l'implementazione. Quando lo stato della distribuzione cambia da `InProgress` a `Deployed`, esegui la fase successiva.

```
aws cloudfront get-distribution --id $DISTRIBUTION_ID --query 'Distribution.Status'
```

In alternativa, puoi utilizzare il comando `wait` per attendere l'implementazione della distribuzione.

```
aws cloudfront wait distribution-deployed --id $DISTRIBUTION_ID
```

Accedi ai tuoi contenuti tramite CloudFront

Per accedere ai tuoi contenuti CloudFront, combina il nome di dominio utilizzato per la CloudFront distribuzione con la pagina principale dei tuoi contenuti. Sostituisci il nome di CloudFront dominio di esempio con il tuo.

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

Se hai seguito i passaggi precedenti e creato il file HTML, dovresti vedere una pagina web con la scritta Hello world!.

Quando carichi più contenuti in questo bucket S3, puoi accedervi CloudFront combinando il nome del dominio di CloudFront distribuzione con il percorso dell'oggetto nel bucket S3. Ad esempio, se carichi un nuovo file denominato `new-page.html` nella root del bucket S3, l'URL è simile al seguente:

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

Eliminazione

Se hai creato la distribuzione e il bucket S3 solo a scopo didattico, eliminali in modo da non incorrere in ulteriori costi. Disabilita ed elimina prima la distribuzione.

Come disabilitare ed eliminare una distribuzione standard (AWS CLI)

1. Innanzitutto, disabilita la distribuzione.

```
# Get the current configuration and ETag
ETAG=$(aws cloudfront get-distribution-config --id $DISTRIBUTION_ID --query 'ETag'
 --output text)

# Create a modified configuration with Enabled=false
aws cloudfront get-distribution-config --id $DISTRIBUTION_ID | \
jq '.DistributionConfig.Enabled = false' > temp_disabled_config.json

# Update the distribution to disable it
aws cloudfront update-distribution \
    --id $DISTRIBUTION_ID \
    --distribution-config file://<(jq '.DistributionConfig'
 temp_disabled_config.json) \
    --if-match $ETAG
```

2. Attendi che la distribuzione venga disabilitata.

```
aws cloudfront wait distribution-deployed --id $DISTRIBUTION_ID
```

3. Elimina la distribuzione.

```
# Get the current ETag
ETAG=$(aws cloudfront get-distribution-config --id $DISTRIBUTION_ID --query 'ETag'
 --output text)

# Delete the distribution
aws cloudfront delete-distribution --id $DISTRIBUTION_ID --if-match $ETAG
```

Come eliminare un bucket S3 (AWS CLI)

- Elimina il bucket S3 e il relativo contenuto. Sostituisci il nome bucket di esempio con quello personalizzato.

```
# Delete the bucket contents
aws s3 rm s3://amzn-s3-demo-bucket --recursive

# Delete the bucket
aws s3 rb s3://amzn-s3-demo-bucket
```

Per pulire i file locali creati per questo tutorial, esegui i seguenti comandi:

```
# Clean up local files
rm -f distribution-config.json bucket-policy.json temp_disabled_config.json
rm -rf ~/cloudfront-demo
```

Facoltativamente, puoi eliminare l'OAC creato per questo tutorial.

```
# Get the OAC ETag
OAC_ETAG=$(aws cloudfront get-origin-access-control --id $OAC_ID --query 'ETag' --
output text)

# Delete the OAC
aws cloudfront delete-origin-access-control --id $OAC_ID --if-match $OAC_ETAG
```

Nozioni di base sull'utilizzo di un sito web statico sicuro

È possibile iniziare con Amazon CloudFront utilizzando la soluzione descritta in questo argomento per creare un sito Web statico protetto per il nome di dominio. Un sito Web statico utilizza solo file statici, come HTML, CSS, JavaScript, immagini e video, e non necessita di server o elaborazione lato server. Con questa soluzione, il tuo sito web ottiene i seguenti vantaggi:

- Utilizza lo storage durevole di Amazon Simple Storage Service (Amazon S3): questa soluzione crea un bucket Amazon S3 per ospitare i contenuti del tuo sito Web statico. Per aggiornare il tuo sito web, basta caricare i nuovi file nel bucket S3.
- Viene velocizzata dalla rete di distribuzione dei contenuti di Amazon CloudFront: questa soluzione crea una distribuzione CloudFront per servire il tuo sito web ai visualizzatori con bassa latenza. La distribuzione è configurata con un controllo di accesso origine (OAC) per assicurarsi che il sito web sia accessibile solo tramite CloudFront, non direttamente da S3.

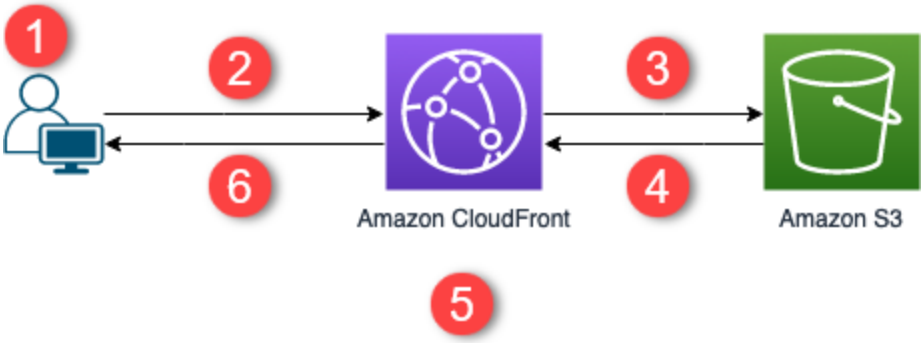
- È protetto da HTTPS e intestazioni di sicurezza: questa soluzione crea un certificato TLS/SSL in AWS Certificate Manager (ACM) e lo collega alla distribuzione CloudFront. Questo certificato consente alla distribuzione di servire il sito Web del dominio in modo sicuro con HTTPS.
- È configurato e distribuito con AWS CloudFormation: questa soluzione utilizza un modello CloudFormation per configurare tutti i componenti, in modo da potersi concentrare maggiormente sul contenuto del sito Web e meno sulla configurazione dei componenti.

Questa soluzione è open source su GitHub. Per visualizzare il codice, inviare una richiesta pull o aprire un problema, andare su https://github.com/aws-samples/amazon-cloudfront-secure-static-site.

Argomenti

Panoramica della soluzione

Il diagramma seguente mostra una panoramica del funzionamento di questa soluzione per siti Web statici:



1. Il visualizzatore richiede il sito web all'indirizzo www.example.com.
2. Se l'oggetto richiesto viene memorizzato nella cache, CloudFront restituisce l'oggetto dalla relativa cache al visualizzatore.
3. Se l'oggetto non si trova nella cache di CloudFront, CloudFront richiede l'oggetto dall'origine (un bucket S3).
4. S3 restituisce l'oggetto a CloudFront.
5. CloudFront memorizza l'oggetto nella cache.

6. Gli oggetti vengono restituiti al visualizzatore. Le richieste successive per l'oggetto che arrivano alla stessa posizione edge CloudFront vengono servite dalla cache CloudFront.

Implementazione della soluzione

Per distribuire questa soluzione per siti Web statici protetti, è possibile scegliere una delle seguenti opzioni:

- Utilizza la console CloudFormation per distribuire la soluzione con contenuto predefinito, quindi caricare il contenuto del sito Web in Amazon S3.
- Clona la soluzione sul tuo computer per aggiungere il contenuto del tuo sito web. Quindi, distribuire la soluzione con AWS Command Line Interface (AWS CLI).

> **Note**
>
> È necessario utilizzare la Regione Stati Uniti orientali (Virginia settentrionale) per implementare il modello CloudFormation.

Argomenti

Prerequisiti

Per utilizzare questa soluzione, è necessario disporre dei seguenti prerequisiti:

- Nome di dominio registrato, ad esempio example.com, che punta a una zona Amazon Route 53 ospitata. La zona ospitata deve trovarsi nello stesso Account AWS in cui si implementa questa soluzione. Se non si dispone di un nome di dominio registrato, è possibile registrarne uno con Route 53. Se si dispone di un nome di dominio registrato ma non è puntato a una zona Route 53 ospitata, configurare Route 53 come servizio DNS.
- AWS Identity and Access Management (IAM) per avviare modelli CloudFormation che creano ruoli IAM e autorizzazioni per creare tutte le risorse AWS nella soluzione. Per ulteriori informazioni,

consulta Controllo dell'accesso con AWS Identity and Access Management nella Guida per l'utente di AWS CloudFormation.

L'utente è responsabile dei costi sostenuti durante l'utilizzo di questa soluzione. Per ulteriori informazioni sui costi, consulta le pagine relative ai prezzi per ciascun Servizio AWS.

Utilizzo della console CloudFormation

Per eseguire la distribuzione tramite la console CloudFormation

1. Avvia questa soluzione nella console CloudFormation. Se necessario, accedi al tuo Account AWS.
2. Viene visualizzata la procedura guidata Crea stack nella console CloudFormation, con campi precompilati che specificano il modello CloudFormation di questa soluzione.

   Nella parte inferiore della pagina scegli Next (Avanti).
3. Nella pagina Specificare i dettagli dello stack immettere i valori per i campi riportati di seguito.

   - Sottodominio: inserire il sottodominio da utilizzare per il tuo sito web. Ad esempio, se il sottodominio è www, il sito Web è disponibile all'indirizzo *www*.example.com. Sostituire example.com con il nome di dominio, come spiegato nel punto seguente.
   - NomeDominio: immettere il nome di dominio, ad esempio *example.com*. Questo dominio deve essere puntato a una zona Route 53 ospitata.
   - HostedZoneId: l'ID di zona ospitata Route 53 del nome di dominio.
   - CreateApex: (facoltativo) crea un alias per l'apex del dominio (example.com) nella configurazione CloudFront.
4. Al termine, scegli Apply (Applica).
5. (Facoltativo) Nella pagina Configura opzioni stack, aggiungere tag e altre opzioni di stack.
6. Al termine, scegli Apply (Applica).
7. Nella pagina Revisione scorrere fino alla fine della pagina, quindi selezionare le due caselle nella sezione Funzionalità. Queste funzionalità consentono a CloudFormation di creare un ruolo IAM che permette l'accesso alle risorse dello stack e assegnare un nome dinamico alle risorse.
8. Scegli Crea stack.
9. Attendi che lo stack termini la creazione. Lo stack crea alcuni stack nidificati e il completamento di questa operazione può richiedere alcuni minuti. Al termine, lo stato viene modificato in CREATE_COMPLETE.

Quando lo stato è CREATE_COMPLETE, andare su https://*www.example.com* per visualizzare il sito Web (sostituire www.example.com con il sottodominio e il nome di dominio specificati al passaggio 3). Dovresti vedere il contenuto predefinito del sito Web:

Per sostituire il contenuto predefinito del sito Web con il proprio

1. Apri la console Amazon S3 su https://console.aws.amazon.com/s3/.
2. Scegli il bucket il cui nome inizia con amazon-cloudfront-secure-static-site-s3bucketroot-.

> **Note**
>
> Assicurati di scegliere il bucket con s3bucketroot nel suo nome, non s3bucketlogs. Il bucket con s3bucketroot nel suo nome contiene il contenuto del sito web. Quello con s3bucketlogs contiene solo file di log.

3. Elimina il contenuto predefinito del sito Web, quindi carica il tuo.

> **Note**
>
> Se hai visualizzato il tuo sito Web con il contenuto predefinito di questa soluzione, è probabile che parte del contenuto predefinito venga memorizzato nella cache in una posizione edge CloudFront. Per assicurarsi che gli spettatori visualizzino il contenuto aggiornato del sito Web, invalidare i file per rimuovere le copie memorizzate nella cache dalle posizioni edge CloudFront. Per ulteriori informazioni, consulta Invalidare i file per rimuovere il contenuto.

Clonazione locale della soluzione

Prerequisiti

Per aggiungere il contenuto del sito Web prima di distribuire questa soluzione, è necessario creare un pacchetto locale degli artefatti della soluzione, che richiede Node.js e npm. Per ulteriori informazioni, consulta https://www.npmjs.com/get-npm.

Per aggiungere il contenuto del sito Web e distribuire la soluzione

1. Clona o scarica la soluzione da https://github.com/aws-samples/amazon-cloudfront-secure-static-site. Dopo averlo clonato o scaricato, aprire un prompt dei comandi o un terminale e passare alla cartella `amazon-cloudfront-secure-static-site`.
2. Eseguire il comando seguente per installare e creare il pacchetto degli artefatti della soluzione:

```
make package-static
```

3. Copiare il contenuto del sito Web nella cartella `www`, sovrascrivendo il contenuto predefinito del sito Web.
4. Eseguire il seguente comando AWS CLI per creare un bucket Amazon S3 e memorizzare gli artefatti della soluzione. Sostituire *amzn-s3-demo-bucket-for-artifacts* con il nome del bucket.

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

5. Eseguire il comando AWS CLI seguente per creare il pacchetto degli artefatti della soluzione come modello CloudFormation. Sostituire *amzn-s3-demo-bucket-for-artifacts* con il nome del bucket creato nel passaggio precedente.

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

6. Eseguire il comando seguente per distribuire la soluzione con CloudFormation, sostituendo i seguenti valori:

   - *your-CloudFormation-stack-name*: sostituire con un nome per lo stack CloudFormation.
   - *example.com*: sostituisci con il nome di dominio. Questo dominio deve essere indirizzato a una zona ospitata Route 53 nello stesso Account AWS.
   - *www*: sostituire con il sottodominio da utilizzare per il tuo sito web. Ad esempio, se il sottodominio è www, il tuo sito web è disponibile all'indirizzo www.example.com.

- *hosted-zone-ID*: sostituire l'ID della zona ospitata Route 53 del nome di dominio.

```
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
```

- (Facoltativo) Per implementare lo stack con un apex di dominio, eseguire invece il comando seguente.

```
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. Attendere che lo stack CloudFormation finisca la creazione. Lo stack crea alcuni stack nidificati e il completamento di questa operazione può richiedere alcuni minuti. Al termine, lo stato viene modificato in CREATE_COMPLETE.

   Quando lo stato cambia in CREATE_COMPLETE, visitare https://www.example.com per visualizzare il sito Web (sostituire www.example.com con il sottodominio e il nome di dominio specificati nel passaggio precedente). Dovresti vedere il contenuto del tuo sito web.

Ricerca dei log di accesso

Questa soluzione abilita i registri di accesso per la distribuzione CloudFront. Per individuare i registri di accesso della distribuzione, completare la procedura seguente.

Per individuare i registri di accesso della distribuzione

1. Apri la console Amazon S3 su https://console.aws.amazon.com/s3/.
2. Scegliere il bucket il cui nome inizia con amazon-cloudfront-secure-static-site-s3bucketlogs-.

> **Note**
>
> Assicurarsi di scegliere il bucket con s3bucketlogs nel suo nome, non s3bucketroot. Il bucket con s3bucketlogs nel suo nome contiene file di registro. Quello con s3bucketroot contiene il contenuto del sito web.

3. La cartella denominata cdn contiene i registri di accesso CloudFront.

CloudFront piani tariffari forfettari

CloudFront i piani tariffari forfettari combinano la rete CloudFront globale di distribuzione dei contenuti (CDN) di Amazon con molteplici Servizi AWS funzionalità in un prezzo mensile senza costi aggiuntivi, indipendentemente dai picchi di traffico o dagli attacchi.

I piani tariffari forfettari includono le seguenti funzionalità a un semplice prezzo mensile:

- CloudFront CDN
- AWS WAF e protezione DDo S
- Gestione e analisi dei bot
- Amazon Route 53 DNS
- Inserimento di Amazon CloudWatch Logs
- Certificato TLS
- Elaborazione perimetrale senza server
- Crediti di storage Amazon S3 ogni mese

I piani sono disponibili nei livelli Free, Pro, Business e Premium per soddisfare le esigenze dell'applicazione. I piani non richiedono un impegno annuale per ottenere le migliori tariffe disponibili. Inizia con il piano gratuito ed esegui l'upgrade per accedere a più funzionalità e quote di utilizzo più ampie.

Argomenti

Vantaggi dei piani CloudFront tariffari forfettari

Il piano CloudFront tariffario offre diversi vantaggi chiave:

- Servizi e prezzi consolidati

  Combina più Servizi AWS funzionalità in un unico piano con un'unica tariffa fissa. Progettato per eliminare l'acquisto separato dei servizi e il calcolo anticipato dei prezzi.

- Nessuna eccedenza

  Non sono previsti costi aggiuntivi indipendentemente dai picchi di traffico o dagli attacchi.

- Chiare le indennità di utilizzo

  Ogni piano include quote di utilizzo pubblicate progettate per prestazioni ottimali a quel livello. Monitora l'utilizzo, ricevi notifiche proattive e aggiorna in base alle esigenze dell'applicazione, senza impegni a lungo termine.

- Proteggiti dagli attacchi DDo S

  CloudFront e AWS WAF assorbe e blocca gli attacchi prima che raggiungano la tua infrastruttura. Riserva l'utilizzo dell'elaborazione, del database e dell'infrastruttura solo per il traffico legittimo. Gli attacchi Blocked DDo S e le richieste bloccate da AWS WAF non contano mai ai fini del limite di utilizzo consentito.

- Riduci i costi complessivi AWS

  Il trasferimento di dati da AWS applicazioni in esecuzione su servizi come Amazon S3, AWS Application Load Balancer (ALB) o Amazon API Gateway continua CloudFront a essere gratuito. Se servi AWS le tue applicazioni tramite Internet CloudFront anziché direttamente su Internet, il tuo piano forfettario copre i costi di trasferimento dei dati tra le tue applicazioni e i tuoi visualizzatori a un semplice prezzo mensile senza il rischio di eccedenze. Un minor numero di richieste che arrivano all'origine riduce anche i costi dei servizi che vengono addebitati in base all'utilizzo.

Funzionalità per livello del piano tariffario

Ogni piano tariffario copre una CloudFront distribuzione con un massimo di un dominio apex (root) che combina funzionalità e servizi essenziali in un unico prezzo mensile. Ogni piano include anche crediti di storage S3 aggiuntivi.

I piani di livello superiore includono tutte le funzionalità dei piani di livello inferiore e funzionalità aggiuntive.

- Gratuito: per principianti, studenti e sviluppatori.
- Pro: avvia e fai crescere siti Web, blog e applicazioni di piccole dimensioni.
- Business: proteggi e accelera le applicazioni aziendali.
- Premium: scalate e proteggete le applicazioni aziendali e mission-critical.

Seleziona un livello di piano che includa le funzionalità e le configurazioni necessarie per le tue applicazioni. Scopri le seguenti funzionalità per piano tariffario.

Caratteristiche del piano tariffario

La tabella seguente mostra le CloudFront funzionalità di Amazon Route 53 CloudWatch, Amazon e Amazon S3 incluse in ogni livello del piano tariffario. AWS WAF DDo

Prestazioni e consegna	Gratuito	Pro	Business	premio
CDN globale	Sì	Sì	Sì	Sì
Utilizza CloudFront le oltre 750 edge location globali come punto di accesso unico, massiccio e distribuito per la tua applicazione web. Accelera le applicazioni statiche, dinamiche e non memorizzabili nella cache.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Memorizzazione nella cache dei contenuti Archivia copie dei tuoi contenuti nelle oltre 750 edge location CloudFront di tutto il mondo, distribuendoli agli utenti dalla posizione più vicina. Riduce i tempi di caricamento, protegge l'applicazione dai picchi di traffico e consente di risparmiare sui costi servendo le richieste ripetute localmente anziché dai server delle applicazioni.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Invalidazioni rapide della cache Rimuovi o aggiorna i contenuti memorizzati nella cache in tutte le edge location in pochi secondi.	Sì 	Sì 	Sì 	Sì 
Routing intelligente Indirizza in modo intelligente gli utenti verso la posizione periferica ottimale utilizzando dati di rete in tempo reale e si connette all' AWS origine tramite la rete AWS privata per prestazioni migliori.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Caching a più livelli Le cache edge regionali si trovano tra le edge location e l'applicazione per archiviare i contenuti più a lungo, ridurre il carico sull'applicazione e garantire una distribuzione rapida.	Sì 	Sì 	Sì 	Sì 
Regole di memorizzazione nella cache predefinite Prende decisioni efficaci sulla memorizzazione nella cache per memorizzare nella cache la maggior parte delle applicazioni Web senza configurazioni personalizzate.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Regole di memorizzazione nella cache personalizzate [Controlla il modo in cui memorizza CloudFront i contenuti nella cache specificando quali valori di richiesta utilizzare, ottimizzando le prestazioni, la personalizzazione e le esigenze di freschezza dell'applicazione utilizzando le politiche di cache.]			Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Routing di origine ad alta velocità Con Origin Shield, le richieste dinamiche vengono instradate dalle edge location all'origine utilizzando CloudFront la rete privata per un percorso ad alte prestazioni verso l'origine.				Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Riduzione del carico di origine Aggiunge un ulteriore livello di caching vicino all'appli cazione web utilizzando Origin Shield. Origin Shield consolida le richieste provenien ti da tutte le edge location, riducendo il carico sull'appl icazione, in particolare durante i picchi di traffico.				Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Failover automatico di origine Indirizza automaticamente il traffico verso un'origine di backup in caso di guasto dell'origine principale, mantenendo un'elevata disponibilità senza interrompere le attività degli utenti.				Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Regole di richiesta di origine predefinite Controlla quali informazioni provenienti dalle richieste dei visualizzatori vengono incluse automaticamente nelle richieste di origine, utilizzando politiche di richiesta di origine AWS gestite ottimizzate per scenari comuni.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Regole di intestazione di risposta predefinite Utilizza politiche AWS gestite di intestazione di risposta per aggiungere o rimuovere intestazioni HTTP nelle risposte ai visualizzatori, preconfigurate per intestazioni di sicurezza comuni, impostazioni CORS e altri casi d'uso standard.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Regole di richiesta di origine personalizzate			Sì	Sì
Crea le tue politiche di richiesta di origine per specificare esattamente quali stringhe di query URL, intestazioni e cookie vengono inoltrati alla tua origine, abilitando analisi personalizzate e gestione delle richieste.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Regole di intestazione di risposta personalizzate			Sì	Sì
Crea le tue policy di intestazione di risposta per controllare esattamente quali intestazioni HTTP vengono CloudFront aggiunte o rimosse nelle risposte ai visualizzatori, ad esempio intestazioni di sicurezza, Content Security Policy (CSP), impostazioni CORS e intestazioni di applicazioni personalizzate.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Numero di comportamenti della cache	5	10	50	100
Configura i comportamenti della cache per controllare la modalità di CloudFront gestione delle richieste per modelli URL specifici, tra cui l'origine che fornisce il contenuto, il modo in cui il contenuto viene memorizzato nella cache e se sono necessari HTTPS o firmati URLs.				
Sicurezza e protezione				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Protezione S sempre attiva DDo DDoProteggiti dagli attacchi S che prendono di mira i tuoi siti Web o le tue applicazioni.	Sì	Sì	Sì	Sì
Protezione DDo S avanzata Identifica e blocca gli attacchi DDo S in pochi secondi utilizzando Anti DDo S AMR. AWS apprende i vostri modelli applicativi unici per distingue re tra attacchi e sovratens ioni naturali provenienti da utenti legittimi.			Sì	Sì

Prestazioni e consegna	Gratuito	Pro	Business	premio
Web Application Firewall (WAF) Proteggiti dalle vulnerabilità delle applicazioni comuni e dalle potenziali minacce in base all'intelligence interna sulle minacce di Amazon. Le richieste vengono bloccate prima di raggiungere i tuoi server.	Sì 	Sì 	Sì 	Sì 
Numero di regole WAF Numero totale di regole di sicurezza che è possibile creare e abilitare nella configurazione WAF, incluse regole personalizzate e regole AWS gestite.	5	25	50	75

Prestazioni e consegna	Gratuito	Pro	Business	premio
Protezioni per WordPress database PHP e SQL Usa regole di sicurezza basate sui casi per proteggere applicazioni e sistemi operativi comuni come PHP WordPress , database SQL, Linux e Windows.		Sì 	Sì 	Sì 
Limitazione della velocità basata su IP Blocca automaticamente gli indirizzi IP che superano un numero configurabile di richieste in un periodo di 5 minuti, proteggendoli dagli attacchi HTTP flood e dai tentativi di Denial of Service (DoS).	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Blocco del traffico geografico Blocca le richieste provenienti da paesi o regioni selezionati.	Sì 	Sì 	Sì 	Sì 
Filtraggio delle minacce basato sugli header Crea regole di sicurezza WAF che filtrano le minacce in base alle intestazioni delle richieste HTTP.		Sì 	Sì 	Sì 
Filtraggio delle minacce basato su Regex Crea regole di sicurezza WAF utilizzando espressioni regolari per abbinare i percorsi URI e gli attributi delle richieste HTTP.			Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
JavaScript sfida			Sì	Sì
Blocca le minacce automatizzate richiedendo ai browser di completare JavaScript le sfide che verificano gli utenti legittimi.				
Gestione e analisi dei bot			Sì	Sì
Rileva e analizza il traffico dei AWS WAF bot con Bot Control per i bot più comuni. Fornisce controlli per bloccare, contestare o consentire i bot non verificati identificando e distinguendo i bot verificati come i motori di ricerca.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Risposta WAF personalizzata Imposta un codice di stato HTTP specifico e una risposta opzionale personalizzata HTML, testo semplice o JSON quando le richieste vengono bloccate da una regola.		Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Inserimento dell'intestazione	Sì	Sì	Sì	Sì
Aggiungi intestazioni HTTP personalizzate alle richieste che superano l'ispezione WAF, consentendo alle applicazioni downstream di elaborare le richieste in modo diverso o di contrassegnarle per l'analisi.				
Richiedi l'ispezione dell'organismo	16 KB	16 KB	64 KB	64 KB
Dimensione massima del contenuto del corpo della richiesta HTTP che può essere ispezionato alla AWS WAF ricerca di minacce e schemi dannosi.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Origini private all'interno di VPC Migliora la sicurezza mantenendo la tua applicazione in una sottorete privata VPC, accessibile solo tramite le tue CloudFront distribuzioni e nascosta dalla rete Internet pubblica, utilizzando origini VPC.			Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Origin Access Control (OAC) Mantieni un bucket S3 privato e consenti l'accesso solo tramite la CloudFron t distribuzione designata, assicurandoti che i contenuti siano protetti dalle regole WAF, dai limiti di velocità e dagli altri controlli di sicurezza configurati nella distribuzione. CloudFront	Sì 	Sì 	Sì 	Sì 
Certificato TLS gratuito Certificato TLS gratuito per il tuo dominio con rinnovo automatico tramite. AWS Certificate Manager	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Firmato URLs	Sì	Sì	Sì	Sì
Crea contenuti sicuri URLs che forniscono l'accesso temporaneo ai contenuti privati per utenti specifici. Utilizzato comunemente per condividere documenti privati con utenti autorizzati o garantire l'accesso sicuro ai contenuti protetti dopo la verifica del pagamento.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
TLS reciproco (MTL) Limita l'accesso alla tua applicazione utilizzando l'autenticazione MTLS, assicurando che solo i client affidabili con certificati validi possano connettersi.				Sì 
Edge Compute				
Elaborazione perimetrale senza server Esegui un JavaScript approccio leggero all'edge per modificare le URLs intestazioni HTTP e gli request/response elementi in millisecondi utilizzando Functions. CloudFront	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Archivio chiave-valore di Edge		Sì	Sì	Sì
Archivia i dati all'edge utilizzando KeyValueStorela personalizzazione rapida e dinamica dei contenuti con Functions. CloudFront				
Supporto per reti e protocolli				
IPv6	Sì	Sì	Sì	Sì
Distribuisci contenuti tramite IPv4 connessioni moderne IPv6 e tradizionali CloudFront agli spettatori e alle origini. Abilita end-to-end IPv6 il supporto per le tue applicazioni.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
HTTP/2	Sì	Sì	Sì	Sì
Abilita caricamenti più rapidi delle pagine tramite funzionalità di protocollo moderne come il multiplexing, la compressione delle intestazioni e la prioritizzazione dei flussi. Utilizzato automaticamente se supportato da browser e client.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
HTTP/3	Sì	Sì	Sì	Sì
Distribuisci contenuti utilizzando QUIC ai browser e ai client che li supportano, abilitando connessioni più veloci e prestazioni migliorate. Avvantaggia in particolare gli utenti mobili e mantiene le connessioni quando le condizioni della rete cambiano.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
TLS 1.3	Sì	Sì	Sì	Sì
Offri connessioni HTTPS più veloci attraverso un processo di handshake che richiede un andata e ritorno rispetto ai due di TLS 1.2. Riduce la latenza del primo byte fino al 33% rispetto alle versioni TLS precedenti. Abilitato per end-to-end le tue applicazioni.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
WebSockets	Sì	Sì	Sì	Sì
Abilita una comunicazione bidirezionale persistente e in tempo reale tra browser e server. Ideale per applicazioni di chat basate sull'intelligenza artificiale, giochi multigiocatore, spazi di lavoro collaborativi e feed di dati in tempo reale come le piattaforme di trading finanziario.				
Logging e monitoraggio				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Registri di accesso Accedi ai log dettagliati delle CloudFront richieste per comprendere i modelli di traffico di sicurezza e consegna, con Amazon CloudWatch Logs, l'inserimento è incluso senza costi aggiuntivi.		Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Registri delle richieste WAF Accedi ai registri dettagliati delle AWS WAF richieste per comprende re i modelli di traffico relativi alla sicurezza e alla consegna. L'inserimento di Amazon CloudWatch Logs è incluso senza costi aggiuntivi.		Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
Dashboard di sicurezza	Sì	Sì	Sì	Sì
Monitora gli eventi di sicurezza, indaga sulle minacce e intraprendi azioni di blocco immediate utilizzando l'analisi visiva senza scrivere regole di sicurezza. Pro e versioni successive includono un analizzatore visivo dei log per comprendere rapidamente i modelli di traffico senza interroga re i log.				
DNS				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Amazon Route 53 DNS	Sì	Sì	Sì	Sì
Servizio DNS pubblico autoritativo veloce e affidabile che utilizza Route 53.				
Record per zona ospitata Il numero massimo di record DNS consentiti nella zona ospitata.	50	100	1000	5000

Prestazioni e consegna	Gratuito	Pro	Business	premio
DNSSEC	Sì	Sì	Sì	Sì
Proteggi il tuo dominio dallo spoofing DNS e man-in-the-middle dagli attacchi in cui gli aggressori intercettano le query DNS e reindirizzano i visitatori verso siti Web falsi. Protegge il traffico DNS firmando crittogra ficamente i tuoi record DNS.				
Storage				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Archiviazione Amazon S3	5 GB	50 GB	1 TB	5 TB
Crediti di storage Amazon S3 che compensano i costi di storage S3 Standard del tuo. Account AWS	Non limitato ai CloudFront contenuti o soggetto alle indennità di utilizzo del piano.			
Support e affidabilità				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Supporto per account e fatturazione 24 ore su 24, 7 giorni su 7	Sì 	Sì 	Sì 	Sì 
One-on-one risposte a domande sull'account e sulla fatturazione.				
Se disponi di un piano di assistenza a pagamento, hai diritto a ricevere assistenza su tutti i piani forfettari.				

Prestazioni e consegna	Gratuito	Pro	Business	premio
Documentazione e forum Supporto AWS Accedi alla documentazione sui prodotti, ai documenti tecnici, alle guide sulle best practice, ai forum AWS re:Post della community e alle informazioni sullo stato del servizio per aiutarti a pianificare e risolvere i problemi.	Sì 	Sì 	Sì 	Sì 

Prestazioni e consegna	Gratuito	Pro	Business	premio
SLA Uptime			Sì	Sì
I Service Level Agreement (SLA) per Amazon CloudFront AWS WAF, Amazon Route 53 e Amazon CloudWatch prevedono impegni di disponibilità del servizio. Nel caso in cui AWS non soddisfi l'impegno dello SLA associato, avrai diritto a ricevere un credito di servizio.				

Indennità di utilizzo mensili

Ogni piano forfettario include un'indennità di utilizzo mensile progettata per prestazioni ottimali a quel livello. Puoi tenere traccia dell'indennità di utilizzo nella CloudFront console in qualsiasi momento. Riceverai anche notifiche e-mail automatiche quando raggiungerai il 50%, 80% e 100% del tuo limite, anche se le notifiche potrebbero subire ritardi.

Seleziona un piano in cui l'indennità di utilizzo mensile si adatti al traffico di base relativo sia alle richieste che al trasferimento dei dati. Se superi l'indennità, non dovrai sostenere alcun costo aggiuntivo. Ciò consente di utilizzare l'applicazione senza preoccuparsi dei costi derivanti da picchi di traffico o attacchi imprevisti. Se superi le funzionalità del tuo piano o subisci una modifica nel traffico

di base, esegui l'upgrade al livello successivo per accedere a più funzionalità e aumentare l'indennità di utilizzo mensile. Se l'utilizzo supera le indennità previste dal piano CloudFront tariffario forfettario, puoi AWS adottare le misure appropriate, tra cui la riduzione delle prestazioni (ad esempio, la distribuzione del traffico da un numero minore o più distante di edge location, la riduzione della velocità effettiva o la limitazione) o la richiesta di una modifica della struttura tariffaria.

Se l'utilizzo di base dell'applicazione supera i 500 milioni di richieste o 50 TB al mese, contattaci per informazioni sui prezzi personalizzati.

Indennità di utilizzo mensili per livello di piano

	Gratuito	Pro	Business	premio
Richieste	1 M	10 M	125 M	500 M
Trasferimento dei dati	100 GB	50 TB	50 TBC	50 TBC

> **Note**
>
> Gli attacchi Blocked DDo S e le richieste bloccate da AWS WAF non contano mai ai fini del limite di utilizzo.

Idoneità basata sull'utilizzo storico

CloudFront L'utilizzo storico può influire sulla tua idoneità all'iscrizione o al downgrade a livelli di piano specifici. Se l'utilizzo recente supera le quote di utilizzo di un livello di piano, potrebbe essere necessario selezionare un livello superiore che si adatti meglio al carico di lavoro.

Costi coperti dal piano

Il piano copre i costi per:

- La tua CloudFront distribuzione
- L'ACL AWS WAF web associato alla tua distribuzione
- CloudWatch Inserimento dei log per i log di CloudFront accesso della distribuzione e per i log WAF associati

- La zona ospitata da Route 53, i record DNS e le query DNS se collegate al piano di distribuzione

Riceverai anche crediti S3 per compensare l'utilizzo dello storage S3 Standard nel tuo account di pagamento, indipendentemente dal fatto che un bucket S3 venga utilizzato o meno come origine per la distribuzione. CloudFront

La gestione del DNS di Route 53 e il tuo piano

Se utilizzi Route 53 per DNS e colleghi la zona al tuo piano, il piano forfettario può includere i costi della zona ospitata della Route 53. Puoi collegare la zona al tuo piano nella sezione Gestisci piano della tua CloudFront distribuzione. Quando la zona è associata al piano, quest'ultimo copre i costi standard della zona ospitata, tra cui la tariffa mensile per la zona ospitata, i record DNS e le tariffe per le query DNS, in base alle rispettive indennità per livello, riportate di seguito. La zona ospitata deve soddisfare i seguenti requisiti:

- Esiste nello stesso AWS account della tua CloudFront distribuzione
- Mantieni il numero di record consentiti per zona ospitata per il tuo livello di piano
- Copri il dominio utilizzato dalla tua CloudFront distribuzione

Se la tua zona ospitata non è collegata al tuo piano, rimarrà inclusa nella pay-as-you-go tariffa, dove sarai responsabile di tutti i costi standard di Route 53.

Comprensione delle quote mensili per le query DNS

Quando la tua zona ospitata è collegata al tuo piano, ottieni:

1. Query DNS ai record ALIAS che puntano alla tua CloudFront distribuzione e altre informazioni supportate Servizi AWS
2. Un'indennità mensile aggiuntiva per altri tipi di record DNS

	Gratuito	Pro	Business	premio
Query DNS ai record ALIAS (CloudFro	Nessun limite	Nessun limite	Nessun limite	Nessun limite

	Gratuito	Pro	Business	premio
nt e altri dati supportati Servizi AWS) al mese				
Indennità di query DNS aggiuntiva al mese	1 M	5 M	20 M	100 M

> **Note**
>
> Per massimizzare i vantaggi del tuo piano, utilizza i record ALIAS per indicare la tua CloudFront distribuzione. I record ALIAS che puntano a CloudFront e altri dati supportati Servizi AWS non vengono conteggiati ai fini della quota mensile di query DNS. Tutte le altre query DNS, compresi i record CNAME a, vengono conteggiate ai fini del limite consentito per le CloudFront query DNS.

Superamento dei limiti consentiti per le query DNS

Se l'utilizzo delle tue query DNS supera l'indennità mensile del tuo piano, potresti avvisarti. AWS A quel punto, puoi scollegare la tua zona ospitata dal piano nella sezione Gestisci piano della tua CloudFront distribuzione per riportare la zona ospitata ai prezzi. pay-as-you-go Se non scolleghi la zona ospitata dopo aver ricevuto questa notifica, puoi AWS trasferire automaticamente la zona ospitata ai pay-as-you-go prezzi. Quando una zona ospitata passa alla pay-as-you-go tariffazione, sei responsabile di tutti i costi standard della Route 53. La CloudFront distribuzione e tutti gli altri vantaggi del piano rimangono invariati.

Riduci AWS i costi complessivi con i piani tariffari

CloudFront I piani tariffari forfettari possono ridurre i AWS costi complessivi in tre modi:

Innanzitutto, i costi di trasferimento dei dati tra CloudFront e le AWS applicazioni in esecuzione su servizi come Amazon S3, AWS Application Load Balancer (ALB) o Amazon API Gateway vengono

automaticamente esclusi. Se servi AWS le tue applicazioni tramite Internet CloudFront anziché direttamente su Internet, il tuo piano forfettario copre i costi di trasferimento dei dati tra le tue applicazioni e i tuoi visualizzatori a un semplice prezzo mensile senza il rischio di eccedenze.

In secondo luogo, CloudFront riduce i costi di elaborazione e database proteggendo l'infrastruttura delle applicazioni e riducendo il numero di richieste che arrivano all'origine. Serve contenuti memorizzati nella cache da postazioni periferiche o cache periferiche regionali, comprime le richieste duplicate e blocca il traffico dannoso e indesiderato prima che raggiunga i servizi di backend. Ciò significa un minor numero di richieste che arrivano ai server delle applicazioni, ai database e ad altri dispositivi che vengono addebitati in base all'utilizzo, il Servizi AWS che riduce i costi.

Infine, ogni piano include crediti di storage Amazon S3 Standard per compensare l'utilizzo dello storage per te. Account AWS

Per massimizzare questi risparmi, configura le tue AWS origini in modo che accetti solo traffico da. CloudFront Per S3, usa Origin Access Control OAC con bucket privati per concedere l'accesso alla distribuzione designata. CloudFront Per le istanze di Application Load Balancer, Network Load Balancer e EC2 Amazon in sottoreti private, limita l'accesso alla distribuzione designata utilizzando VPC Origins. CloudFront

Gestisci i tuoi piani tariffari forfettari

Segui queste procedure nella CloudFront console per sottoscrivere, aggiornare, effettuare il downgrade o annullare un piano tariffario per le tue distribuzioni.

Sottoscrivi una nuova distribuzione a un piano tariffario

Quando crei una nuova distribuzione, puoi sottoscrivere un piano tariffario.

Per sottoscrivere una nuova distribuzione a un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Distribuzioni, quindi segui i passaggi per creare una distribuzione.
3. Scegli il piano tariffario della tua distribuzione. Tieni presente che alcune funzionalità non sono disponibili per ogni livello del piano tariffario. Controlla le funzionalità di ogni piano e scegli il piano tariffario più adatto alla tua applicazione.

4. Completa i passaggi per creare la tua distribuzione.

Sottoscrivi una distribuzione esistente a un piano tariffario

Quando aggiorni una distribuzione, puoi sottoscrivere un piano tariffario. Prima di scegliere un piano tariffario, assicurati che la configurazione di distribuzione sia compatibile con il piano che desideri.

> **Tip**
>
> Se la tua distribuzione attuale utilizza funzionalità non supportate, devi disabilitarle prima di sottoscrivere il piano tariffario. Ciò include la disabilitazione di funzionalità come Lambda @Edge o i log di accesso in tempo reale.

Una volta che la configurazione di distribuzione è compatibile, puoi scegliere il piano tariffario desiderato mentre aggiorni una distribuzione.

Per abbonare una distribuzione esistente a un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi segui i passaggi per aggiornare una distribuzione esistente.
3. Scegli il piano tariffario della tua distribuzione. Tieni presente che alcune funzionalità non sono disponibili per ogni livello del piano tariffario. Controlla le funzionalità di ogni piano e scegli il piano tariffario più adatto alla tua applicazione.
4. Completa i passaggi per aggiornare la tua distribuzione.

Aggiorna un piano tariffario

Ti consigliamo di aggiornare un piano se ti stai avvicinando o hai superato l'indennità di utilizzo mensile o se desideri abilitare una funzionalità disponibile nel livello successivo.

Quando effettui l'upgrade a un piano superiore, le modifiche hanno effetto immediato. Il prezzo e l'indennità di utilizzo vengono ripartiti proporzionalmente. La distribuzione e le risorse associate avranno accesso alle funzionalità disponibili e alla maggiore quota di utilizzo del nuovo piano.

Per aggiornare un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegli la tua distribuzione che è abbonata a un piano tariffario esistente.
4. Segui le istruzioni per aggiornare il piano tariffario della tua distribuzione.
5. Completa i passaggi per aggiornare una distribuzione esistente.

Effettua il downgrade di un piano tariffario

Ti consigliamo di effettuare il downgrade a un piano inferiore se non hai bisogno delle funzionalità aggiuntive del piano esistente. Ad esempio, potresti effettuare il downgrade se prevedi che la tua applicazione subisca una riduzione del traffico.

Se effettui il downgrade a un livello inferiore, le modifiche alla fatturazione entreranno in vigore all'inizio del ciclo di fatturazione successivo.

Se la tua distribuzione attualmente supera l'indennità di utilizzo prevista per un piano, puoi effettuare il downgrade una volta che l'utilizzo rientra nel limite di utilizzo previsto per il livello desiderato. Per evitare l'addebito del piano esistente al ciclo di fatturazione successivo, esegui il downgrade prima della fine del mese.

Per effettuare il downgrade di un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegli la tua distribuzione che è abbonata a un piano tariffario esistente.
4. Segui le istruzioni per effettuare il downgrade del piano tariffario della tua distribuzione. Se hai funzionalità non supportate, devi rimuovere la funzionalità o la risorsa dalla distribuzione.
5. Completa i passaggi per aggiornare una distribuzione esistente.

Annullare un piano tariffario

Quando annulli un piano tariffario, manterrai il prezzo forfettario fino alla fine del ciclo di fatturazione corrente. La distribuzione e tutte le risorse del piano associate passeranno quindi alla pay-as-you-go determinazione dei prezzi all'inizio del ciclo di fatturazione successivo.

Per annullare un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegli la tua distribuzione che è abbonata a un piano tariffario esistente.
4. Segui le istruzioni per annullare il piano tariffario della tua distribuzione. Se hai funzionalità non supportate, devi rimuovere la funzionalità o la risorsa dalla distribuzione.
5. Completa i passaggi per aggiornare una distribuzione esistente.

Annullare una modifica del piano in sospeso

Se hai effettuato il downgrade o annullato il piano tariffario forfettario, devi attendere la fine del ciclo di fatturazione corrente prima che le modifiche abbiano effetto. Per mantenere il piano tariffario forfettario esistente, effettuare nuovamente l'upgrade o il downgrade del piano tariffario, devi prima annullare la modifica in sospeso del piano.

Per annullare una modifica in sospeso del piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegli la tua distribuzione che è abbonata a un piano tariffario esistente.
4. Segui le istruzioni per annullare la modifica del piano in sospeso della distribuzione.
5. Scegli il piano tariffario che desideri per la tua distribuzione.
6. Completa i passaggi per aggiornare una distribuzione esistente.

Eliminazione di una distribuzione con un piano tariffario

Non puoi eliminare una distribuzione sottoscritta a un piano tariffario. Devi prima annullare il piano tariffario e poi, dopo il ciclo di fatturazione corrente, eliminare la distribuzione.

Per eliminare una distribuzione con un piano tariffario

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Segui i passaggi precedenti per annullare il piano tariffario della distribuzione.
4. Segui i passaggi per eliminare la distribuzione.

> **Note**
>
> Puoi disabilitare una distribuzione sottoscritta a un piano tariffario, ma ti verranno comunque addebitati dei costi per quel piano. Per evitare di incorrere in addebiti per il tuo piano, devi prima annullarlo.

Permissions

Per visualizzare o gestire gli abbonamenti ai piani tariffari per le tue CloudFront distribuzioni, devi disporre delle autorizzazioni richieste. Per ulteriori informazioni, consultare AWS politica gestita: CloudFrontFullAccess e AWS politica gestita: CloudFrontReadOnlyAccess.

Quote del piano tariffario forfettario

La tabella seguente mostra le quote e le restrizioni per i piani tariffari CloudFront forfettari.

> **Note**
>
> Queste quote non possono essere aumentate per te. Account AWS

Quote a livello di account	Quote
Piani tariffari per Account AWS	100
Piani gratuiti per Account AWS	3
Domini di livello APEX per piano	1

Caratteristiche non supportate

Prima di poter associare una distribuzione a un piano tariffario, devi assicurarti che alcune funzionalità siano disabilitate e che le associazioni vengano rimosse.

> **Note**
>
> - Se la tua distribuzione o il tuo account presentano una di queste restrizioni, devi risolverle prima di poter utilizzare i piani tariffari. Dopo aver apportato modifiche alla distribuzione, attendi che le modifiche si propaghino a tutte le edge location.
> - È necessario che alla distribuzione sia associato un ACL AWS WAF Web se si utilizza un piano tariffario. Questa risorsa non può essere rimossa o dissociata dalla distribuzione a meno che non si passi alla pay-as-you-go determinazione dei prezzi per quella distribuzione.

Caratteristiche non supportate

Non puoi sottoscrivere distribuzioni a un piano tariffario se la loro configurazione contiene le seguenti funzionalità non supportate. Puoi disabilitare la funzionalità non supportata e utilizzare un'opzione alternativa oppure conservarla pay-as-you-go per la tua distribuzione.

Caratteristiche non supportate	Opzioni alternative	Servizio AWS
Distribuzioni multi-tenant	Utilizza una distribuzione o una determinazione dei prezzi standard pay-as-you-go	CloudFront

Caratteristiche non supportate	Opzioni alternative	Servizio AWS
Distribuzione continua e distribuzioni stagionali	Usa i prezzi pay-as-you-go	CloudFront
Configurazione dell'elenco IP Anycast	Usa i prezzi pay-as-you-go	CloudFront
Registri di accesso in tempo reale	Utilizza registri di accesso o prezzi standard pay-as-you-go	CloudFront
Funzioni Lambda @Edge	Usa CloudFront le funzioni o pay-as-you-go i prezzi	CloudFront
Bot mirati	Usa bot o prezzi comuni pay-as-you-go	AWS WAF
CAPTCHA	Utilizza la sfida o pay-as-you-go il prezzo	AWS WAF
Regole gestite dai partner	Usa pay-as-you-go i prezzi	AWS WAF
Creazione di account e prevenzione delle frodi	Usa pay-as-you-go i prezzi	AWS WAF
Protezione dall'acquisizione dell'account	Usa i prezzi pay-as-you-go	AWS WAF
Gruppi di regole	Crea regole individuali (i gruppi di regole sono AWS WAF regole condivise che possono essere applicate a un ACL Web, analogamente alle politiche suCloudFront)	AWS WAF

Caratteristiche non supportate	Opzioni alternative	Servizio AWS
Funzionalità precedenti		
Configurazione di Forwarded Values	Usa le politiche di richiesta di Origin	CloudFront
IP/SSL dedicato	pay-as-you-goUsa i prezzi	CloudFront
Criptaggio a livello di campo	Usa pay-as-you-go i prezzi	CloudFront
AWS Identity and Access Management certificati server (IAM)	Usa AWS Certificate Manager certificati (ACM)	CloudFront
Identità di accesso all'origine (OAI)	Usa Origin Access Control (OAC)	CloudFront
Impostazioni della cache precedente	Utilizza le politiche di cache e le politiche di richiesta di origine.	CloudFront

Associazioni non supportate

Non è possibile sottoscrivere una distribuzione a un piano tariffario se la distribuzione è già associata a una delle seguenti risorse che sono già associate ad altre distribuzioni. Le risorse associate a una distribuzione sottoscritta a un piano tariffario possono essere utilizzate solo per tale distribuzione. Ad esempio, se si dispone di una CloudFront funzione che utilizza un archivio di valori chiave, né la funzione né l'archivio valori chiave possono essere condivisi per una distribuzione che rientra in un piano tariffario.

- CloudFront Funzioni
- CloudFront Funzioni associate a un archivio di valori chiave
- AWS WAF App ACLs

Per sottoscrivere una distribuzione a un piano tariffario, rimuovi la risorsa associata o sostituiscila con un'altra.

Vincoli a livello di account

Account AWS non sono idonei ai piani tariffari se soddisfano una delle seguenti condizioni:

- Hai raggiunto il numero massimo di abbonamenti consentiti. Per informazioni, consulta Quote del piano tariffario forfettario.
- Il tuo account sta utilizzando Piano gratuito di AWS.

Vincoli a livello di risorsa

Le distribuzioni non sono idonee ai piani tariffari se soddisfano una delle seguenti condizioni:

- La tua distribuzione è abilitata AWS Shield Advanced
- La tua distribuzione ha abilitato il servizio Firewall Manager per il tuo ACL web. Firewall Manager non gestirà il WebACL della tua CloudFront distribuzione in un piano tariffario.

Funzionalità aggiuntive che possono influire sul piano tariffario

I piani tariffari forfettari consentono di pagare una tariffa forfettaria per la CloudFront distribuzione e le funzionalità sopra elencate, incluse nel piano e associate alla CloudFront distribuzione. Tutte le altre funzionalità possono comportare costi aggiuntivi, tra cui, a titolo esemplificativo ma non esaustivo, quanto segue:

Route 53

- Route 53 DNSSEC ha un costo AWS KMS
- Blocchi IP Route 53 (CIDR) (i primi 1.000 sono gratuiti per ogni blocco) Account AWS
- Route 53 Health Checks (i primi 50 sono gratuiti per persona Account AWS)

Funzionalità di registrazione

- Registri delle query DNS di Route 53, registri CloudFront delle funzioni e registri delle funzioni di connessione CloudFront

- AWS WAF consegna dei log ad Amazon S3
- CloudFront o consegna dei AWS WAF log ad Amazon Data Firehose
- CloudWatch Metriche aggiuntive per CloudFront
- CloudFront registri di accesso in formato Parquet

> **Note**
>
> Il tuo piano include l'inserimento di Amazon CloudWatch Logs per i log CloudFront standard (log di accesso) e i log WAF senza costi aggiuntivi. Tutti gli altri CloudWatch costi, come lo storage e l'esecuzione di query, non sono coperti dal tuo piano. Anche tutti gli altri registri vengono fatturati separatamente.

> **Note**
>
> Il tuo piano include il DNS pubblico autoritativo di Route 53. Se la zona ospitata Route 53 è associata al piano tariffario, il piano copre i costi standard della zona ospitata, tra cui la tariffa mensile per la zona ospitata, i record DNS e le tariffe per le query DNS, soggette alle rispettive quote per livello. Tutti gli altri costi derivanti dall'utilizzo della Route 53 e le funzionalità non elencate sopra e incluse nel piano non sono coperti dal piano.

Piani tariffari e prezzi pay-as-you-go

I piani e i pay-as-you-go prezzi forfettari offrono diversi vantaggi in base alle tue esigenze. Con i piani a tariffa fissa, paghi un'unica tariffa che include più opzioni Servizi AWS come CloudFront Route 53 e CloudWatch Logs Ingestion e non dovrai mai affrontare addebiti aggiuntivi, nemmeno in caso di picchi di traffico o attacchi. AWS WAF

Per quanto riguarda pay-as-you-go i prezzi, ti vengono fatturati separatamente per ogni servizio e funzionalità in base all'utilizzo effettivo. Sebbene ciò offra una flessibilità completa nella selezione e nella configurazione dei servizi, i costi possono variare di mese in mese in base ai modelli di traffico e dovrai monitorare l'utilizzo di più servizi per gestire i costi.

I piani a tariffa fissa sono ideali se desideri una fatturazione mensile combinata, una configurazione semplificata del servizio e funzionalità di sicurezza integrate senza preoccuparti dei costi aggiuntivi. Pay-as-you-gola tariffazione è la scelta migliore se hai bisogno del controllo completo sulle singole

funzionalità del servizio, sulle configurazioni personalizzate, sull'accesso a funzionalità non disponibili nei piani a tariffa fissa o se prevedi di gestire picchi di traffico elevati e prevedibili. I piani CloudFront tariffari forfettari di Amazon non possono essere combinati con altre offerte, promozioni o sconti.

Configurazione delle distribuzioni

Crei una CloudFront distribuzione Amazon per indicare CloudFront da dove desideri che vengano distribuiti i contenuti e i dettagli su come monitorare e gestire la distribuzione dei contenuti.

Quando crei la tua CloudFront distribuzione, configura CloudFront automaticamente la maggior parte delle impostazioni di distribuzione per te, in base al tipo di origine dei contenuti. Per ulteriori dettagli sulle impostazioni preconfigurate, consulta Riferimento alle impostazioni di distribuzione preconfigurate. Facoltativamente, puoi scegliere di modificare manualmente le impostazioni di distribuzione. Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.

È possibile configurare le seguenti impostazioni:

- L'origine dei tuoi contenuti: il bucket AWS Elemental MediaPackage , il canale, il contenitore AWS Elemental MediaStore , il sistema di bilanciamento del carico Elastic Load Balancing o il server HTTP di Amazon S3 da cui provengono i file da CloudFront distribuire. Per una singola distribuzione, è possibile specificare qualsiasi combinazione fino a un massimo di 25 origini.
- Accesso: indica se i file devono essere disponibili per tutti gli utenti o se intendi limitare l'accesso ad alcuni utenti.
- Sicurezza: indica se vuoi abilitare la protezione AWS WAF e richiedere agli utenti di usare HTTPS per accedere ai tuoi contenuti. Per le distribuzioni multi-tenant, sono supportate solo le liste di controllo degli accessi Web AWS WAF V2 (). ACLs
- Chiave cache: indica quali valori, se presenti, desideri includere nella chiave cache. La chiave cache identificherà in modo univoco ogni file nella cache per una determinata distribuzione.
- Impostazioni della richiesta Origin: se desideri CloudFront includere intestazioni HTTP, cookie o stringhe di query nelle richieste inviate all'origine.
- Restrizioni geografiche: se desideri impedire CloudFront agli utenti di determinati paesi di accedere ai tuoi contenuti.
- Registri: sia che vogliate CloudFront creare registri standard o registri di accesso in tempo reale che mostrino l'attività degli spettatori.

Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.

Per il numero massimo attuale di distribuzioni che puoi creare per ciascuna, consulta. Account AWSQuote generali sulle distribuzioni Non esiste un numero massimo di file che è possibile servire per distribuzione.

Puoi utilizzare le distribuzioni per distribuire i seguenti contenuti su HTTP o HTTPS:

- Download di contenuti statici e dinamici, ad esempio HTML JavaScript, CSS e file di immagine, tramite HTTP o HTTPS.
- Video on demand in diversi formati, ad esempio Apple HTTP Live Streaming (HLS) e Microsoft Smooth Streaming. Per le distribuzioni multi-tenant, Smooth Streaming non è supportato. Per ulteriori informazioni, consulta Distribuisci video su richiesta con CloudFront.
- Un evento live, ad esempio un meeting, una conferenza o un concerto, in tempo reale. Per lo streaming live, puoi creare la distribuzione automaticamente utilizzando uno CloudFormation stack. Per ulteriori informazioni, consulta Offri lo streaming video con CloudFront e AWS Media Services.

I seguenti argomenti forniscono maggiori dettagli sulle CloudFront distribuzioni e su come configurarle per soddisfare le esigenze aziendali. Per informazioni su come creare una distribuzione, consulta Creazione di una distribuzione.

Argomenti

Comprendere il funzionamento delle distribuzioni multi-tenant

È possibile creare distribuzioni CloudFront multi-tenant con impostazioni che possono essere riutilizzate su più tenant di distribuzione. Con una distribuzione multi-tenant, puoi CloudFront configurare automaticamente le impostazioni di distribuzione in base al tipo di origine dei contenuti. Per ulteriori dettagli sulle impostazioni preconfigurate, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

I vantaggi dell'utilizzo di una distribuzione multi-tenant anziché di una distribuzione standard includono:

- Riduzione degli oneri operativi.
- Configurazioni riutilizzabili per amministratori Web e fornitori di software per gestire la CloudFront distribuzione di più applicazioni Web che forniscono contenuti agli utenti finali.
- Integrazioni avanzate con altri Servizi AWS per offrire una gestione automatizzata dei certificati, controlli di sicurezza unificati e un controllo della configurazione senza problemi su larga scala.
- Mantenimento di modelli di risorse coerenti in tutte le implementazioni. Definire le impostazioni che devono essere condivise e quindi specificare le personalizzazioni per le impostazioni da sovrascrivere.
- Impostazioni di origine e sicurezza personalizzabili per soddisfare esigenze specifiche a livello di tenant di distribuzione.
- Organizzare i tenant di distribuzione in diversi livelli. Ad esempio, se alcuni tenant di distribuzione richiedono Origin Shield e altri no, è possibile raggruppare i tenant di distribuzione in diverse distribuzioni multi-tenant.
- Condivisione di una configurazione DNS comune su più domini.

A differenza di una distribuzione standard, non è possibile accedere direttamente a una distribuzione multi-tenant perché non dispone di un endpoint di routing. CloudFront Pertanto, deve essere utilizzata insieme a un gruppo di connessioni e uno o più tenant di distribuzione. Sebbene le distribuzioni standard abbiano un proprio CloudFront endpoint e siano accessibili direttamente dagli utenti finali, non possono essere utilizzate come modello per altre distribuzioni.

Per ulteriori informazioni sulle quote di distribuzione multi-tenant, consulta Quote sulle distribuzioni multi-tenant.

Argomenti

Come funziona

In una distribuzione standard, la distribuzione contiene tutte le impostazioni da abilitare per il sito web o la tua applicazione, come le configurazioni di origine, i comportamenti della cache e le impostazioni di sicurezza. Se desideri creare un sito web separato e utilizzare molte delle stesse impostazioni, devi creare una nuova distribuzione ogni volta.

CloudFront Le distribuzioni multi-tenant sono diverse in quanto è possibile creare una distribuzione multi-tenant iniziale. Per ogni nuovo sito web, crea un tenant di distribuzione che eredita automaticamente i valori definiti della relativa distribuzione di origine. Quindi, personalizza le impostazioni specifiche per il tenant di distribuzione.

Panoramica di

1. Per iniziare, devi prima creare una distribuzione multi-tenant. CloudFront configura automaticamente le impostazioni di distribuzione, in base al tipo di origine dei contenuti. Puoi personalizzare le impostazioni per tutte le origini tranne VPC Origins. Le impostazioni VPC Origins vengono personalizzate sulla risorsa di origine VPC stessa. Per ulteriori informazioni sulle impostazioni di distribuzione multi-tenant che puoi personalizzare, consulta Riferimento alle impostazioni di distribuzione preconfigurate.
   - Il certificato TLS che utilizzi per la distribuzione multi-tenant può essere ereditato dai tenant di distribuzione. La distribuzione multi-tenant stessa non è instradabile, quindi non avrà un nome di dominio associato.
2. Per impostazione predefinita, CloudFront crea automaticamente un gruppo di connessione. Il gruppo di connessione controlla il modo in cui si connettono le richieste di contenuto degli utenti CloudFront. Puoi personalizzare alcune impostazioni di instradamento nel gruppo di connessioni.

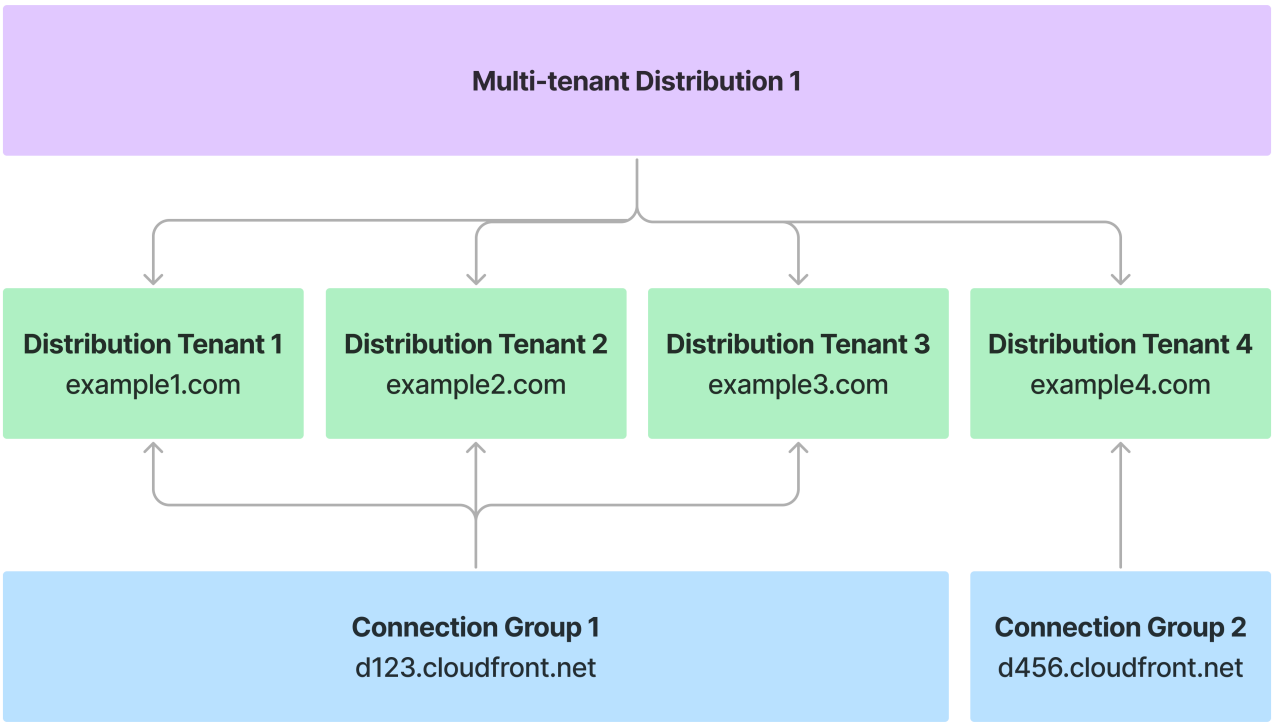
Puoi modificare questa impostazione creando manualmente un gruppo di connessioni. Per ulteriori informazioni, consulta Creazione di un gruppo di connessioni personalizzato (opzionale).

3. Quindi, crea uno o più tenant di distribuzione. Il tenant di distribuzione è la “porta d’ingresso” per consentire ai visualizzatori di accedere ai contenuti. Ogni tenant di distribuzione fa riferimento alla distribuzione multi-tenant e viene automaticamente associato al gruppo di connessione CloudFront creato per te. Il tenant di distribuzione supporta un singolo dominio o sottodominio.
4. Puoi quindi personalizzare alcune impostazioni del tenant di distribuzione, come i domini vanity e i percorsi di origine. Per ulteriori informazioni, consulta Personalizzazioni dei tenant di distribuzione.
5. Infine, devi aggiornare il record DNS nell’host DNS per indirizzare il traffico verso il tenant di distribuzione. A tale scopo, ottieni il valore dell' CloudFront endpoint dal tuo gruppo di connessione e crea un record CNAME che punti all'endpoint. CloudFront

Example Esempio

Il grafico seguente mostra come una distribuzione multi-tenant, i tenant di distribuzione e i gruppi di connessioni interagiscono per fornire contenuti ai visualizzatori di più domini.

1. La distribuzione multi-tenant definisce le impostazioni ereditate per ciascun tenant di distribuzione. Si utilizza la distribuzione multi-tenant come modello.
2. Ogni tenant di distribuzione creato dalla distribuzione multi-tenant dispone di un proprio dominio.
3. I tenant di distribuzione vengono aggiunti automaticamente al gruppo di connessione CloudFront creato per te quando hai creato la distribuzione multi-tenant. I gruppi di connessione controllano il modo in cui le richieste dei visualizzatori sono connesse alla rete. CloudFront



Per informazioni dettagliate sulla creazione di distribuzioni multi-tenant, consulta Crea una CloudFront distribuzione nella console.

Termini

I seguenti concetti descrivono i componenti delle distribuzioni multi-tenant:

Distribuzione multi-tenant

Una distribuzione multi-tenant, blueprint che specifica tutte le impostazioni di configurazione condivise per tutti i tenant di distribuzione, inclusi il comportamento cache, le protezioni di sicurezza e le origini. Le distribuzioni multi-tenant non possono gestire direttamente il traffico. Devono essere utilizzate insieme a gruppi di connessioni e tenant di distribuzione.

Distribuzione standard

Una distribuzione che non dispone di funzionalità multi-tenant. Queste distribuzioni sono ideali per supportare singoli siti Web o app.

Tenant di distribuzione

Un tenant di distribuzione eredita la configurazione di distribuzione multi-tenant. Alcune impostazioni di configurazione possono essere personalizzate a livello di tenant di distribuzione. Il tenant di distribuzione deve disporre di un certificato TLS valido, che può essere ereditato dalla distribuzione multi-tenant purché copra il dominio o sottodominio del tenant di distribuzione.

Il tenant di distribuzione deve essere associato a un gruppo di connessione. CloudFront crea automaticamente un gruppo di connessione quando si crea un tenant di distribuzione e assegna automaticamente tutti i tenant di distribuzione a quel gruppo di connessione.

Multilocazione

Puoi utilizzare la distribuzione multi-tenant per fornire contenuti su più domini, condividendo al contempo la configurazione e l'infrastruttura. Questo approccio consente a domini diversi (chiamati tenant) di condividere impostazioni comuni dalla distribuzione multi-tenant, mantenendo al contempo le proprie personalizzazioni.

Gruppo di connessioni

Fornisce l'endpoint CloudFront di routing che fornisce i contenuti agli spettatori. È necessario associare ogni tenant di distribuzione a un gruppo di connessione per ottenere l'endpoint di CloudFront routing corrispondente per il record CNAME creato per il dominio o il sottodominio del tenant di distribuzione. I gruppi di connessioni possono essere condivisi tra più tenant di distribuzione. I gruppi di connessione gestiscono le impostazioni di routing per i tenant di distribuzione, ad esempio le impostazioni dell'elenco IP Anycast. IPv6

Parameters

Un elenco di coppie chiave-valore per i valori segnaposto, ad esempio i percorsi di origine e i nomi di dominio. Puoi definire i parametri nella distribuzione multi-tenant e fornire valori per tali parametri a livello di tenant di distribuzione. Puoi scegliere se i valori dei parametri devono essere inseriti per il tenant di distribuzione.

Se non fornisci un valore per un parametro opzionale in un tenant di distribuzione, viene utilizzato il valore predefinito della distribuzione multi-tenant.

CloudFront endpoint di routing

DNS canonico per il gruppo di connessioni, ad esempio `d123.cloudfront.net`. Utilizzato nel record CNAME per il dominio o sottodominio del tenant di distribuzione.

Personalizzazioni

Puoi personalizzare i tenant di distribuzione in modo che utilizzino impostazioni diverse dalla distribuzione multi-tenant. Per ogni tenant di distribuzione, è possibile specificare una lista di controllo degli accessi AWS WAF Web (ACL), certificati TLS e restrizioni geografiche diversi.

Caratteristiche non supportate

Le seguenti funzionalità non possono essere utilizzate con una distribuzione multi-tenant. Se desideri creare una nuova distribuzione multi-tenant utilizzando le stesse impostazioni della distribuzione standard, tieni presente che alcune impostazioni non sono disponibili.

> **Note**
>
> - Attualmente, AWS Firewall Manager le politiche si applicano solo alle distribuzioni standard. Firewall Manager aggiungerà il supporto per le distribuzioni multi-tenant in una versione futura.
> - A differenza delle distribuzioni standard, il nome di dominio (alias) viene specificato a livello di tenant di distribuzione. Per ulteriori informazioni, consulta Richiedi i certificati per il tuo tenant CloudFront di distribuzione e il funzionamento dell'CreateDistributionTenantAPI.

- Implementazione continua
- Identità di accesso origine (OAI): utilizza invece il controllo di accesso origine (OAI).
- Supporto SSL personalizzato con IP dedicato: è supportato solo il metodo `sni-only`.
- AWS WAF ACL web classico (V1): sono supportati solo i siti Web AWS WAF ACLs V2.
- Registrazione di log standard (legacy)
- TTL minimo
- TTL predefinito
- TTL massimo
- ForwardedValues
- PriceClass
- Firmatari attendibili
- Smooth Streaming

- AWS Identity and Access Management certificati del server (IAM)
- Indirizzi IP dedicati
- Versione minima del protocollo SSLv3

Le seguenti impostazioni non possono essere configurate in una distribuzione multi-tenant o in un tenant di distribuzione. Imposta invece i valori che desideri in un gruppo di connessioni. Tutti i tenant di distribuzione associati al gruppo di connessioni utilizzeranno queste impostazioni. Per ulteriori informazioni, consulta Creazione di un gruppo di connessioni personalizzato (opzionale).

- Abilita IPv6 (richieste del visualizzatore)
- Elenco di IP statici anycast

Personalizzazioni dei tenant di distribuzione

Quando si utilizza una distribuzione multi-tenant, i tenant di distribuzione ereditano la configurazione di distribuzione multi-tenant. Tuttavia, puoi personalizzare alcune impostazioni a livello di tenant di distribuzione.

Puoi personalizzare gli elementi seguenti:

- Parametri: i parametri sono coppie chiave-valore che puoi utilizzare per il dominio di origine o i percorsi di origine. Per informazioni, consulta Come funzionano i parametri con tenant di distribuzione.
- AWS WAF Web ACL (V2): è possibile specificare un ACL Web separato per il tenant di distribuzione, che sostituirà l'ACL Web utilizzato per la distribuzione multi-tenant. Puoi anche disabilitare questa impostazione per un tenant di distribuzione specifico, il che significa che il tenant di distribuzione non erediterà le protezioni ACL Web dalla distribuzione multi-tenant. Per ulteriori informazioni, consulta AWS WAF ACL web.
- Restrizioni geografiche: le restrizioni geografiche specificate per un tenant di distribuzione sovrascriveranno qualsiasi restrizione geografica per la distribuzione multi-tenant. Ad esempio, se blocchi Germania (DE) nella distribuzione multi-tenant, anche tutti i tenant di distribuzione associati bloccheranno DE. Tuttavia, se consenti DE per un tenant di distribuzione specifico, le impostazioni di tale tenant di distribuzione sovrascriveranno le impostazioni per la distribuzione multi-tenant. Per ulteriori informazioni, consulta Limitazione della distribuzione geografica del contenuto.
- Percorsi di invalidazione: specifica i percorsi dei file del contenuto che desideri invalidare per il tenant di distribuzione. Per ulteriori informazioni, consulta Invalidare i file.

- Certificati TLS personalizzati: i certificati AWS Certificate Manager (ACM) specificati per i tenant di distribuzione sono supplementari al certificato fornito nella distribuzione multi-tenant. Tuttavia, se lo stesso dominio è coperto sia dalla distribuzione multi-tenant che dai certificati tenant di distribuzione, viene utilizzato il certificato tenant. Per ulteriori informazioni, consulta Richiedi i certificati per il tuo tenant CloudFront di distribuzione.
- Nomi di dominio: devi specificare almeno un nome di dominio per tenant di distribuzione.

Come funzionano i parametri con tenant di distribuzione

Un parametro è una coppia chiave-valore che puoi utilizzare per i valori segnaposto. Definisci i parametri che desideri utilizzare nella distribuzione multi-tenant e specifica se sono obbligatori.

Quando definisci i parametri nella distribuzione multi-tenant, puoi scegliere se tali parametri devono essere inseriti a livello di tenant di distribuzione.

- Se definisci i parametri come richiesti nella distribuzione multi-tenant, devono essere inseriti a livello di tenant di distribuzione. (Non vengono ereditati).
- Se i parametri non sono richiesti, puoi fornire un valore predefinito nella distribuzione multi-tenant ereditata dal tenant di distribuzione.

Puoi inoltre utilizzare i seguenti parametri di input:

- Origin Domain Name (Nome dominio origine)
- Percorso origine

Nella distribuzione multi-tenant, puoi definire fino a due parametri per ciascuna delle proprietà precedenti.

Parametri di esempio

Vedi i seguenti esempi per l'utilizzo dei parametri per il nome di dominio e il percorso di origine.

Parametri dei nomi di dominio

Nella configurazione di distribuzione multi-tenant, puoi definire un parametro per il nome di dominio di origine come negli esempi seguenti:

Simple Storage Service (Amazon S3)

- {{*parameter1*}}.amzn-s3-demo-logging-bucket.s3.us-east-1.amazonaws.com
- {{*parameter1*}}-amzn-s3-demo-logging-bucket.s3.us-east-1.amazonaws.com

Origini personalizzate

- {{*parameter1*}}.lambda-url.us-east-1.on.aws
- {{*parameter1*}}.mediapackagev2.ap-south-1.amazonaws.com

Quando crei un tenant di distribuzione, specifica il valore da utilizzare per *parameter1*.

```
"Parameters": [
  {
    "Name": "parameter1",
    "Value": "mycompany-website"
  }
]
```

Utilizzando gli esempi precedenti specificati nella distribuzione multi-tenant, il nome di dominio di origine per il tenant di distribuzione viene risolto come segue:

- *mycompany-website*.amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com
- *mycompany-website*-amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com
- *mycompany-website*.lambda-url.us-east-1.on.aws
- *mycompany-website*.mediapackagev2.ap-south-1.amazonaws.com

Parametri del percorso di origine

Allo stesso modo, puoi definire i parametri per il percorso di origine nella distribuzione multi-tenant come negli esempi seguenti:

- /{{*parameter2*}}
- /{{*parameter2*}}/test
- /public/{{*parameter2*}}/test
- /search?name={{*parameter2*}}

Quando crei un tenant di distribuzione, specifica il valore da utilizzare per *parameter2*.

```
"Parameters": [
  {
    "Name": "parameter2",
    "Value": "myBrand"
  }
]
```

Utilizzando gli esempi precedenti specificati nella distribuzione multi-tenant, il percorso di origine per il tenant di distribuzione viene risolto come segue:

- */myBrand*
- */myBrand*/test
- /public/*myBrand*/test
- /search?name=*myBrand*

Example Esempio

Desideri creare più siti web (tenant) per i clienti e devi assicurarti che ogni risorsa del tenant di distribuzione utilizzi i valori corretti.

1. Crea una distribuzione multi-tenant e includi due parametri per la configurazione del tenant di distribuzione.
2. Per il nome di dominio di origine, create un parametro denominato *customer-name* e specificate che è obbligatorio. Inserisci il parametro prima del bucket S3, in modo che venga visualizzato come:

   {{*customer-name*}}.amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com.
3. Per il percorso di origine, create un secondo parametro denominato *my-theme* e specificate che è facoltativo, con un valore predefinito di*basic*. Il percorso di origine viene visualizzato come: / {{*my-theme*}}
4. Quando crei un tenant di distribuzione:
   - Per il nome di dominio, è necessario specificare un valore per*customer-name*, poiché è contrassegnato come obbligatorio nella distribuzione multi-tenant.

- Per il percorso di origine, puoi facoltativamente specificare un valore *my-theme* o utilizzare il valore predefinito.

Richiedi i certificati per il tuo tenant CloudFront di distribuzione

Quando crei un tenant di distribuzione, il tenant eredita il certificato condiviso AWS Certificate Manager (ACM) dalla distribuzione multi-tenant. Questo certificato condiviso fornisce HTTPS per tutti i tenant associati alla distribuzione multi-tenant.

Quando si crea o si aggiorna un tenant di CloudFront distribuzione per aggiungere domini, è possibile aggiungere un certificato gestito da ACM. CloudFront CloudFront ottiene quindi un certificato convalidato HTTP da ACM per tuo conto. Puoi utilizzare questo certificato ACM a livello di tenant per configurazioni di dominio personalizzate. CloudFront semplifica il flusso di lavoro di rinnovo per aiutare a mantenere i certificati up-to-date e la distribuzione sicura dei contenuti senza interruzioni.

> **Note**
>
> Il certificato è di tua proprietà, ma può essere utilizzato solo con CloudFront risorse e la chiave privata non può essere esportata.

Puoi richiedere il certificato quando crei o aggiorni il tenant di distribuzione.

Argomenti

- Aggiunta di un dominio e di un certificato (tenant di distribuzione)
- Configurazione completa del dominio
- Indirizza i domini a CloudFront
- Considerazioni sul dominio (tenant di distribuzione)
- Domini con carattere jolly (tenant di distribuzione)

Aggiunta di un dominio e di un certificato (tenant di distribuzione)

Nella procedura seguente viene illustrato come aggiungere un dominio e aggiornare il certificato per un tenant di distribuzione.

Come aggiungere un dominio e un certificato (tenant di distribuzione)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. In SaaS, scegli Tenant di distribuzione.
3. Cerca il tenant di distribuzione. Utilizza il menu a discesa nella barra di ricerca per filtrare per dominio, nome, ID distribuzione, ID certificato, ID gruppo di connessioni o ID ACL Web.
4. Scegli il nome del tenant di distribuzione.
5. Per Domini, scegli Gestisci dominio.
6. Per Certificato, scegli se utilizzare un certificato TLS personalizzato per il tenant di distribuzione. Il certificato verifica se disponi dell'autorizzazione per utilizzare il nome di dominio. Il certificato deve esistere nella Regione Stati Uniti orientali (Virginia settentrionale).
7. Per Domini, scegli Aggiungi dominio e inserisci il nome di dominio. A seconda del dominio, sotto il nome di dominio inserito verranno visualizzati i seguenti messaggi.

   - Questo dominio è coperto dal certificato.
   - Questo dominio è coperto dal certificato, in attesa di convalida.
   - Questo dominio non è coperto dal certificato. (Ciò significa che occorre verificare la proprietà del dominio).
8. Scegli Aggiorna tenant di distribuzione.

   Nella pagina dei dettagli del tenant, in Domini, puoi vedere i seguenti campi:

   - Proprietà del dominio: lo stato della proprietà del dominio. Prima di CloudFront poter pubblicare contenuti, è necessario verificare la proprietà del dominio utilizzando la convalida del certificato TLS.
   - Stato DNS: i record DNS del tuo dominio devono puntare a CloudFront indirizzare correttamente il traffico.
9. Se la proprietà del dominio non è verificata, nella pagina dei dettagli del tenant, in Domini, scegli Configurazione completa del dominio, quindi completa la procedura seguente per indirizzare il record DNS al tuo nome di dominio. CloudFront

Configurazione completa del dominio

Segui queste procedure per verificare di essere il proprietario del dominio per i tenant di distribuzione. A seconda del dominio, scegli una delle seguenti procedure.

Note

Se il tuo dominio è già CloudFront indirizzato a un record di alias Amazon Route 53, devi aggiungere il record DNS TXT `_cf-challenge.` davanti al nome di dominio. Questo record TXT verifica che il tuo nome di dominio sia collegato a. CloudFront Ripeti questa fase per ogni dominio. Di seguito viene illustrato come aggiornare il record TXT:

- Nome del record: `_cf-challenge.`*`DomainName`*
- Tipo di record: `TXT`
- Valore del record: *`CloudFrontRoutingEndpoint`*

Ad esempio, l'aspetto del record TXT potrebbe essere simile al seguente: `_cf-challenge.example.com TXT d111111abcdef8.cloudfront.net`
Puoi trovare il tuo endpoint CloudFront di routing nella console nella pagina dei dettagli del tenant di distribuzione o utilizzare l'azione ListConnectionGroupsAPI in Amazon CloudFront API Reference per trovarlo.

Tip

Se sei un provider SaaS e desideri consentire l'emissione di certificati senza richiedere ai clienti (tenant) di aggiungere un record TXT direttamente al loro DNS, procedi come segue:

1. Se sei il proprietario del dominio `example-saas-provider.com`, assegna sottodomini ai tenant, ad esempio `customer-123.example-saas-provider.com`
2. Nel DNS, aggiungi il record TXT `_cf-challenge.customer-123.example-saas-provider.com TXT d111111abcdef8.cloudfront.net` alla configurazione DNS.
3. Successivamente, i clienti (i tenant) possono aggiornare il proprio record DNS per mappare il nome di dominio al sottodominio fornito.

   ```
   www.customer-domain.com CNAME customer-123.example-saas-provider.com
   ```

I have existing traffic

Seleziona questa opzione se il dominio non può tollerare tempo di inattività. Devi avere accesso al tuo server. origin/web Utilizza la procedura riportata di seguito per convalidare la proprietà del dominio.

Come completare la configurazione del dominio in presenza di traffico

1. Per Specifica il traffico web, scegli Ho traffico esistente, quindi seleziona Avanti.
2. Per Verifica la proprietà del dominio, scegli una delle seguenti opzioni:

   - Usa certificato esistente: cerca un certificato ACM esistente o inserisci l'ARN del certificato che copre i domini elencati.
   - Caricamento manuale file: scegli questa opzione se hai accesso diretto per caricare file sul server web.

     Per ogni dominio, crea un file di testo semplice che contenga il token di convalida dalla Posizione token e caricalo nell'origine del Percorso file specificato sul server esistente. Ad esempio, l'aspetto del percorso del file potrebbe essere simile all'esempio seguente: `/.well-known/pki-validation/acm_9c2a7b2ec0524d09fa6013efb73ad123.txt`. Dopo aver completato questa fase, ACM verifica il token e quindi emette il certificato TLS per il dominio.
   - Reindirizzamento HTTP: scegli questa opzione se non hai accesso diretto per caricare file sul server web o se utilizzi un servizio CDN o proxy.

     Per ogni dominio, crea un reindirizzamento 301 sul server esistente. Copia il percorso noto in Reindirizza da e indica l'endpoint del certificato specificato in Reindirizza a. L'aspetto del reindirizzamento potrebbe essere simile all'esempio seguente:

     ```
     If the URL matches: example.com/.well-known/pki-validation/
     leabe938a4fe077b31e1ff62b781c123.txt
     Then the settings are:Forwarding URL
     Then 301 Permanent Redirect:To validation.us-east-1.acm-
     validations.aws/123456789012/.well-known/pki-validation/
     leabe938a4fe077b31e1ff62b781c123.txt
     ```

> **Note**
>
> Puoi scegliere Verifica stato del certificato per verificare quando ACM emette il certificato per il dominio.

3. Scegli Next (Successivo).
4. Completa le fasi descritte in Indirizza i domini a CloudFront.

I don't have traffic

Seleziona questa opzione se stai aggiungendo nuovi domini. CloudFront gestirà la convalida dei certificati per te.

Come completare la configurazione del dominio in assenza di traffico

1. Per Specifica il traffico web, scegli Non ho ancora traffico.
2. Per ogni nome di dominio, completa le fasi indicate in Indirizza i domini a CloudFront.
3. Dopo aver aggiornato i record DNS per ogni nome di dominio, scegli Avanti.
4. Attendi che venga emesso il certificato.

> **Note**
>
> Puoi scegliere Verifica stato del certificato per verificare quando ACM emette il certificato per il dominio.

5. Seleziona Invia.

Indirizza i domini a CloudFront

Aggiorna i tuoi record DNS per indirizzare il traffico da ogni dominio all'endpoint di CloudFront routing. Puoi avere più nomi di dominio, ma devono tutti risolversi in questo endpoint.

Indirizzare i domini a CloudFront

1. Copia il valore dell'endpoint CloudFront di routing, ad esempio d111111abcdef8.cloudfront.net.

2. Aggiorna i tuoi record DNS per indirizzare il traffico da ogni dominio all'endpoint di routing. CloudFront

   1. Accedi al registrar di domini o console di gestione del provider DNS.
   2. Passa alla sezione Gestione DNS del dominio.
      - Per i sottodomini: crea un record CNAME. Esempio:
        - Nome: il sottodominio (ad esempio, `www` o `app`)
        - Valore/Target: l'endpoint di routing CloudFront
        - Tipo di record: CNAME
        - TTL: 3600 (o qualsiasi altro valore appropriato per il caso d'uso)
      - Per i apex/root domini: ciò richiede una configurazione DNS unica, poiché i record CNAME standard non possono essere utilizzati a livello di dominio root o apex. Poiché la maggior parte dei provider DNS non supporta i record ALIAS, è consigliabile creare un record ALIAS in Route 53. Esempio:
        - Nome: il dominio apex (ad esempio `example.com`)
        - Tipo di record: A
        - Alias: Sì
        - Alias target: il tuo endpoint di routing CloudFront
        - Policy di instradamento: semplice (o quella appropriata per il caso d'uso)
   3. Verifica che la modifica del DNS sia stata propagata. (Questo di solito accade quando il TTL è scaduto. A volte possono essere necessarie 24-48 ore.) Usa uno strumento come `dig` o `nslookup`.

      ```
      dig www.example.com
      # Should eventually return a CNAME pointing to your CloudFront routing endpoint
      ```

3. Torna alla CloudFront console e scegli Invia. Quando il dominio è attivo, CloudFront aggiorna lo stato del dominio per indicare che il dominio è pronto a servire il traffico.

Per ulteriori informazioni, consulta la documentazione relativa al provider DNS:

- Cloudflare
- ClouDNS
- DNSimple

- Gandi.net
- GoDaddy
- Google Cloud DNS
- Nome a buon mercato

Considerazioni sul dominio (tenant di distribuzione)

Quando un dominio è attivo, il controllo del dominio è stato stabilito e CloudFront risponderà a tutte le richieste dei visualizzatori di questo dominio. Una volta attivato, un dominio non può essere disattivato o modificato in uno stato inattivo. Il dominio non può essere associato a un'altra CloudFront risorsa mentre è già in uso. Per associare il dominio a un'altra distribuzione, usa la UpdateDomainAssociationrichiesta per spostare il dominio da una CloudFront risorsa all'altra.

Quando un dominio è inattivo, CloudFront non risponde alle richieste degli utenti al dominio. Mentre il dominio è inattivo, tieni presente quanto segue:

- Se hai una richiesta di certificato in sospeso, CloudFront risponderà alle richieste per il percorso noto. Mentre la richiesta è in sospeso, il dominio non può essere associato a nessun'altra CloudFront risorsa.
- Se non hai una richiesta di certificato in sospeso, CloudFront non risponderà alle richieste per il dominio. Puoi associare il dominio ad altre CloudFront risorse.
- È possibile avere solo una richiesta di certificato in sospeso per ogni tenant di distribuzione. Prima di poter richiedere un altro certificato per domini aggiuntivi, è necessario annullare la richiesta in sospeso esistente. L'annullamento di una richiesta di certificato esistente non elimina il certificato ACM associato. Puoi eliminarla utilizzando l'API ACM.
- Se applichi un nuovo certificato al tenant di distribuzione, il certificato precedente verrà dissociato. Puoi riutilizzare il certificato per coprire il dominio di un altro tenant di distribuzione.

Come per i rinnovi dei certificati convalidati dal DNS, riceverai una notifica quando il rinnovo del certificato è andato a buon fine. Tuttavia, non devi fare nient'altro. CloudFront gestirà automaticamente il rinnovo del certificato per il tuo dominio.

> **Note**
>
> Non è necessario chiamare le operazioni API ACM per creare o aggiornare le risorse dei certificati. Puoi gestire i tuoi certificati utilizzando le operazioni CreateDistributionTenante UpdateDistributionTenantAPI per specificare i dettagli della tua richiesta di certificato gestita.

Domini con carattere jolly (tenant di distribuzione)

I domini con carattere jolly sono supportati per i tenant di distribuzione nelle seguenti situazioni:

- Quando il carattere jolly è incluso nel certificato condiviso ereditato dalla distribuzione multi-tenant principale
- Quando si utilizza un certificato TLS personalizzato esistente valido per il tenant di distribuzione

Creazione di un gruppo di connessioni personalizzato (opzionale)

Per impostazione predefinita, CloudFront crea automaticamente un gruppo di connessione quando si crea una distribuzione multi-tenant. Il gruppo di connessione controlla il modo in cui si connettono le richieste di contenuto degli utenti. CloudFront

Ti consigliamo di utilizzare il gruppo di connessioni predefinito. Tuttavia, se è necessario isolare le applicazioni aziendali o gestire separatamente gruppi di tenant di distribuzione, è possibile scegliere di creare un gruppo di connessioni personalizzato. Ad esempio, potrebbe essere necessario spostare un tenant di distribuzione in un gruppo di connessione separato se subisce un attacco DDo S. In questo modo, è possibile proteggere gli altri tenant di distribuzione dall'impatto.

Creazione di un gruppo di connessioni personalizzato (opzionale)

Facoltativamente, puoi scegliere di creare un gruppo di connessioni personalizzato per i tenant di distribuzione.

Come creare un gruppo di connessioni personalizzato (opzionale)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione scegli Impostazioni.
3. Attiva le impostazioni del Gruppo di connessioni.

4. Nel riquadro di navigazione, scegli Gruppi di connessioni, quindi seleziona Crea gruppo di connessioni.
5. Per Nome gruppo di connessioni, immetti un nome per il gruppo di connessioni. Non è possibile aggiornare questo nome dopo aver creato il gruppo di connessioni.
6. Per IPv6, specifica se desideri abilitare questo protocollo IP. Per ulteriori informazioni, consulta Abilita IPv6 (richieste del visualizzatore).
7. Per Elenco di IP statici anycast, specifica se desideri distribuire il traffico ai tenant di distribuzione da un set di indirizzi IP. Per ulteriori informazioni, consulta Elenco di IP statici anycast.
8. (Facoltativo) Aggiungi tag al gruppo di connessioni.
9. Scegli Crea gruppo di connessioni.

Una volta creato il gruppo di connessioni, puoi trovare le impostazioni specificate, nonché l'ARN e l'endpoint.

- L'aspetto dell'ARN è simile a quello dell'esempio seguente: `arn:aws:cloudfront::123456789012:connection-group/cg_2uVbA9KeWaADTbKzhj9lcKDoM25`
- L'aspetto dell'endpoint è simile a quello dell'esempio seguente: d111111abcdef8.cloudfront.net

Puoi modificare o eliminare il gruppo di connessioni personalizzato dopo averlo creato. Prima di poter eliminare un gruppo di connessioni, è necessario eliminare tutti i tenant di distribuzione associati. Non puoi eliminare il gruppo di connessione predefinito CloudFront creato per te quando hai creato la distribuzione multi-tenant.

> **Important**
>
> Se si modifica il gruppo di connessione per un tenant di distribuzione, CloudFront continuerà a trasmettere traffico per il tenant di distribuzione, ma con una maggiore latenza. Si consiglia di aggiornare il record DNS per il tenant di distribuzione per utilizzare l'endpoint di CloudFront routing del nuovo gruppo di connessione.
> Fino all'aggiornamento del record DNS, il routing CloudFront verrà eseguito in base alle impostazioni definite per l'endpoint di routing a cui il sito Web punta attualmente tramite DNS. Ad esempio, supponiamo che il gruppo di connessione predefinito non utilizzi Anycast static IPs ma il nuovo gruppo di connessioni personalizzato sì. È necessario aggiornare il record

DNS prima di CloudFront utilizzare Anycast static IPs per i tenant di distribuzione nel gruppo di connessione personalizzato.

Migrazione a una distribuzione multi-tenant

Se disponi di una distribuzione CloudFront standard e desideri migrare a una distribuzione multi-tenant, segui questi passaggi.

Come migrare da una distribuzione standard a una distribuzione multi-tenant

1. Rivedere le Caratteristiche non supportate.
2. Crea una distribuzione multi-tenant con la stessa configurazione della distribuzione standard, senza le funzionalità non supportate. Per ulteriori informazioni, consulta Crea una CloudFront distribuzione nella console.
3. Crea un tenant di distribuzione e aggiungi un nome di dominio alternativo di cui sei il proprietario.

   > **Warning**
   >
   > Non utilizzare il nome di dominio corrente associato alla distribuzione standard. Aggiungi invece un dominio segnaposto. Trasferirai il dominio in un secondo momento. Per informazioni su come creare un tenant di distribuzione, consulta Crea una CloudFront distribuzione nella console.

4. Fornisci un certificato esistente per il dominio del tenant di distribuzione. Questo è il certificato che coprirà il dominio segnaposto e il dominio che desideri spostare.
5. Copia l'endpoint CloudFront di routing dalla pagina dei dettagli del tenant di distribuzione nella console. In alternativa, puoi trovarlo utilizzando l'azione ListConnectionGroupsAPI in Amazon CloudFront API Reference.
6. Per verificare la proprietà del dominio, crea un record TXT DCV con un prefisso di sottolineatura (_) che punti all'endpoint di CloudFront routing per il tenant di distribuzione. Per ulteriori informazioni, consulta Indirizza i domini a CloudFront.
7. Una volta propagate le modifiche, aggiorna il tenant di distribuzione in modo che utilizzi il dominio utilizzato in precedenza per la distribuzione standard.

   - Console: per istruzioni dettagliate, consulta Aggiunta di un dominio e di un certificato (tenant di distribuzione).

- API: utilizza l'azione UpdateDomainAssociationAPI in Amazon CloudFront API Reference.

> **Important**
>
> Questa operazione ripristina la chiave della cache per i contenuti in uso. Dopodiché, CloudFront inizia a memorizzare nella cache i contenuti utilizzando la nuova chiave cache. Per ulteriori informazioni, consulta Comprensione della chiave della cache.

8. Aggiorna il record DNS per indirizzare il dominio verso l'endpoint di CloudFront routing del tenant di distribuzione. Una volta completata questa fase, il dominio sarà pronto per fornire il traffico al tenant di distribuzione. Per ulteriori informazioni, consulta Indirizza i domini a CloudFront.
9. (Facoltativo) Dopo aver eseguito correttamente la migrazione del dominio su un tenant di distribuzione, è possibile utilizzare un certificato CloudFront gestito diverso che copra il nome di dominio del tenant di distribuzione. Per richiedere un certificato gestito, crea un record TXT separato per emettere il certificato e segui le fasi descritte in Configurazione completa del dominio.

Creazione di una distribuzione

Questo argomento spiega come utilizzare la CloudFront console per creare una distribuzione.

Panoramica di

1. Crea uno o più bucket Amazon S3 oppure configura server HTTP come server di origine. Per origine si intende la posizione in cui viene archiviata la versione originale dei contenuti. Quando CloudFront riceve una richiesta per i tuoi file, passa all'origine per ottenere i file che distribuisce nelle edge location. Puoi utilizzare una qualsiasi combinazione di bucket Amazon S3 e server HTTP come server di origine.

   - Se utilizzi Amazon S3, il nome di bucket deve essere tutto in minuscolo e non deve includere spazi.
   - Se utilizzi un EC2 server Amazon o un'altra origine personalizzata, consultaUsa Amazon EC2 (o un'altra origine personalizzata).
   - Per il numero massimo corrente di origini che puoi creare per una distribuzione o per richiedere una quota più elevata, consulta Quote generali sulle distribuzioni.

2. Carica il contenuto nei server di origine. Rendi i tuoi oggetti leggibili pubblicamente oppure puoi usare CloudFront signed URLs per limitare l'accesso ai tuoi contenuti.

   > **Important**
   >
   > È tua responsabilità garantire la protezione del tuo server di origine. Devi assicurarti di avere il CloudFront permesso di accedere al server e che le impostazioni di sicurezza salvaguardino i tuoi contenuti.

3. Crea la tua CloudFront distribuzione:

   - Per una procedura dettagliata per creare una distribuzione nella CloudFront console, consultaCrea una CloudFront distribuzione nella console.
   - Per informazioni sulla creazione di una distribuzione utilizzando l' CloudFront API, CreateDistributionconsulta Amazon CloudFront API Reference.

4. (Facoltativo) Se utilizzi la CloudFront console per creare la tua distribuzione, crea più comportamenti o origini della cache per la distribuzione. Per ulteriori informazioni sui comportamenti e sulle origini, consulta Come aggiornare una distribuzione multi-tenant.

5. Esegui il test della distribuzione. Per ulteriori informazioni sull'esecuzione di test, consulta Esecuzione del test di una distribuzione.

6. Sviluppa il sito Web o l'applicazione per accedere al tuo contenuto utilizzando il nome di dominio che CloudFront ha restituito dopo la creazione della distribuzione nella fase 3. Ad esempio, se CloudFront restituisce d111111abcdef8.cloudfront.net come nome di dominio per la tua distribuzione, l'URL del file in un bucket `image.jpg` Amazon S3 o nella directory principale di un server HTTP è. `https://d111111abcdef8.cloudfront.net/image.jpg`

   Se hai specificato uno o più nomi di dominio alternativi (CNAMEs) quando hai creato la distribuzione, puoi usare il tuo nome di dominio. In tal caso, l'URL per `image.jpg` potrebbe essere `https://www.example.com/image.jpg`.

   Tenere presente quanto segue:

   - Se desideri utilizzare signed URLs per limitare l'accesso ai tuoi contenuti, consultaOffri contenuti privati con cookie firmati URLs e firmati.
   - Se desideri servire contenuto compresso, consulta Distribuzione di file compressi.
   - Per informazioni sul comportamento di CloudFront richiesta e risposta per Amazon S3 e sulle origini personalizzate, consulta. Comportamento di richieste e risposte

Argomenti

Crea una CloudFront distribuzione nella console

Quando crei una distribuzione, CloudFront configura automaticamente le impostazioni di distribuzione, in base al tipo di origine del contenuto. Per ulteriori dettagli sulle impostazioni preconfigurate, consulta Riferimento alle impostazioni di distribuzione preconfigurate. Puoi anche creare distribuzioni multi-tenant con impostazioni riutilizzabili su più tenant di distribuzione. Per ulteriori informazioni, consulta Comprendere il funzionamento delle distribuzioni multi-tenant. In alternativa, puoi configurare manualmente le impostazioni di distribuzione.

Multi-tenant

Come creare una distribuzione multi-tenant

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Distribuzioni, quindi scegli Crea distribuzione.
3. Scegli Architettura multi-tenant, Avanti.
4. Inserisci un Nome di distribuzione per la distribuzione multi-tenant. Il nome verrà visualizzato come valore per la chiave `Name`. Puoi modificare questo valore in un secondo momento. Puoi aggiungere fino a 50 tag per la distribuzione multi-tenant. Per ulteriori informazioni, consulta Tagging di una distribuzione.
5. (Facoltativo) Per il certificato Wildcard, scegli il certificato AWS Certificate Manager (ACM) che coprirà tutti i sottodomini del dominio principale, ad esempio. `*.example.com` Il certificato deve essere disponibile nella Regione Stati Uniti orientali (Virginia settentrionale).
6. Scegli Next (Successivo).
7. Nella pagina Specificare l'origine, seleziona il tipo di origine da cui CloudFront riceverai i tuoi contenuti. CloudFront utilizzerà le impostazioni consigliate per quel tipo di origine per la distribuzione multi-tenant. Per ulteriori informazioni sulle impostazioni consigliate, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

8. Per Origine, nel tipo di origine selezionato, scegli o inserisci l'origine da utilizzare.
9. Per Percorso origine, inserisci il carattere barra obliqua (/), seguito dal percorso di origine.
10. (Facoltativo) Per aggiungere un parametro, scegli Inserisci il parametro per il nome di dominio di origine o il percorso di origine. Puoi immettere fino a due parametri per ogni campo.

    a. Scegli Crea nuovo parametro.

    b. Nella finestra di dialogo Crea nuovo parametro, in Nome parametro, immetti un nome univoco per il parametro e, facoltativamente, una descrizione.

    c. Per Parametro obbligatorio, seleziona la casella di controllo per rendere obbligatorio questo valore del parametro a livello di tenant di distribuzione. Se non è obbligatorio, inserisci un Valore predefinito che verrà ereditato dal tenant di distribuzione.

    d. Scegli Create parameter (Crea parametro). Questo parametro viene visualizzato nel campo corrispondente.
11. Per Opzioni, scegli una delle seguenti opzioni:

    - Usa impostazioni di origine consigliate: utilizza le impostazioni predefinite consigliate della cache e dell'origine per il tipo di origine selezionato.
    - Personalizza impostazioni di origine: personalizza le impostazioni della cache e dell'origine. Se scegli questa opzione, specifica i valori da visualizzare.
12. Scegli Next (Successivo).
13. Nella pagina Abilita le protezioni di sicurezza, scegli se abilitare AWS WAF le protezioni di sicurezza. Puoi personalizzare l'ACL Web per tenant di distribuzione specifici in un secondo momento. Per ulteriori informazioni, consulta Abilitazione di AWS WAF per una nuova distribuzione.
14. Scegli Avanti, Crea distribuzione.
15. Nella pagina Distribuzioni, la distribuzione multi-tenant viene visualizzata nell'elenco delle risorse. Puoi scegliere il menu a discesa Tutte le distribuzioni per filtrare in base alla distribuzione standard o alla distribuzione multi-tenant. Puoi anche scegliere la colonna Tipo per filtrare in base alla distribuzione standard o multi-tenant.

Per impostazione predefinita, CloudFront crea automaticamente un gruppo di connessione. Il gruppo di connessione controlla il modo in cui si connettono le richieste di contenuto degli utenti CloudFront. Puoi personalizzare alcune impostazioni di instradamento nel gruppo di connessioni. Per ulteriori informazioni, consulta Comprendere il funzionamento delle distribuzioni multi-tenant.

Puoi creare tenant di distribuzione aggiuntivi utilizzando la distribuzione multi-tenant come modello.

Come creare una distribuzione tenant

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, esegui una delle seguenti operazioni:
   - Scegli Distribuzioni, seleziona una distribuzione multi-tenant, quindi scegli Crea tenant.
   - Seleziona Tenant di distribuzione, quindi scegli Crea tenant.
3. Per Nome del tenant di distribuzione, inserisci il nome. Il nome deve essere univoco nel tuo Account AWS account e non può essere modificato dopo averlo creato.
4. Per Distribuzione dei modelli, scegli un ID di distribuzione multi-tenant dall'elenco.
5. Per Gestisci tag, aggiungi fino a 50 coppie chiave-valore per il tenant di distribuzione. Per ulteriori informazioni, consulta Tagging di una distribuzione.
6. Scegli Next (Successivo).
7. Nella pagina Aggiungi domini, per Certificato, scegli se desideri un Certificato TLS personalizzato per il tenant di distribuzione. Il certificato verifica se disponi dell'autorizzazione per utilizzare il nome di dominio. Il certificato deve esistere nella Regione Stati Uniti orientali (Virginia settentrionale).
8. Per Domini, inserisci il nome di dominio.

   > **Note**
   >
   > Se hai inserito un nome di dominio non coperto da certificato, devi verificare di essere il proprietario del dominio. Per ora puoi comunque creare il tenant di distribuzione e verificare la proprietà del dominio in un secondo momento. Per ulteriori informazioni, consulta Richiedi i certificati per il tuo tenant CloudFront di distribuzione.

9. Scegli Next (Successivo).
10. Nella pagina Definisci parametri, vengono visualizzati i parametri specificati nella distribuzione multi-tenant. Per i parametri obbligatori, inserisci un valore accanto al nome del parametro e salva le modifiche.
11. Per aggiungere un altro parametro, scegli Aggiungi parametro e inserisci un nome e un valore.

12. Scegli Next (Successivo).
13. (Facoltativo) Per Personalizzazione della sicurezza, se scegli di sovrascrivere le impostazioni di distribuzione, seleziona l'opzione per il caso d'uso specifico.
14. (Facoltativo) Per Personalizzazione delle restrizioni geografiche, se scegli di sovrascrivere le impostazioni di distribuzione, seleziona il Tipo di restrizione e i Paesi appropriati per il tenant di distribuzione. Per ulteriori informazioni, consulta Limitazione della distribuzione geografica del contenuto.
15. Scegli Next (Successivo).
16. Scegli Crea tenant di distribuzione.

Puoi trovare tutti i tenant di distribuzione nella pagina Tenant di distribuzione. Puoi filtrare in base alle seguenti categorie:

Associazione

- ID distribuzione
- ID del certificato
- ID del gruppo di connessioni
- ID della lista di controllo accessi Web

Properties

- Name
- Dominio

Puoi modificare i tenant di distribuzione per personalizzare impostazioni specifiche. Per ulteriori informazioni, consulta Personalizzazioni dei tenant di distribuzione.

Standard

Come creare una distribuzione standard

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Distribuzioni, quindi scegli Crea distribuzione.

3. Immetti un Nome della distribuzione per la distribuzione standard. Il nome verrà visualizzato come valore per la chiave `Name` come un tag. Puoi modificare questo valore in un secondo momento. Puoi aggiungere fino a 50 tag per la distribuzione standard. Per ulteriori informazioni, consulta Tagging di una distribuzione.
4. Scegli Singolo sito web o app, Avanti.
5. (Facoltativo) Per la configurazione del dominio, inserisci un dominio già registrato con Route 53 nel tuo Account AWS o registra un nuovo dominio. Completa le fasi di configurazione.

   - Se il dominio utilizza un provider DNS diverso da Route 53, puoi comunque aggiungere il dominio, ma devi eseguire questa operazione dopo aver creato la distribuzione. Per ora, ignora la configurazione del dominio per procedere con la creazione della distribuzione. Devi configurare manualmente il dominio e il certificato TLS in un secondo momento. Per ulteriori informazioni, consulta Aggiungi un dominio alla tua distribuzione CloudFront standard.
6. Scegli Next (Successivo).
7. Nella pagina Specificare l'origine, seleziona il tipo di origine da cui CloudFront riceverai i tuoi contenuti. CloudFront utilizzerà le impostazioni consigliate per quel tipo di origine per la distribuzione. Per ulteriori informazioni sulle impostazioni consigliate, consulta Riferimento alle impostazioni di distribuzione preconfigurate.
8. Per Origine, scegli o inserisci l’origine.
9. Per Impostazioni, scegli una delle seguenti opzioni:

   - Usa impostazioni di origine consigliate: utilizza le impostazioni predefinite consigliate della cache e dell’origine per il tipo di origine selezionato.
   - Personalizza impostazioni di origine: personalizza le impostazioni della cache e dell’origine. Se scegli questa opzione, specifica i tuoi valori.
10. Scegli Next (Successivo).
11. Nella pagina Abilita le protezioni di sicurezza, scegli se abilitare le protezioni AWS WAF di sicurezza.
12. Scegli Next (Successivo).
13. (Facoltativo) Se utilizzi Route 53 per il dominio, viene visualizzata la pagina Certificato TLS. Se non CloudFront riesci a trovare un certificato AWS Certificate Manager (ACM) esistente per il tuo dominio Account AWS nel `us-east-1` Regione AWS, puoi scegliere di creare automaticamente un certificato o crearlo manualmente. Dopo aver creato il certificato, scegli Avanti.

14. Controlla i dettagli della distribuzione e scegli Crea distribuzione.
15. Dopo aver CloudFront creato la distribuzione, il valore della colonna Status per la distribuzione cambierà da Deploying alla data e all'ora di distribuzione della distribuzione.

    Il nome di dominio CloudFront assegnato alla distribuzione viene visualizzato nell'elenco delle distribuzioni. (questo viene visualizzato anche nella scheda General (Generale) per una distribuzione selezionata).

    > **Tip**
    >
    > Puoi utilizzare un nome di dominio alternativo, anziché il nome che ti è stato assegnato da CloudFront, seguendo la procedura riportata di seguito. Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs

16. Una volta implementata la distribuzione, conferma di poter accedere ai contenuti utilizzando il nuovo CloudFront URL (d111111abcdef8.cloudfront.net) o il CNAME. Per ulteriori informazioni, consulta Esecuzione del test di una distribuzione.
17. Assicurati di aggiornare i tuoi record DNS in modo che indichino quando sei pronto a inviare traffico alla tua distribuzione. CloudFront Per ulteriori informazioni, consulta Indirizza i domini a CloudFront (distribuzione standard).

Valori CloudFront visualizzati nella console

Quando crei una nuova distribuzione o aggiorni una distribuzione esistente, CloudFront visualizza le seguenti informazioni nella CloudFront console.

> **Note**
>
> I firmatari attendibili attivi, Account AWS che dispongono di una CloudFront key pair attiva e possono essere utilizzati per creare firme firmate valide URLs, attualmente non sono visibili nella CloudFront console.

ID distribuzione

Quando si esegue un'azione su una distribuzione utilizzando l' CloudFront API, si utilizza l'ID di distribuzione per specificare quale distribuzione utilizzare, `EDFDVBD6EXAMPLE` ad esempio. Non puoi modificare l'ID distribuzione di una distribuzione.

Implementazione e stato

Quando si implementa una distribuzione, viene visualizzato lo stato Implementazione in corso nella colonna Ultima modifica. Attendi che la distribuzione termini l'implementazione e assicurati che la colonna Stato indichi Abilitata. Per ulteriori informazioni, consulta Distribution State (Stato distribuzione).

Ultima modifica

La data e l'ora dell'ultima modifica della distribuzione, espressa nel formato ISO 8601; ad esempio, 2012-05-19T19:37:58Z. Per ulteriori informazioni, consulta https://www.w3.org/TR/NOTE-datetime.

Domain name (Nome dominio)

Puoi utilizzare il nome di dominio della distribuzione nei collegamenti agli oggetti. Ad esempio, se il nome di dominio della distribuzione è `d111111abcdef8.cloudfront.net`, il collegamento a `/images/image.jpg` sarebbe `https://d111111abcdef8.cloudfront.net/images/image.jpg`. Non puoi modificare il nome di dominio di CloudFront per la tua distribuzione. Per ulteriori informazioni sui CloudFront URLs collegamenti ai tuoi oggetti, consultaPersonalizzazione del formato URL per i file in CloudFront.

Se avete specificato uno o più nomi di dominio alternativi (CNAMEs), potete utilizzare i vostri nomi di dominio per i collegamenti agli oggetti anziché utilizzare il nome di CloudFront dominio. Per ulteriori informazioni su CNAMEs, vedereNomi di dominio alternativi () CNAMEs.

> **Note**
>
> CloudFront i nomi di dominio sono unici. Il nome di dominio della tua distribuzione non è mai stato utilizzato per una distribuzione precedente e non sarà mai riutilizzato per un'altra distribuzione in futuro.

Link aggiuntivi

Per ulteriori informazioni sulla creazione di una distribuzione, consulta i link seguenti.

- Per informazioni su come creare una distribuzione che utilizza un'origine bucket Amazon Simple Storage Service (Amazon S3) con controllo di accesso origine (OAC), consulta Inizia con una distribuzione CloudFront standard.

- Per informazioni sull'utilizzo di CloudFront APIs per creare una distribuzione, CreateDistributionconsulta Amazon CloudFront API Reference.
- Per informazioni sull'aggiornamento di una distribuzione (ad esempio, per aggiungere comportamenti cache alle distribuzioni standard o per personalizzare i tenant di distribuzione), consulta Aggiornamento di una distribuzione.
- Per visualizzare il numero massimo corrente di distribuzioni che puoi creare per ogni AWS account o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote generali sulle distribuzioni.

Aggiungi un dominio alla tua distribuzione CloudFront standard

Dopo aver creato una nuova distribuzione CloudFront standard, puoi aggiungervi un dominio. Facoltativamente, puoi configurare un dominio Amazon Route 53 per la distribuzione standard al momento della creazione. Per ulteriori informazioni, consulta Crea una CloudFront distribuzione nella console.

Aggiunta di un dominio alla distribuzione standard esistente

Come aggiungere un dominio alla distribuzione standard

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi scegli l'ID distribuzione.
3. In Impostazioni, Nomi di dominio alternativi, scegli Aggiungi un dominio.
4. Inserisci fino a cinque domini da servire.
5. Scegli Next (Successivo).
6. Per quanto riguarda il certificato TLS, se non CloudFront riesci a trovare un certificato AWS Certificate Manager (ACM) esistente per il tuo dominio Account AWS nel tuo sito `us-east-1` Regione AWS, puoi crearne uno.
   - Se utilizzi Amazon Route 53 (Route 53), crea CloudFront automaticamente un certificato per te.
7. Una volta effettuato il provisioning del certificato, devi aggiornare i record DNS con il provider DNS per dimostrare la proprietà del dominio. Quindi, scegli Convalida certificato. Per ulteriori informazioni, consulta Indirizza i domini a CloudFront (distribuzione standard).

- Se utilizzi Route 53, CloudFront aggiorna i tuoi record DNS per te.

8. Scegli Next (Successivo).
9. Rivedi le modifiche e scegli Aggiungi domini.
10. Prima di inviare traffico alla tua distribuzione, assicurati di aggiornare i record DNS in modo che puntino a. CloudFront Per ulteriori informazioni, scegli Indirizza i domini CloudFront nella sezione Impostazioni della pagina dei dettagli di distribuzione.

    - Se utilizzi Route 53, puoi CloudFront configurare automaticamente il routing DNS.

Indirizza i domini a CloudFront (distribuzione standard)

Aggiorna i tuoi record DNS per indirizzare il traffico da ogni dominio al CloudFront nome host. Puoi avere più nomi di dominio, ma devono tutti risolversi in questo nome host.

Indirizzare i domini a CloudFront

1. Copia il valore del CloudFront nome host, ad esempio d111111abcdef8.cloudfront.net.
2. Aggiorna i tuoi record DNS per indirizzare il traffico da ogni dominio all'hostname. CloudFront

    1. Accedi al registrar di domini o console di gestione del provider DNS.
    2. Passa alla sezione Gestione DNS del dominio.
        - Per i sottodomini: crea un record CNAME. Esempio:
            - Nome: il sottodominio (ad esempio, `www` o `app`)
            - Value/Target: il tuo hostname CloudFront
            - Tipo di record: CNAME
            - TTL: 3600 (o qualsiasi altro valore appropriato per il caso d’uso)
        - Per i apex/root domini: ciò richiede una configurazione DNS unica, poiché i record CNAME standard non possono essere utilizzati a livello di dominio root o apex. Poiché la maggior parte dei provider DNS non supporta i record ALIAS, è consigliabile creare un record ALIAS in Route 53. Esempio:
            - Nome: il dominio apex (ad esempio `example.com`)
            - Tipo di record: A
            - Alias: Sì
            - Alias target: il tuo hostname CloudFront

- Policy di instradamento: semplice (o quella appropriata per il caso d'uso)

3. Verifica che la modifica del DNS sia stata propagata. (Questo di solito accade quando il TTL è scaduto. A volte possono essere necessarie 24-48 ore.) Usa uno strumento come `dig` o `nslookup`.

```
dig www.example.com
# Should eventually return a CNAME pointing to your CloudFront hostname
```

3. Torna alla CloudFront console e scegli Invia. Quando il dominio è attivo, CloudFront aggiorna lo stato del dominio per indicare che il dominio è pronto a servire il traffico.

Per ulteriori informazioni, consulta la documentazione relativa al provider DNS:

- Cloudflare
- ClouDNS
- DNSimple
- Gandi.net
- GoDaddy
- Google Cloud DNS
- Nome a buon mercato

Riferimento alle impostazioni di distribuzione preconfigurate

Quando crei la tua CloudFront distribuzione, configura CloudFront automaticamente la maggior parte delle impostazioni di distribuzione, in base al tipo di origine del contenuto. Facoltativamente, puoi scegliere di modificare manualmente le impostazioni di distribuzione. Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.

Nelle sezioni seguenti vengono descritte le impostazioni di preconfigurazione predefinite per le distribuzioni e le impostazioni che puoi personalizzare.

Origine Amazon S3

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l'origine Amazon S3 in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Origin Access Control (solo console): lo CloudFront configura automaticamente. CloudFront tenta di aggiungere la policy del bucket S3 per le distribuzioni standard e per le distribuzioni multi-tenant senza parametri utilizzati nel dominio di origine.
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3

Di seguito sono riportate le impostazioni della cache CloudFront preconfigurate per l'origine Amazon S3 in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì
- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD`
- Limita accesso visualizzatore: No
- Policy della cache: `CachingOptimized`
- Policy di richiesta origine: Nessuna
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: no
- Funzioni: No

Di seguito sono riportate le impostazioni che è possibile personalizzare per l’origine Amazon S3 in una distribuzione multi-tenant.

Impostazioni personalizzabili

- Accesso S3: lo CloudFront imposta automaticamente, in base alle impostazioni del bucket S3:
  - Se il bucket è pubblico: non è necessaria alcuna policy di controllo di accesso origine (OAC).
  - Se il bucket è privato: puoi scegliere o creare una policy OAC da utilizzare.

- Abilita Origin Shield: no
- Comprimi oggetti automaticamente: Sì
  - Se scegli Sì, viene utilizzata la policy di caching `CachingOptimized`.
  - Se scegli No, viene utilizzata la policy di caching `CachingOptimizedForUncompressedObjects`.

Origine Gateway API

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l'origine dell'API Gateway in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Protocollo: Solo HTTPS
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: Nessuno
- Origin Access Control (solo console): CloudFront lo configura automaticamente
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache che CloudFront preconfigurano l'origine dell'API Gateway in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì
- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Metodi HTTP della cache: No

- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Policy della cache: `CachingDisabled` (valori possibili: `UseOriginCacheControlHeaders`, `UseOriginCacheControlHeaders-QueryStrings`)
- Policy di richiesta origine: `AllViewerExceptHostHeader` (valori possibili: `AllViewer`, `AllViewerandCloudFrontHeaders-2022-06`)
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

Di seguito sono riportate le impostazioni che puoi personalizzare per l'origine Gateway API in una distribuzione multi-tenant.

Impostazioni personalizzabili

- Abilita Origin Shield: (impostazione predefinita: No)
- Comprimi oggetti automaticamente: (impostazione predefinita: Sì)

Origine e EC2 istanza personalizzate

Di seguito sono riportate le impostazioni di origine CloudFront preconfigurate per l'origine personalizzata in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Protocollo: Visualizzatore corrispondente
- Porta HTTP: 80
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: Nessuno
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No

- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache che CloudFront preconfigurano l'origine e l' EC2 istanza personalizzate in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì
- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Metodi HTTP della cache: No
- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Policy della cache: `UseOriginCacheControlHeaders` (valori possibili: `UseOriginCacheControlHeaders-QueryStrings`, `CachingDisabled`, `CacheOptimized`, `CachingOptimizedForUncompressedObjects`)
- Policy di richiesta origine: `AllViewer` (valori possibili: `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

Di seguito sono riportate le impostazioni che è possibile personalizzare per l'origine e l' EC2 istanza personalizzate in una distribuzione multi-tenant.

Impostazioni personalizzabili

- Abilita Origin Shield: (impostazione predefinita: No)
- Comprimi oggetti automaticamente: (impostazione predefinita: Sì)

- Caching: (impostazione predefinita: `Cache by Default`)
  - Se `Cache by Default` è selezionata, viene utilizzata la policy della cache `UseOriginCacheControlHeaders`.
  - Se `Do Not Cache by Default` è selezionata, viene utilizzata la policy della cache `CachingDisabled`.
- Includi la stringa di query nella cache: (impostazione predefinita: Sì, se `Cache by Default` è già selezionata)
  - Se `Do Not Cache by Default` è già selezionata e scegli di includere la stringa di query nella cache, viene utilizzata la policy della cache `UseOriginCacheControlHeaders-QueryStrings`.

Origine ELB

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l'origine ELB in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Protocollo: Solo HTTPS
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: Nessuno
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache che CloudFront preconfigurano l'origine ELB in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì

- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Metodi HTTP della cache: No
- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Caching: (impostazione predefinita: `Cache by Default`)
  - Se `Cache by Default` è selezionata, viene utilizzata la policy della cache `UseOriginCacheControlHeaders`.
  - Se `Do Not Cache by Default` è selezionata, viene utilizzata la policy della cache `CachingDisabled`.
- Includi la stringa di query nella cache: (impostazione predefinita: Sì, se `Cache by Default` è già selezionata)
  - Se `Do Not Cache by Default` è già selezionata e scegli di includere la stringa di query nella cache, viene utilizzata la policy della cache `UseOriginCacheControlHeaders-QueryStrings`.
- Policy di richiesta origine: `All Viewer` (valori possibili: `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

Di seguito sono riportate le impostazioni che è possibile personalizzare per l'origine ELB in una distribuzione multi-tenant.

Impostazioni personalizzabili

- Abilita Origin Shield: (impostazione predefinita: No)
- Comprimi oggetti automaticamente: (impostazione predefinita: Sì)
- Caching: (impostazione predefinita: `Cache by Default`)
  - Se `Cache by Default` è selezionata, viene utilizzata la policy della cache `UseOriginCacheControlHeaders`.

  - Se `Do Not Cache by Default` è selezionata, viene utilizzata la policy della cache `CachingDisabled`.
- Includi la stringa di query nella cache: (impostazione predefinita: Sì, se `Cache by Default` è già selezionata)
  - Se `Do Not Cache by Default` è già selezionata e scegli di includere la stringa di query nella cache, viene utilizzata la policy della cache `UseOriginCacheControlHeaders-QueryStrings`.

MediaPackage origine v1

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l'origine MediaPackage v1 in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Protocollo: Solo HTTPS
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: lo fornisci inserendo il tuo MediaPackage URL.
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache che CloudFront preconfigurano l'origine MediaPackage v1 in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì
- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD`
- Metodi HTTP della cache: No

- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Policy della cache: `Elemental-MediaPackage`
- Policy di richiesta origine: Nessuna
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

MediaPackage origine v2

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l'origine MediaPackage v2 in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Origin Access Control: lo CloudFront configura per te e aggiunge la politica
- Protocollo: Solo HTTPS
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: Nessuno
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache CloudFront preconfigurate per l'origine MediaPackage v2 in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì

- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD`
- Metodi HTTP della cache: No
- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Policy della cache: `Elemental-MediaPackage`
- Policy di richiesta origine: Nessuna
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

MediaTailor origine

Di seguito sono riportate le impostazioni di origine che CloudFront preconfigurano l' MediaTailor origine in una distribuzione multi-tenant.

Impostazioni di origine (preconfigurate)

- Protocollo: Solo HTTPS
- Porta HTTPS: 443
- Protocollo SSL di origine minima: 2. TLSv1
- Percorso di origine: lo fornisci inserendo il tuo MediaPackage URL.
- Aggiungi intestazione personalizzata: Nessuna
- Abilita Origin Shield: No
- Tentativi di connessione: 3
- Timeout di risposta: 30
- Timeout keep-alive: 5

Di seguito sono riportate le impostazioni della cache che CloudFront preconfigurano l' MediaTailor origine in una distribuzione multi-tenant.

Impostazioni della cache (preconfigurate)

- Comprimi oggetti automaticamente: Sì
- Policy del protocollo del visualizzatore: Reindirizza a HTTPS
- Metodi HTTP consentiti: `GET, HEAD`
- Metodi HTTP della cache: No
- Consentire richieste gRPC su HTTP/2: No
- Limita accesso visualizzatore: No
- Policy della cache: Nessuna
- Policy di richiesta origine: `Elemental-MediaTailor-PersonalizedManifests`
- Policy di intestazione della risposta: Nessuna
- Smooth Streaming: No
- Crittografia a livello di campo: No
- Abilita i log di accesso in tempo reale: No
- Funzioni: No

Riferimento a tutte le impostazioni di distribuzione

Puoi scegliere di modificare manualmente le impostazioni di CloudFront distribuzione quando crei o aggiorni la distribuzione. Di seguito sono riportate le impostazioni che puoi modificare.

Tuttavia, CloudFront configura automaticamente la maggior parte delle impostazioni di distribuzione, in base al tipo di origine del contenuto. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

Per ulteriori informazioni sulla creazione o l'aggiornamento di una distribuzione utilizzando la console CloudFront, consulta the section called “Creazione di una distribuzione” o the section called “Aggiornamento di una distribuzione”.

Argomenti

- Restrizioni geografiche

Origin Settings (Impostazioni di origine)

Quando utilizzi la CloudFront console per creare o aggiornare una distribuzione, fornisci informazioni su una o più posizioni, note come origini, in cui archivi le versioni originali dei tuoi contenuti web. CloudFront recupera i tuoi contenuti web dalle tue origini e li fornisce agli utenti tramite una rete mondiale di server periferici.

Per il numero massimo corrente di origini che puoi creare per una distribuzione o per richiedere una quota più elevata, consulta the section called “Quote generali sulle distribuzioni”.

Se desideri eliminare un'origine, devi dapprima modificare o eliminare i comportamenti cache associati a tale origine.

> **Important**
>
> Se elimini un'origine, verifica che i file precedentemente serviti da quell'origine sono disponibili in un'altra origine e che i comportamenti cache instradano le richieste per quei file alla nuova origine.

Quando crei o aggiorni una distribuzione, specifichi i valori seguenti per ogni origine.

Argomenti

- Dominio origine
- Protocollo (solo origini personalizzate)
- Percorso origine
- Name
- Accesso all'origine (solo origini Amazon S3)
- Aggiunta di intestazioni personalizzate
- Abilitazione di Origin Shield
- Tentativi di connessione
- Timeout di connessione
- Timeout di risposta
- Timeout completamento risposta

- Timeout keep-alive (solo origini personalizzate e VPC)
- Quote timeout di risposta e keep-alive

Dominio origine

Il dominio di origine è il nome di dominio DNS della risorsa da cui CloudFront verranno ottenuti gli oggetti per la tua origine, come un bucket Amazon S3 o un server HTTP. Esempio:

- Bucket Amazon S3 – *amzn-s3-demo-bucket*.s3.*us-west-2*.amazonaws.com

> **Note**
>
> Se hai creato di recente il bucket S3, la CloudFront distribuzione potrebbe restituire `HTTP 307 Temporary Redirect` risposte per un massimo di 24 ore. Possono essere necessarie fino a 24 ore prima che il nome del bucket S3 si propaghi a tutte le regioni AWS . Quando la propagazione è completa, la distribuzione interrompe automaticamente l'invio di queste risposte di reindirizzamento; non è necessario intraprendere alcuna operazione. Per ulteriori informazioni, vedere Perché ricevo una risposta di reindirizzamento temporaneo HTTP 307 da Amazon S3? e Reindirizzamento delle richieste temporanee.

- Bucket Amazon S3 configurato come sito Web – *amzn-s3-demo-bucket*.s3-website.*us-west-2*.amazonaws.com
- MediaStore contenitore — *examplemediastore*.data.mediastore.*us-west-1*.amazonaws.com
- MediaPackage punto finale — *examplemediapackage*.mediapackage.*us-west-1*.amazonaws.com
- EC2 Istanza Amazon: *ec2-203-0-113-25*.compute-1.amazonaws.com
- Bilanciatore di carico ELB — *example-load-balancer-1234567890*.*us-west-2*.elb.amazonaws.com
- Il tuo server web – `www.example.com`

Scegli il nome di dominio nel campo Origin Domain Name (Nome dominio origine) o digita il nome. Le risorse delle Regioni di adesione devono essere inserite manualmente. Il nome di dominio non fa distinzione tra maiuscole e minuscole. Il dominio di origine deve avere un nome DNS risolvibile pubblicamente che instrada le richieste dai client alle destinazioni su Internet.

Se configuri la connessione CloudFront all'origine tramite HTTPS, uno dei nomi di dominio nel certificato deve corrispondere al nome di dominio specificato per Origin Domain Name. Se nessun nome di dominio corrisponde, CloudFront restituisce il codice di stato HTTP 502 (Bad Gateway) al visualizzatore. Per ulteriori informazioni, consultare Nomi di dominio nella CloudFront distribuzione e nel certificato e Errore di negoziazione SSL/TLS tra e un server di origine personalizzato CloudFront .

> **Note**
>
> Se si utilizza una policy di richiesta di origine che inoltra l'intestazione host del visualizzatore all'origine, l'origine deve rispondere con un certificato che corrisponda all'intestazione host del visualizzatore. Per ulteriori informazioni, consulta Aggiunta di intestazioni della richiesta CloudFront.

Se la tua origine è un bucket Amazon S3, tieni presente quanto segue:

- Se il bucket è configurato come un sito Web, inserisci l'endpoint di hosting del sito Web statico di Simple Storage Service (Amazon S3) per il bucket; non selezionare il nome del bucket dall'elenco nel campo Origin Domain (Dominio origine). L'endpoint di hosting del sito Web statico è visualizzato nella console di Simple Storage Service (Amazon S3), nella pagina Properties (Proprietà) sotto Static Website Hosting (Hosting sito Web statico). Per ulteriori informazioni, consulta the section called "Utilizzo di un bucket Amazon S3 configurato come un endpoint del sito web".
- Se hai configurato Amazon S3 Transfer Acceleration per il bucket, non specificare l'endpoint `s3-accelerate` per Origin Domain Name (Nome dominio origine).
- Se stai utilizzando un bucket di un altro AWS account e se il bucket non è configurato come sito Web, inserisci il nome utilizzando il seguente formato:

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

  Se il bucket si trova nella Regione degli Stati Uniti e vuoi che Amazon S3 instradi le richieste a una struttura in Virginia settentrionale, utilizza il seguente formato:

  bucket-name`.s3.us-east-1.amazonaws.com`
- I file devono essere leggibili pubblicamente a meno che non protegga i contenuti in Amazon S3 utilizzando CloudFront un controllo di accesso all'origine. Per ulteriori informazioni sul controllo degli accessi, consulta the section called "Limitazione dell'accesso a un'origine Amazon S3".

> **Important**
>
> Se l'origine è un bucket Amazon S3, il nome di bucket deve essere conforme ai requisiti di denominazione DNS. Per ulteriori informazioni, consultare Restrizioni e limitazioni dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Quando modifichi il valore del dominio Origin per un'origine, inizia CloudFront immediatamente a replicare la modifica nelle edge location. CloudFront Fino a quando la configurazione di distribuzione non viene aggiornata in una determinata edge location, CloudFront continua a inoltrare le richieste all'origine precedente. Non appena la configurazione di distribuzione viene aggiornata in quella edge location, CloudFront inizia a inoltrare le richieste alla nuova origine.

La modifica dell'origine non richiede CloudFront di ripopolare le cache edge con oggetti della nuova origine. Se le richieste visualizzatore nella tua applicazione non vengono modificate, CloudFront continua a distribuire oggetti già presenti in una cache edge fino alla scadenza del TTL di ogni oggetto o fino a che gli oggetti richiesti raramente non vengono rimossi.

Protocollo (solo origini personalizzate)

> **Note**
>
> Si applica solo alle origini personalizzate.

La politica del protocollo che desideri utilizzare CloudFront per recuperare oggetti dalla tua origine.

Seleziona uno dei seguenti valori:

- Solo HTTP: CloudFront utilizza solo HTTP per accedere all'origine.

> **Important**
>
> HTTP only (Solo HTTP) è l'impostazione di default quando l'origine è un endpoint di hosting di siti Web statici Simple Storage Service (Amazon S3), perché Simple Storage Service (Amazon S3) non supporta le connessioni HTTPS per gli endpoint di hosting di siti Web statici. La CloudFront console non supporta la modifica di questa impostazione per gli endpoint di hosting di siti Web statici di Amazon S3.

- Solo HTTPS: CloudFront utilizza solo HTTPS per accedere all'origine.
- Match viewer: CloudFront comunica con l'origine tramite HTTP o HTTPS, a seconda del protocollo della richiesta del visualizzatore. CloudFront memorizza l'oggetto nella cache una sola volta anche se i visualizzatori effettuano richieste utilizzando entrambi i protocolli HTTP e HTTPS.

> **Important**
>
> Per le richieste dei visualizzatori HTTPS che vengono CloudFront inoltrate a questa origine, uno dei nomi di dominio nel SSL/TLS certificato sul server di origine deve corrispondere al nome di dominio specificato per il dominio di origine. Altrimenti, CloudFront risponde alle richieste del visualizzatore con un codice di stato HTTP 502 (Bad Gateway) anziché restituire l'oggetto richiesto. Per ulteriori informazioni, consulta the section called “Requisiti per l'utilizzo di certificati con SSL/TLS CloudFront”.

Argomenti

Porta HTTP

> **Note**
>
> Si applica solo alle origini personalizzate.

(Facoltativo) È possibile specificare la porta HTTP su cui ascolta l'origine personalizzata. I valori validi includono le porte 80, 443 e da 1024 a 65535. Il valore predefinito è la porta 80.

> **Important**
>
> La porta 80 è l'impostazione predefinita quando l'origine è un endpoint di hosting di siti Web Amazon S3 statici, poiché Amazon S3 supporta solo la porta 80 per gli endpoint di hosting di siti Web statici. La CloudFront console non supporta la modifica di questa impostazione per gli endpoint di hosting di siti Web statici di Amazon S3.

Porta HTTPS

> **Note**
>
> Si applica solo alle origini personalizzate.

(Facoltativo) È possibile specificare la porta HTTPS su cui ascolta l'origine personalizzata. I valori validi includono le porte 80, 443 e da 1024 a 65535. Il valore predefinito è la porta 443. Quando Protocol (Protocollo) è impostato su HTTP only (Solo HTTP), non è possibile specificare un valore per HTTPS port (Porta HTTPS).

Protocollo SSL di origine minimo

> **Note**
>
> Si applica solo alle origini personalizzate.

Scegli il TLS/SSL protocollo minimo da CloudFront utilizzare quando stabilisce una connessione HTTPS con la tua origine. Protocolli TLS inferiori sono meno sicuri, pertanto ti consigliamo di scegliere il protocollo TLS più recente supportato dall'origine. Quando Protocol (Protocollo) è impostato su HTTP only (Solo HTTP), non è possibile specificare un valore per Minimum origin SSL protocol (Protocollo SSL di origine minimo).

Se utilizzi l' CloudFront API per impostare il TLS/SSL protocollo CloudFront da utilizzare, non puoi impostare un protocollo minimo. Devi invece specificare tutti i TLS/SSL protocolli che CloudFront puoi utilizzare con la tua origine. Per ulteriori informazioni, OriginSslProtocolsconsulta Amazon CloudFront API Reference.

Percorso origine

Se desideri richiedere CloudFront i tuoi contenuti da una directory nella tua cartella di origine, inserisci il percorso della directory, che inizia con una barra (/). CloudFront aggiunge il percorso della directory al valore del dominio Origin, ad esempio. **`cf-origin.example.com/production/images`** Non aggiungere una barra (/) alla fine del percorso.

Ad esempio, supponiamo che siano stati specificati i seguenti valori per la distribuzione:

- Origin domain (Dominio origine): un bucket Simple Storage Service (Amazon S3) denominato **`amzn-s3-demo-bucket`**
- Origin Path (Percorso origine): **`/production`**
- Alternate domain names (CNAME) (Nomi di dominio alternativi (CNAME): **`example.com`**

Quando un utente entra `example.com/index.html` in un browser, CloudFront invia una richiesta ad Amazon S3 per. `amzn-s3-demo-bucket/production/index.html`

Quando un utente entra `example.com/acme/index.html` in un browser, CloudFront invia una richiesta ad Amazon S3 per. `amzn-s3-demo-bucket/production/acme/index.html`

Name

Un nome è una stringa che identifica in modo univoco questa origine in questa distribuzione. Se crei comportamenti di cache oltre al comportamento predefinito della cache, usi il nome che specifichi qui per identificare l'origine a cui vuoi CloudFront indirizzare una richiesta quando la richiesta corrisponde al modello di percorso per quel comportamento di cache.

Accesso all'origine (solo origini Amazon S3)

> **Note**
>
> Si applica solo alle origini del bucket Amazon S3, quelle che non utilizzano l'endpoint del sito Web statico S3.

Scegli le impostazioni di controllo degli accessi di Origin (consigliato) se desideri consentire di limitare l'accesso a un'origine di bucket Amazon S3 solo a distribuzioni specifiche. CloudFront

Scegli Pubblico se l'origine del bucket Amazon S3 è accessibile al pubblico.

Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

Per informazioni su come richiedere agli utenti di accedere agli oggetti su un'origine personalizzata solo CloudFront URLs utilizzando, consulta. the section called “Limitazione dell’accesso ai file su origini personalizzate”

Aggiunta di intestazioni personalizzate

Se desideri CloudFront aggiungere intestazioni personalizzate ogni volta che invia una richiesta all'origine, specifica il nome dell'intestazione e il relativo valore. Per ulteriori informazioni, consulta the section called “Aggiunta di intestazioni personalizzate alle richieste di origine”.

Per conoscere il numero massimo corrente di intestazioni personalizzate che è possibile aggiungere, la lunghezza massima del nome e del valore di un'intestazione personalizzata e la lunghezza totale massima di tutti i nomi e i valori di intestazione, consulta Quote.

Abilitazione di Origin Shield

Scegli Sì per abilitare CloudFront Origin Shield. Per ulteriori informazioni sul Origin Shield, consulta the section called “Utilizzo di Origin Shield”.

Tentativi di connessione

Puoi impostare il numero di volte in cui CloudFront tenta di connettersi all'origine. È possibile specificare 1, 2 o 3 come numero di tentativi. Il numero predefinito (se non si specifica diversamente) è 3.

Utilizzate questa impostazione insieme a Connection timeout per specificare quanto tempo occorre CloudFront attendere prima di tentare di connettersi all'origine secondaria o restituire una risposta di errore al visualizzatore. Per impostazione predefinita, CloudFront attende fino a 30 secondi (3 tentativi da 10 secondi ciascuno) prima di tentare di connettersi all'origine secondaria o restituire una risposta di errore. È possibile ridurre questo tempo specificando un minor numero di tentativi, un timeout di connessione più breve o entrambi.

Se il numero specificato di tentativi di connessione fallisce, CloudFront esegue una delle seguenti operazioni:

- Se l'origine fa parte di un gruppo di origine, CloudFront tenta di connettersi all'origine secondaria. Se il numero specificato di tentativi di connessione all'origine secondaria fallisce, CloudFront restituisce una risposta di errore al visualizzatore.
- Se l'origine non fa parte di un gruppo di origine, CloudFront restituisce una risposta di errore al visualizzatore.

Per un'origine personalizzata (incluso un bucket Amazon S3 configurato con hosting di siti Web statici), questa impostazione specifica anche il numero di volte in cui si CloudFront tenta di ottenere una risposta dall'origine. Per ulteriori informazioni, consulta the section called “Timeout di risposta”.

Timeout di connessione

Il timeout di connessione è il numero di secondi che CloudFront attendono quando si tenta di stabilire una connessione all'origine. È possibile specificare un numero di secondi compreso tra 1 e 10 (inclusi). Il timeout predefinito (se non si specifica diversamente) è di 10 secondi.

Utilizzate questa impostazione insieme ai tentativi di connessione per specificare i tempi di CloudFront attesa prima di tentare di connettersi all'origine secondaria o prima di restituire una risposta di errore al visualizzatore. Per impostazione predefinita, CloudFront attende fino a 30 secondi (3 tentativi da 10 secondi ciascuno) prima di tentare di connettersi all'origine secondaria o restituire una risposta di errore. È possibile ridurre questo tempo specificando un minor numero di tentativi, un timeout di connessione più breve o entrambi.

Se CloudFront non stabilisce una connessione all'origine entro il numero di secondi specificato, CloudFront esegue una delle seguenti operazioni:

- Se il numero specificato di tentativi di connessione è superiore a 1, CloudFront riprova a stabilire una connessione. CloudFront prova fino a 3 volte, in base al valore dei tentativi di connessione.
- Se tutti i tentativi di connessione non riescono e l'origine fa parte di un gruppo di origine, CloudFront tenta di connettersi all'origine secondaria. Se il numero specificato di tentativi di connessione all'origine secondaria fallisce, CloudFront restituisce una risposta di errore al visualizzatore.
- Se tutti i tentativi di connessione falliscono e l'origine non fa parte di un gruppo di origine, CloudFront restituisce una risposta di errore al visualizzatore.

Timeout di risposta

Il timeout di risposta origine, noto anche come timeout di lettura origine o timeout di richiesta origine, si applica a entrambi i valori seguenti:

- Quanto tempo (in secondi) CloudFront attende una risposta dopo l'inoltro di una richiesta all'origine.
- Quanto tempo (in secondi) CloudFront attende dopo aver ricevuto un pacchetto di risposta dall'origine e prima di ricevere il pacchetto successivo.

> **Tip**
>
> Se desideri aumentare il valore di timeout perché si stanno verificando errori con codice di stato HTTP 504, prendi in considerazione la possibilità di individuare altri metodi per eliminare questi errori prima di modificare il valore di timeout. Consulta i suggerimenti per la risoluzione dei problemi in the section called “Codice di stato HTTP 504 (Timeout del gateway)”.

CloudFront il comportamento dipende dal metodo HTTP nella richiesta del visualizzatore:

- `GET`e `HEAD` richieste: se l'origine non risponde o smette di rispondere entro la durata del timeout di risposta, CloudFront interrompe la connessione. CloudFront riprova a connettersi in base al valore di. the section called “Tentativi di connessione”
- `DELETE`,`OPTIONS`, `PATCH`PUT, e `POST` richieste: se l'origine non risponde per la durata del timeout di lettura, CloudFront interrompe la connessione e non riprova a contattare l'origine. Il client può inoltrare nuovamente la richiesta, se necessario.

Timeout completamento risposta

> **Note**
>
> Il timeout completamento risposta non supporta la funzionalità di implementazione continua.

Il tempo (in secondi) in cui una richiesta dall' CloudFront origine può rimanere aperta e attendere una risposta. Se la risposta completa non viene ricevuta dall'origine entro quest'ora, CloudFront termina la connessione.

A differenza del timeout di risposta, che è il tempo di attesa per i singoli pacchetti di risposta, il timeout di completamento della risposta è il tempo massimo consentito di CloudFront attesa per il completamento della risposta. Puoi utilizzare questa impostazione per assicurarti che CloudFront non attenda all'infinito un'origine lenta o che non risponde, anche se altre impostazioni di timeout consentono un'attesa più lunga.

Questo timeout massimo include quanto specificato per altre impostazioni di timeout e il numero di Tentativi di connessione per ogni nuovo tentativo. Puoi utilizzare queste impostazioni insieme per specificare quanto tempo di CloudFront attesa per la richiesta completa e quando terminare la richiesta, indipendentemente dal fatto che sia completa o meno.

Ad esempio, se utilizzi le seguenti impostazioni:

- Tentativi di connessione: 3
- Timeout connessione è 10 secondi
- Timeout di risposta è 30 secondi
- Timeout completamento risposta è 60 secondi

Ciò significa che CloudFront cercherà di connettersi all'origine (fino a 3 tentativi totali), con un timeout di ogni tentativo di connessione di 10 secondi. Una volta connesso, CloudFront aspetterà fino a 30 secondi affinché l'origine risponda alla richiesta fino a quando non riceve l'ultimo pacchetto della risposta.

Indipendentemente dal numero di tentativi di connessione o dal timeout di risposta, CloudFront interromperà la connessione se la risposta completa dall'origine impiega più di 60 secondi per essere completata. CloudFront restituirà quindi al visualizzatore una risposta di the section called “Codice di stato HTTP 504 (Timeout del gateway)” errore o una risposta di errore personalizzata, se ne hai specificata una.

> **Note**
>
> - L’eventuale valore impostato per il timeout completamento risposta deve essere uguale o superiore al valore per il timeout di risposta (timeout lettura origine).
> - Se non si imposta un valore per il timeout di completamento della risposta, CloudFront non impone un valore massimo.

Timeout keep-alive (solo origini personalizzate e VPC)

Il timeout keep-alive indica per quanto tempo (in secondi) CloudFront tenta di mantenere una connessione all'origine personalizzata dopo aver ricevuto l'ultimo pacchetto di una risposta. Una connessione permanente consente di risparmiare il tempo necessario a ristabilire la connessione TCP e a eseguire un altro handshake TLS per le richieste successive. L'aumento del timeout keep-alive aiuta a migliorare la metrica per le distribuzioni. request-per-connection

> **Note**
>
> Affinché il valore Keep-alive Timeout (Timeout keep-alive) abbia un effetto, l'origine deve essere configurata per permettere connessioni permanenti.

Quote timeout di risposta e keep-alive

- Il valore predefinito per Timeout di risposta è 30 secondi.
- Il valore predefinito per Timeout keep-alive è 5 secondi.

Se richiedi un aumento del timeout per il tuo Account AWS, aggiorna le origini della distribuzione in modo che abbiano i valori di timeout di risposta e timeout keep-alive desiderati. Un aumento della quota per l'account non aggiorna automaticamente le origini. Ad esempio, se utilizzi una funzione Lambda@Edge per impostare un timeout keep-alive di 90 secondi, l'origine deve già avere un timeout keep-alive di 90 secondi o superiore. In caso contrario, l'esecuzione della funzione Lambda@Edge potrebbe non andare a buon fine.

Per ulteriori informazioni sulle quote di distribuzione, incluso come richiedere un aumento, consulta Quote generali sulle distribuzioni.

Cache Behavior Settings (Impostazioni del comportamento della cache)

Impostando il comportamento della cache, puoi configurare una serie di CloudFront funzionalità per un determinato modello di percorso URL per i file sul tuo sito web. Ad esempio, un comportamento cache potrebbe applicarsi a tutti i file `.jpg` nella directory `images` su un server Web che utilizzi come server di origine per CloudFront. Le funzionalità che puoi configurare per ogni comportamento cache sono:

- Il modello di percorso
- Se hai configurato più origini per la tua CloudFront distribuzione, l'origine a cui desideri CloudFront inoltrare le tue richieste
- Se le stringhe di query devono essere inoltrate alla tua origine
- Se l'accesso ai file specificati richiede la firma URLs
- Se gli utenti devono utilizzare HTTPS per accedere a tali file
- Il periodo minimo di permanenza di tali file nella CloudFront cache indipendentemente dal valore delle `Cache-Control` intestazioni aggiunte dall'origine ai file

Quando crei una nuova distribuzione, specifichi impostazioni per il comportamento cache di default, il quale inoltra automaticamente tutte le richieste all'origine che hai indicato alla creazione della distribuzione. Dopo aver creato una distribuzione, è possibile creare comportamenti aggiuntivi della cache che definiscono il modo in cui CloudFront risponde quando riceve una richiesta di oggetti che corrispondono a un modello di percorso, ad esempio,. `*.jpg` Se crei ulteriori comportamenti cache, quello di default è sempre l'ultimo a essere elaborato. Gli altri comportamenti della cache vengono elaborati nell'ordine in cui sono elencati nella CloudFront console o, se utilizzi l' CloudFront API, nell'ordine in cui sono elencati nell'`DistributionConfig`elemento per la distribuzione. Per ulteriori informazioni, consulta Modello di percorso.

Quando crei un comportamento di cache, specifichi l'unica origine da cui desideri CloudFront ottenere gli oggetti. Di conseguenza, se desiderate CloudFront distribuire oggetti da tutte le origini, dovete avere almeno tanti comportamenti di cache (incluso il comportamento predefinito della cache) quante sono le origini. Ad esempio, se avete due origini e solo il comportamento predefinito della cache, il comportamento predefinito della cache fa sì CloudFront che gli oggetti vengano recuperati da una delle origini, ma l'altra origine non viene mai utilizzata.

Per il numero massimo corrente di comportamenti della cache che puoi aggiungere a una distribuzione o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote generali sulle distribuzioni.

Argomenti

- Modello di percorso
- Origine o gruppo di origini
- Viewer Protocol Policy (Policy protocollo visualizzatore)
- Allowed HTTP Methods (Metodi HTTP consentiti)
- Field Level Encryption Config (Configurazione della crittografia a livello di campo)
- Cached HTTP Methods (Metodi HTTP in cache)
- Consentire richieste gRPC su HTTP/2
- Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate)
- Intestazioni elenco consentiti
- Object Caching (Caching oggetti)
- Minimum TTL (TTL minimo)
- Maximum TTL (TTL massimo)
- Default TTL (TTL di default)

- Forward Cookies (Inoltra cookie)
- Cookie elenco consentiti
- Query String Forwarding and Caching (Inoltro e caching di stringhe di query)
- Elenco consentiti stringhe di query
- Smooth Streaming
- Limita l'accesso degli spettatori (usa cookie firmati URLs o firmati)
- Firmatari fidati
- Account AWS numeri
- Comprimi oggetti automaticamente
- CloudFront evento
- ARN della funzione Lambda
- Includi corpo

Modello di percorso

Un modello di percorso (ad esempio, `images/*.jpg`) specifica le richieste a cui applicare questo comportamento della cache. Quando CloudFront riceve una richiesta dell'utente finale, il percorso richiesto viene confrontato con i modelli di percorso nell'ordine in cui i comportamenti della cache sono elencati nella distribuzione. La prima corrispondenza determina quale comportamento cache viene applicato a quella richiesta. Ad esempio, supponi di avere tre comportamenti cache con i seguenti tre modelli di percorso, in questo ordine:

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

> **Note**
>
> È possibile includere facoltativamente una barra (/) all'inizio del modello di percorso, ad esempio. `/images/*.jpg` CloudFront il comportamento è lo stesso con o senza la /. Se non si specifica/all'inizio del percorso, questo carattere viene automaticamente implicito; CloudFront tratta il percorso allo stesso modo con o senza la /. Ad esempio, CloudFront tratta come `/*product.jpg` `*product.jpg`

Una richiesta per il file `images/sample.gif` non corrisponde al primo modello di percorso, di conseguenza i comportamenti cache associati non sono applicati alla richiesta. Il file corrisponde al secondo modello di percorso, quindi vengono applicati i comportamenti cache associati al secondo modello di percorso anche se la richiesta corrisponde anche al terzo modello di percorso.

> **Note**
>
> Quando crei una nuova distribuzione, il valore di Path Pattern (Modello di percorso) per il comportamento cache di default è * (tutti i file) e non può essere modificato. Questo valore fa sì CloudFront che tutte le richieste relative agli oggetti vengano inoltrate all'origine specificata nel Dominio origine campo. Se la richiesta di un oggetto non corrisponde al modello di percorso per nessuno degli altri comportamenti della cache, CloudFront applica il comportamento specificato nel comportamento predefinito della cache.

> **Important**
>
> Definisci attentamente i modelli di percorso e la relativa sequenza, altrimenti potresti fornire agli utenti accesso non desiderato al tuo contenuto. Ad esempio, supponiamo che una richiesta corrisponda al modello di percorso per due comportamenti cache. Il primo comportamento della cache non richiede un segno URLs , mentre il secondo lo richiede. URLs Gli utenti possono accedere agli oggetti senza utilizzare un URL firmato perché CloudFront elabora il comportamento della cache associato alla prima corrispondenza.

Se lavori con un MediaPackage canale, devi includere modelli di percorso specifici per il comportamento della cache che definisci per il tipo di endpoint di origine. Ad esempio, per un endpoint DASH, digita `*.mpd` per Path Pattern (Modello di percorso). Per ulteriori informazioni e istruzioni specifiche, consulta Distribuzione di video live formattati con AWS Elemental MediaPackage.

Il percorso specificato si applica alle richieste per tutti i file nella directory specificata e nelle sottodirectory al di sotto della directory specificata. CloudFront non considera le stringhe di query o i cookie durante la valutazione del modello di percorso. Ad esempio, se una directory `images` contiene le sottodirectory `product1` e `product2`, il modello di percorso `images/*.jpg` è applicabile alle richieste per qualsiasi file .jpg nelle directory `images` `images/product1` e `images/product2`. Se ai file nella directory `images/product1` intendi applicare un comportamento cache diverso rispetto ai file nelle directory `images` e `images/product2`, crea un comportamento cache distinto

per `images/product1` e sposta quel comportamento cache in una posizione sopra (prima) il comportamento cache per la directory `images`.

Puoi utilizzare i seguenti caratteri jolly nel modello di percorso:

- `*` corrisponde a 0 o più caratteri.
- `?` corrisponda esattamente a 1 carattere.

I seguenti esempi mostrano come sono utilizzati i caratteri jolly:

Modello di percorso	File corrispondenti al modello di percorso
`*.jpg`	Tutti i file .jpg.
`images/*.jpg`	Tutti i file .jpg nella directory `images` e nelle sottodirectory della directory `images`.
`a*.jpg`	• Tutti i file .jpg il cui nome inizia con a, ad esempio, `apple.jpg` e `appalachian_trail_2012_05_21.jpg` . • Tutti i file .jpg il cui percorso di file inizia con a, ad esempio, `abra/cadabra/magic.jpg` .
`a??.jpg`	Tutti i file .jpg il cui nome inizia con a ed è seguito da esattamente due altri caratteri, ad esempio, `ant.jpg` e `abe.jpg`.
`*.doc*`	Tutti i file la cui estensione inizia con `.doc`, ad esempio, i file `.doc`, `.docx` e `.docm`. Non puoi utilizzare il modello di percorso `*.doc?` in questo caso, poiché non si applicherebbe alle richieste per file `.doc`; il carattere jolly ? sostituisce esattamente un solo carattere.

La lunghezza massima di un modello di percorso è 255 caratteri. Il valore può contenere uno qualsiasi dei seguenti caratteri:

- A-Z, a-z

  Per i modelli di percorso viene fatta distinzione tra maiuscole e minuscole, quindi il modello di percorso `*.jpg` non è valido per il file `LOGO.JPG`.
- 0-9
- _ - . * $ / ~ " ' @ : +
- &, passato e restituito come `&`

Normalizzazione del percorso

CloudFront normalizza i percorsi URI coerenti con RFC 3986 e quindi abbina il percorso al comportamento corretto della cache. Una volta che il comportamento della cache corrisponde, CloudFront invia il percorso URI non elaborato all'origine. Se non corrispondono, le richieste vengono invece abbinate al comportamento della cache predefinito.

Alcuni caratteri vengono normalizzati e rimossi dal percorso, ad esempio barre multiple (`//`) o punti (`..`). Ciò può modificare l'URL CloudFront utilizzato in modo che corrisponda al comportamento della cache previsto.

Example Esempio

Vengono specificati i percorsi `/a/b*` e `/a*` per il comportamento cache.

- Un visualizzatore che invia il percorso `/a/b?c=1` corrisponderà al comportamento cache `/a/b*`.
- Un visualizzatore che invia il percorso `/a/b/..?c=1` corrisponderà al comportamento cache `/a*`.

Per ovviare alla normalizzazione dei percorsi, è possibile aggiornare i percorsi delle richieste o il modello di percorso per il comportamento cache.

Origine o gruppo di origini

Questa impostazione si applica solo quando si crea o si aggiorna un comportamento cache per una distribuzione esistente.

Immetti il valore di un'origine o di un gruppo di origini esistente. Identifica l'origine o il gruppo di origine a cui si desidera CloudFront indirizzare le richieste quando una richiesta (come https://

example.com /logo.jpg) corrisponde al modello di percorso per un comportamento nella cache (ad esempio*.jpg) o per il comportamento predefinito della cache (*).

Viewer Protocol Policy (Policy protocollo visualizzatore)

Scegliete la politica del protocollo che desiderate che gli spettatori utilizzino per accedere ai vostri contenuti da postazioni periferiche: CloudFront

- HTTP and HTTPS (HTTP e HTTPS): i visualizzatori possono utilizzare entrambi i protocolli.
- Redirect HTTP to HTTPS (Reindirizza HTTP a HTTPS): i visualizzatori possono utilizzare entrambi i protocolli, ma le richieste HTTP vengono automaticamente reindirizzate alle richieste HTTPS.
- HTTPS Only (Solo HTTPS): i visualizzatori possono accedere al tuo contenuto solo se utilizzano HTTPS.

Per ulteriori informazioni, consulta Richiedi HTTPS per la comunicazione tra gli spettatori e CloudFront.

Allowed HTTP Methods (Metodi HTTP consentiti)

Specificate i metodi HTTP che desiderate CloudFront elaborare e inoltrare all'origine:

- GET, HEAD: potete utilizzarli CloudFront solo per recuperare oggetti dall'origine o per ottenere le intestazioni degli oggetti.
- GET, HEAD, OPTIONS: puoi utilizzare CloudFront solo per ottenere oggetti dalla tua origine, ottenere intestazioni di oggetti oppure recuperare un elenco delle opzioni che il tuo server di origine supporta.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE: puoi usarlo CloudFront per ottenere, aggiungere, aggiornare ed eliminare oggetti e per ottenere le intestazioni degli oggetti. Inoltre, puoi eseguire altre operazioni POST, ad esempio inviare dati da un modulo Web.

> **Note**
>
> Se stai utilizzando gRPC nel tuo carico di lavoro, devi selezionare GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. I carichi di lavoro gRPC richiedono il metodo `POST`. Per ulteriori informazioni, consulta Usare gRPC con le distribuzioni CloudFront .
> CloudFront memorizza nella cache le risposte `GET` e le `HEAD` richieste e, facoltativamente, le richieste. `OPTIONS` Le risposte alle `OPTIONS` richieste vengono memorizzate nella cache

separatamente dalle risposte GET e dalle HEAD richieste (il OPTIONS metodo è incluso nella chiave di cache per OPTIONS le richieste). CloudFront non memorizza nella cache le risposte alle richieste che utilizzano altri metodi.

Important

Se scegli GET, HEAD, OPTIONS o GET, HEAD, OPTIONS, POST, PUT, PATCH, DELETE, potresti aver bisogno di limitare l'accesso al tuo bucket Amazon S3 o alla tua origine personalizzata per impedire agli utenti di eseguire operazioni che non sono autorizzati a eseguire. I seguenti esempi descrivono come limitare l'accesso:

- Se utilizzi Amazon S3 come origine per la tua distribuzione: crea un controllo di accesso all' CloudFront origine per limitare l'accesso ai tuoi contenuti Amazon S3 e concedi le autorizzazioni al controllo degli accessi di origine. Ad esempio, se configuri per accettare e CloudFront inoltrare questi metodi solo perché desideri utilizzarliPUT, devi comunque configurare le policy dei bucket di Amazon S3 per gestire DELETE le richieste in modo appropriato. Per ulteriori informazioni, consulta Limitazione dell'accesso a un'origine Amazon S3.
- Se utilizzi un'origine personalizzata: configura il server di origine per gestire tutti i metodi. Ad esempio, se configuri per accettare e CloudFront inoltrare questi metodi solo perché desideri utilizzarliPOST, devi comunque configurare il server di origine per gestire DELETE le richieste in modo appropriato.

Field Level Encryption Config (Configurazione della crittografia a livello di campo)

Se intendi utilizzare la crittografia a livello di campo su specifici campi dati, nell'elenco a discesa scegli una configurazione di crittografia a livello di campo.

Per ulteriori informazioni, consulta Utilizzo della crittografia a livello di campo per la protezione dei dati sensibili.

Cached HTTP Methods (Metodi HTTP in cache)

Specificate se desiderate CloudFront memorizzare nella cache la risposta dall'origine quando un utente invia una OPTIONS richiesta. CloudFront memorizza sempre nella cache la risposta GET e HEAD le richieste.

Consentire richieste gRPC su HTTP/2

Specifica se la distribuzione deve consentire le richieste gRPC. Per abilitare gRPC, seleziona le seguenti impostazioni:

- Per Metodi HTTP consentiti, seleziona i metodi GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. gRPC richiede il metodo `POST`.
- Seleziona la casella di controllo gRPC che viene visualizzata dopo che selezioni il metodo `POST`.
- Per Versioni HTTP supportate, seleziona HTTP/2.

Per ulteriori informazioni, consulta Usare gRPC con le distribuzioni CloudFront .

Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate)

Specificate se desiderate CloudFront memorizzare nella cache gli oggetti in base ai valori delle intestazioni specificate:

- Nessuno (migliora la memorizzazione nella cache): CloudFront non memorizza nella cache gli oggetti in base ai valori dell'intestazione.
- Allowlist: CloudFront memorizza nella cache gli oggetti in base solo ai valori delle intestazioni specificate. Usa Allowlist Headers per scegliere le intestazioni su cui basare la memorizzazione nella cache. CloudFront
- Tutti: CloudFront non memorizza nella cache gli oggetti associati a questo comportamento della cache. CloudFront Invia invece ogni richiesta all'origine. (Non consigliato per origini Amazon S3).

Indipendentemente dall'opzione scelta, CloudFront inoltra determinate intestazioni all'origine e intraprende azioni specifiche in base alle intestazioni inoltrate. Per ulteriori informazioni su come CloudFront gestisce l'inoltro delle intestazioni, consulta. Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

Per ulteriori informazioni su come configurare la memorizzazione nella cache CloudFront utilizzando le intestazioni di richiesta, consulta. Caching dei contenuti in base alle intestazioni di richiesta

Intestazioni elenco consentiti

Queste impostazioni si applicano solo quando si seleziona Elenco consentiti per Cache basata su intestazioni richiesta selezionate.

Specificate le intestazioni da prendere in considerazione durante CloudFront la memorizzazione nella cache degli oggetti. Seleziona le intestazioni dall'elenco di intestazioni disponibili e scegli Add (Aggiungi). Per inoltrare un'intestazione personalizzata, immetti il nome dell'intestazione nel campo e scegli Add Custom (Aggiungi personalizzata).

Per il numero massimo corrente di intestazioni che puoi inserire in liste bianche per ogni comportamento della cache o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote delle intestazioni.

Object Caching (Caching oggetti)

Se il server di origine sta aggiungendo un'`Cache-Control`intestazione agli oggetti per controllare per quanto tempo gli oggetti rimangono nella CloudFront cache e se non vuoi modificare il `Cache-Control` valore, scegli Usa Origin Cache Headers.

Per specificare un periodo minimo e massimo di permanenza degli oggetti nella CloudFront cache indipendentemente dalle **`Cache-Control`** intestazioni e un tempo predefinito in cui gli oggetti rimangono nella CloudFront cache quando l'**`Cache-Control`**intestazione non è presente in un oggetto, scegli Personalizza. Quindi, nei campi Minimum TTL (TTL minimo), Default TTL (TTL di default) e Maximum TTL (TTL massimo), specifica il valore applicabile.

Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Minimum TTL (TTL minimo)

Specificate il periodo minimo, in secondi, per cui desiderate che gli oggetti rimangano nella CloudFront cache prima di CloudFront inviare un'altra richiesta all'origine per determinare se l'oggetto è stato aggiornato.

> **Warning**
>
> Se il TTL minimo è maggiore di 0, CloudFront memorizzerà nella cache il contenuto almeno per la durata specificata nel TTL minimo della policy di cache, anche se le `private` direttive `Cache-Control: no-cache` `no-store`, o sono presenti nelle intestazioni di origine.

Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Maximum TTL (TTL massimo)

Specificate il tempo massimo, in secondi, per cui desiderate che gli oggetti rimangano nella CloudFront cache prima di CloudFront interrogare l'origine per verificare se l'oggetto è stato aggiornato. Il valore specificato per Maximum TTL (TTL massimo) viene utilizzato solo quando l'origine aggiunge intestazioni HTTP, ad esempio `Cache-Control max-age`, `Cache-Control s-maxageo Expires`, agli oggetti. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Per specificare un valore per Maximum TTL (TTL massimo), devi scegliere l'opzione Customize (Personalizza) per l'impostazione Object Caching (Caching oggetti).

Il valore di default per Maximum TTL (TTL massimo) è 31536000 secondi (un anno). Se sostituisci il valore di Minimum TTL (TTL minimo) o Default TTL (TTL di default) con un valore superiore a 31536000 secondi, il valore predefinito di Maximum TTL (TTL massimo) sarà il valore di Default TTL (TTL di default).

Default TTL (TTL di default)

Specificate il periodo di tempo predefinito, in secondi, durante il quale desiderate che gli oggetti rimangano nella CloudFront cache prima di CloudFront inoltrare un'altra richiesta all'origine per determinare se l'oggetto è stato aggiornato. Il valore specificato per TTL predefinito viene utilizzato solo quando l'origine non aggiunge agli oggetti intestazioni HTTP, ad esempio `Cache-Control max-age`, `Cache-Control s-maxage` o `Expires`. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Per specificare un valore per Default TTL (TTL di default), devi scegliere l'opzione Customize (Personalizza) per l'impostazione Object Caching (Caching oggetti).

Il valore di default per Default TTL (TTL di default) è 86400 secondi (un giorno). Se cambi il valore di Minimum TTL in maggiore di 86400 secondi, il valore predefinito di Default TTL sarà uguale al valore di Minimum TTL.

Forward Cookies (Inoltra cookie)

> **Note**
>
> Per le origini Amazon S3, questa opzione si applica solo ai bucket configurati come endpoint di un sito Web.

Specificate se desiderate CloudFront inoltrare i cookie al vostro server di origine e, in caso affermativo, quali. Se scegli di inoltrare solo i cookie selezionati (un elenco consentiti di cookie), immetti i nomi dei cookie nel campo Cookie elenco consentiti. Se scegli All (Tutti), CloudFront inoltra tutti i cookie indipendentemente dal numero di cookie utilizzati dall'applicazione.

Amazon S3 non elabora cookie e l'inoltro di cookie all'origine riduce la capacità di memorizzazione nella cache. Per i comportamenti cache che inoltrano richieste a un'origine di Amazon S3, scegli None (Nessuno) per Forward Cookie (Inoltra cookie).

Per ulteriori informazioni sull'inoltro di cookie all'origine, consulta Caching dei contenuti basati su cookie.

Cookie elenco consentiti

> **Note**
>
> Per le origini Amazon S3, questa opzione si applica solo ai bucket configurati come endpoint di un sito Web.

Se avete scelto Allowlist nell'elenco Inoltra cookie, nel campo Allowlist Cookies, inserite i nomi dei cookie che desiderate CloudFront inoltrare al server di origine per questo comportamento nella cache. Immetti ogni nome di cookie su una nuova riga.

Per i nomi di cookie puoi utilizzare i seguenti caratteri:

- * corrisponde a 0 o più caratteri nel nome di cookie.
- ? corrisponde esattamente a un carattere nel nome del cookie.

Ad esempio, supponiamo che le richieste visualizzatore per un oggetto includano un cookie denominato:

`userid_`*`member-number`*

Per cui ciascuno dei tuoi utenti ha un valore unico. *`member-number`* Desideri CloudFront memorizzare nella cache una versione separata dell'oggetto per ogni membro. Puoi farlo inoltrando tutti i cookie alla tua origine, ma le richieste dei visualizzatori includono alcuni cookie che non desideri CloudFront memorizzare nella cache. In alternativa, puoi specificare il seguente valore come nome del cookie, in CloudFront modo da inoltrare all'origine tutti i cookie che iniziano con: `userid_`

`userid_*`

Per il numero massimo corrente di nomi di cookie che puoi inserire nella lista bianca per ogni comportamento della cache o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote sui cookie (impostazioni della cache legacy).

Query String Forwarding and Caching (Inoltro e caching di stringhe di query)

CloudFront può memorizzare nella cache diverse versioni dei contenuti in base ai valori dei parametri della stringa di query. Seleziona una delle seguenti opzioni:

None (Improves Caching) (Nessuno (Migliora caching))

Scegli questa opzione se l'origine restituisce la stessa versione di un oggetto indipendentemente dai valori dei parametri di stringa di query. Ciò aumenta la probabilità che sia CloudFront possibile evadere una richiesta dalla cache, migliorando le prestazioni e riducendo il carico sull'origine.

Inoltra tutto, cache basata su elenco consentiti

Scegli questa opzione se il tuo server di origine restituisce differenti versioni degli oggetti in base a uno o più parametri di stringa di query. Specificate quindi i parametri che desiderate CloudFront utilizzare come base per la memorizzazione nella cache sul Elenco consentiti stringhe di query campo.

Forward all, cache based on all (Inoltra tutto, cache basata su tutto)

Scegli questa opzione se il tuo server di origine restituisce differenti versioni degli oggetti per tutti i parametri di stringa di query.

Per ulteriori informazioni sul caching in base ai parametri di stringa di query, incluso il modo in cui migliorare le prestazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

Elenco consentiti stringhe di query

Questa impostazione si applica solo quando scegli Inoltra tutti, cache basata su elenco consentiti per Query String Forwarding and Caching (Inoltro e caching di stringhe di query). È possibile specificare i parametri della stringa di query che si desidera CloudFront utilizzare come base per la memorizzazione nella cache.

Smooth Streaming

Scegli Yes (Sì) se desideri distribuire file multimediali nel formato Microsoft Smooth Streaming e non disponi di un server IIS.

Scegli No se disponi di un server Microsoft IIS che vuoi utilizzare come origine per distribuire file multimediali nel formato Microsoft Smooth Streaming, oppure se non distribuirai file multimediali Smooth Streaming.

> **Note**
>
> Se specifichi Yes (Sì), puoi continuare a distribuire altro contenuto utilizzando questo comportamento cache se il contenuto corrisponde al valore di Path Pattern (Modello di percorso).

Per ulteriori informazioni, consulta Configurazione di video on demand per Microsoft Smooth Streaming.

Limita l'accesso degli spettatori (usa cookie firmati URLs o firmati)

Se desideri che le richieste di oggetti che `PathPattern` corrispondono al comportamento di questo tipo di cache vengano utilizzate come pubbliche URLs, scegli No.

Se desiderate che le richieste di oggetti che `PathPattern` corrispondono al comportamento di questo tipo di cache vengano utilizzate firmate URLs, scegliete Sì. Specificate quindi gli AWS account che desiderate utilizzare per creare account firmati URLs; questi account sono noti come firmatari attendibili.

Per ulteriori informazioni sui trusted signer, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

Firmatari fidati

Questa impostazione si applica solo quando scegli Sì per Limita l'accesso degli spettatori (Usa cookie firmati URLs o firmati).

Scegli AWS gli account che desideri utilizzare come firmatari attendibili per questo comportamento nella cache:

- Personale: utilizza l'account con cui hai attualmente effettuato l'accesso Console di gestione AWS come firmatario attendibile. Se al momento hai effettuato l'accesso come utente IAM, l' AWS account associato viene aggiunto come firmatario affidabile.
- Specifica account: immetti i numeri di account per firmatari fidati nel campo Numeri account di AWS .

Per creare un account firmato URLs, un AWS account deve avere almeno una coppia di CloudFront key pair attiva.

> **Important**
>
> Se stai aggiornando una distribuzione che stai già utilizzando per distribuire contenuti, aggiungi firmatari attendibili solo quando sei pronto per iniziare a generare oggetti firmati URLs per i tuoi oggetti. Dopo aver aggiunto firmatari attendibili a una distribuzione, gli utenti devono utilizzare signed URLs per accedere agli oggetti che corrispondono a questo `PathPattern` comportamento di cache.

Account AWS numeri

Questa impostazione si applica solo quando si sceglie Specifica account per Firmatari attendibili.

Se desideri creare un account firmato URLs utilizzando Account AWS in aggiunta o al posto dell'account corrente, inserisci un Account AWS numero per riga in questo campo. Tenere presente quanto segue:

- Gli account che specifichi devono avere almeno una coppia di chiavi CloudFront attiva. Per ulteriori informazioni, consulta Creazione di coppie di chiavi per i firmatari.
- Non puoi creare coppie di CloudFront chiavi per gli utenti IAM, quindi non puoi utilizzare gli utenti IAM come firmatari affidabili.
- Per informazioni su come ottenere il Account AWS numero di un account, consulta Visualizza gli Account AWS identificatori nella Guida di riferimento per la Account AWS gestione.
- Se inserisci il numero di conto per l'account corrente, seleziona CloudFront automaticamente la casella di controllo Self e rimuove il numero di conto dall'elenco dei numeri di AWS conto.

Comprimi oggetti automaticamente

Se desideri CloudFront comprimere automaticamente determinati tipi di file quando gli utenti supportano i contenuti compressi, scegli Sì. Quando CloudFront comprime il tuo contenuto, i download sono più rapidi in quanto i file sono più piccoli e il rendering delle pagine Web è più veloce per i tuoi utenti. Per ulteriori informazioni, consulta Distribuzione di file compressi.

CloudFront evento

Questa impostazione si applica alle Associazioni di funzioni Lambda.

Puoi scegliere di eseguire una funzione Lambda quando si verificano uno o più dei seguenti CloudFront eventi:

- Quando CloudFront riceve una richiesta da un visualizzatore (richiesta del visualizzatore)
- Prima CloudFront inoltra una richiesta all'origine (richiesta di origine)
- Quando CloudFront riceve una risposta dall'origine (origin response)
- Before CloudFront restituisce la risposta allo spettatore (risposta del visualizzatore)

Per ulteriori informazioni, consulta Scelta dell'evento per attivare la funzione.

ARN della funzione Lambda

Questa impostazione si applica alle Associazioni di funzioni Lambda.

Specifica l'ARN (Amazon Resource Name) della funzione Lambda per la quale intendi aggiungere un trigger. Per informazioni su come ottenere l'ARN per una funzione, vedere il passaggio 1 della procedura Aggiungere trigger utilizzando la console. CloudFront

Includi corpo

Questa impostazione si applica alle Associazioni di funzioni Lambda.

Per ulteriori informazioni, consulta la sezione Includere corpo.

Distribution Settings (Impostazioni distribuzione)

I seguenti valori si applicano a tutta la distribuzione.

Argomenti

Price Class (Categoria prezzo)

Scegli la classe di prezzo corrispondente al prezzo massimo che desideri pagare per il servizio. CloudFront Per impostazione predefinita, CloudFront serve gli oggetti da posizioni periferiche in tutte le CloudFront regioni.

Per ulteriori informazioni sulle classi di prezzo e su come la scelta della classe di prezzo influisce sulle CloudFront prestazioni della distribuzione, consulta la pagina CloudFront dei prezzi.

AWS WAF ACL web

Puoi proteggere la tua CloudFront distribuzione con AWS WAFun firewall per applicazioni Web che ti consente di proteggere le tue applicazioni Web e di APIs bloccare le richieste prima che raggiungano

i tuoi server. Puoi farlo Abilitazione di AWS WAF per le distribuzioni quando crei o modifichi una CloudFront distribuzione.

Facoltativamente, è possibile configurare successivamente protezioni di sicurezza aggiuntive per altre minacce specifiche dell'applicazione nella AWS WAF console all'indirizzo. https://console.aws.amazon.com/wafv2/

Per ulteriori informazioni in merito AWS WAF, consulta la Guida per gli AWS WAF sviluppatori.

Nomi di dominio alternativi () CNAMEs

Opzionale. Specificate uno o più nomi di dominio che desiderate utilizzare URLs per i vostri oggetti anziché il nome di dominio CloudFront assegnato quando create la distribuzione. È necessario possedere il nome di dominio o disporre dell'autorizzazione per utilizzarlo, cosa che si verifica aggiungendo un SSL/TLS certificato.

Ad esempio, se desideri l'URL per l'oggetto:

`/images/image.jpg`

Appaia così:

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

Anziché così:

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

Aggiungi un CNAME per `www.example.com`.

> **Important**
>
> Se aggiungi un CNAME per `www.example.com` alla distribuzione, devi anche eseguire le operazioni seguenti:
>
> - Crea (o aggiorna) un record CNAME con il servizio DNS per instradare le query per `www.example.com` a `d111111abcdef8.cloudfront.net`.
> - Aggiungi un certificato rilasciato CloudFront da un'autorità di certificazione (CA) affidabile che copra il nome di dominio (CNAME) che aggiungi alla tua distribuzione, per convalidare l'autorizzazione all'uso del nome di dominio.

Per creare un record CNAME con il provider del servizio DNS per il dominio devi disporre delle autorizzazioni necessarie. Normalmente questo significa che sei il proprietario del dominio o che stai sviluppando un'applicazione per il proprietario del dominio.

Per il numero massimo corrente di nomi di dominio alternativi che puoi aggiungere a una distribuzione o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote generali sulle distribuzioni.

Per ulteriori informazioni sui nomi di dominio alternativi, consulta Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs. Per ulteriori informazioni su CloudFront URLs, consulta. Personalizzazione del formato URL per i file in CloudFront

Certificato SSL

Se hai specificato un nome di dominio alternativo da utilizzare con la distribuzione, scegli Custom SSL Certificate (Certificato SSL personalizzato), quindi, per convalidare l'autorizzazione per utilizzare il nome di dominio alternativo, scegli un certificato che lo copre. Se desideri che i visualizzatori utilizzino HTTPS per accedere ai tuoi oggetti, scegli l'impostazione applicabile.

- CloudFront Certificato predefinito (*.cloudfront.net): scegli questa opzione se desideri utilizzare il nome di CloudFront dominio presente nel campo URLs per i tuoi oggetti, ad esempio. `https://d111111abcdef8.cloudfront.net/image1.jpg`
- Certificato SSL personalizzato: scegli questa opzione se desideri utilizzare il tuo nome di dominio URLs per i tuoi oggetti come nome di dominio alternativo, ad esempio. `https://example.com/image1.jpg` Quindi, scegli un certificato da utilizzare che copre il nome di dominio alternativo. L'elenco di certificati può includere i seguenti:
  - Certificati forniti da AWS Certificate Manager
  - Certificati acquistati da un'autorità di certificazione esterna e caricati in ACM
  - Certificati acquistati da un'autorità di certificazione esterna e caricati nello store certificati di IAM

  Se scegli questa impostazione, ti consigliamo di utilizzare solo un nome di dominio alternativo nell'oggetto URLs (https://example.com/logo.jpg). If you use your CloudFront distribution domain name (https://d111111abcdef8.cloudfront.net/logo.jpg) e un client utilizza un visualizzatore precedente che non supporta SNI. La risposta del visualizzatore dipende dal valore che scegli per Clients Supported:

- Tutti i client: il visualizzatore visualizza un avviso perché il nome di dominio non corrisponde al nome di dominio nel certificato. CloudFront SSL/TLS
- Solo client che supportano Server Name Indication (SNI): CloudFront interrompe la connessione con il visualizzatore senza restituire l'oggetto.

Supporto client SSL personalizzato

Si applica solo quando si sceglie Certificato SSL personalizzato (example.com) per Certificato SSL. Se hai specificato uno o più nomi di dominio alternativi e un certificato SSL personalizzato per la distribuzione, scegli come gestire le richieste CloudFront HTTPS:

- Client che supportano SNI (Server Name Indication) - (scelta consigliata): con questa impostazione, praticamente tutti i browser Web e i client moderni possono connettersi alla distribuzione, poiché supportano SNI. Tuttavia, alcuni visualizzatori potrebbero utilizzare browser Web meno recenti o client che non supportano SNI, il che significa che non possono connettersi alla distribuzione.

  Per applicare questa impostazione utilizzando l' CloudFront API, specifica `sni-only` nel `SSLSupportMethod` campo. In CloudFormation, il campo è denominato `SslSupportMethod` (nota il diverso formato maiuscolo/minuscolo).
- Supporto client legacy: con questa impostazione, i browser Web e i client meno recenti che non supportano SNI possono connettersi alla distribuzione. Tuttavia, questa impostazione comporta costi mensili aggiuntivi. Per il prezzo esatto, vai alla pagina CloudFront dei prezzi di Amazon e cerca SSL personalizzato con IP dedicato.

  Per applicare questa impostazione utilizzando l' CloudFront API, specifica `vip` nel `SSLSupportMethod` campo. In CloudFormation, il campo è denominato `SslSupportMethod` (notate le diverse lettere maiuscole).

Per ulteriori informazioni, consulta Scegli in che modo CloudFront vengono servite le richieste HTTPS.

Policy di sicurezza (versione minima SSL/TLS)

Specificate la politica di sicurezza che desiderate utilizzare CloudFront per le connessioni HTTPS con i visualizzatori (client). Dalla policy di sicurezza dipendono due impostazioni:

- Il SSL/TLS protocollo minimo CloudFront utilizzato per comunicare con gli spettatori.

- I codici che è CloudFront possibile utilizzare per crittografare il contenuto restituito agli utenti.

Per ulteriori informazioni sui criteri di sicurezza, compresi i protocolli e le crittografia inclusi, vedere Protocolli e cifrari supportati tra visualizzatori e CloudFront.

Le politiche di sicurezza disponibili dipendono dai valori specificati per SSL Certificate e Custom SSL Client Support (noti come `CloudFrontDefaultCertificate` e `SSLSupportMethod` presenti nell' CloudFront API):

- Quando il certificato SSL è un CloudFront certificato predefinito (*.cloudfront.net) (quando **`CloudFrontDefaultCertificate`** è presente **`true`** nell'API), imposta automaticamente la politica di sicurezza su. CloudFront TLSv1
- Quando Certificato SSL è Certificato SSL personalizzato (example.com) e Supporto client SSL personalizzato è Client che supportano l'indicazione del nome del server (SNI) - (suggerita) (quando nell'API `CloudFrontDefaultCertificate` è `false` e `SSLSupportMethod` è `sni-only`), puoi scegliere tra le seguenti policy di sicurezza:
  - TLSv1.3_2025
  - TLSv1.2_2025
  - TLSv1.2_2021
  - TLSv1.2_2019
  - TLSv1.2_2018
  - TLSv1.1_2016
  - TLSv1_2016
  - TLSv1
- Quando Certificato SSL è Certificato SSL personalizzato (example.com) e Supporto client SSL personalizzato è Supporto client legacy (quando nell'API `CloudFrontDefaultCertificate` è `false` e `SSLSupportMethod` è `vip`), puoi scegliere tra le seguenti policy di sicurezza:
  - TLSv1
  - SSLv3

  In questa configurazione, le politiche di sicurezza TLSv1 .3_2025, .2_2025, TLSv1 TLSv1 .2_2021, TLSv1 .2_2019, .2_2018, .1_2016 e _2016 non sono disponibili nella console o nell'TLSv1API. TLSv1 TLSv1 CloudFront Se si desidera utilizzare uno di questi criteri di sicurezza, sono disponibili le seguenti opzioni:

- Valutare se la distribuzione necessita di supporto per i client legacy con indirizzi IP dedicati. Se i visualizzatori supportano l'indicazione del nome server (SNI), si consiglia di aggiornare l'impostazione Supporto client SSL personalizzato della distribuzione in Client che supportano l'indicazione del nome server (SNI) (impostare `SSLSupportMethod` su `sni-only` nell'API). Ciò consente di utilizzare qualsiasi politica di sicurezza TLS disponibile e può anche ridurre i costi. CloudFront
- Se devi mantenere Legacy Clients Support con indirizzi IP dedicati, puoi richiedere una delle altre politiche di sicurezza TLS (TLSv1.3_2025, .2_2025, TLSv1 .2_2021, TLSv1 TLSv1 .2_2019, .2_2018, .1_2016 o _2016) creando un caso nel Support Center TLSv1. TLSv1 TLSv1 AWS

> **Note**
>
> Prima di contattare AWS Support per richiedere questa modifica, considera quanto segue:
>
> - Quando aggiungi una di queste politiche di sicurezza (TLSv1.3_2025, .2_2025, TLSv1 TLSv1 .2_2021, .2_2019, .2_2018 TLSv1, .1_2016 o _2016 TLSv1TLSv1) a una distribuzione Legacy Clients Support TLSv1, la politica di sicurezza viene applicata a tutte le richieste di visualizzatori non SNI per tutte le distribuzioni Legacy Clients Support del tuo account. AWS Tuttavia, quando i visualizzatori inviano richieste SNI a una distribuzione con il supporto client legacy, vengono applicate le policy di sicurezza di tale distribuzione. Per assicurarti che la politica di sicurezza desiderata venga applicata a tutte le richieste dei visualizzatori inviate a tutte le distribuzioni Legacy Clients Support del tuo AWS account, aggiungi la politica di sicurezza desiderata a ciascuna distribuzione singolarmente.
> - Per definizione, la nuova policy di sicurezza non supporta gli stessi protocolli e la stessa crittografia di quella precedente. Ad esempio, se scegli di aggiornare la politica di sicurezza di una distribuzione TLSv1 da TLSv1 .1_2016, tale distribuzione non supporterà più il codice DES- -SHA. CBC3 Per ulteriori informazioni sui crittografia e protocolli supportati da ogni policy di protezione, vedere Protocolli e cifrari supportati tra visualizzatori e CloudFront.

Versioni HTTP supportate

Scegli le versioni HTTP che desideri che la tua distribuzione supporti quando gli spettatori comunicano con. CloudFront

Per i visualizzatori e CloudFront per utilizzare HTTP/2, i visualizzatori devono supportare TLSv1 .2 o versioni successive e Server Name Indication (SNI).

Per i visualizzatori e CloudFront per utilizzare HTTP/3, i visualizzatori devono supportare .3 e Server Name Indication (SNI). TLSv1 CloudFront supporta la migrazione della connessione HTTP/3 per consentire allo spettatore di cambiare rete senza perdere la connessione. Per ulteriori informazioni sulla migrazione della connessione, consultare Migrazione della connessione in RFC 9000.

> **Note**
>
> Per ulteriori informazioni sui cifrari TLSv1 .3 supportati, consulta. Protocolli e cifrari supportati tra visualizzatori e CloudFront

> **Note**
>
> Se utilizzi Amazon Route 53, puoi utilizzare i record HTTPS per consentire la negoziazione del protocollo come parte della ricerca DNS, se supportata dal client. Per ulteriori informazioni, consulta Create alias resource record set.

Default Root Object (Oggetto root di default)

Opzionale. L'oggetto che desiderate richiedere CloudFront all'origine (ad esempio,`index.html`) quando un visualizzatore richiede l'URL principale della distribuzione (`https://www.example.com/`) anziché un oggetto nella distribuzione (). `https://www.example.com/product-description.html` La specifica di un oggetto root di default evita l'esposizione del contenuto della distribuzione.

La lunghezza massima del nome è 255 caratteri. Il nome può contenere uno qualsiasi dei seguenti caratteri:

- A-Z, a-z
- 0-9

- _ - . * $ / ~ " '
- &, passato e restituito come `&`

Quando specifichi l'oggetto root di default, immetti solo il nome dell'oggetto, ad esempio, `index.html`. Non aggiungere una / prima del nome dell'oggetto.

Per ulteriori informazioni, consulta Specifica di un oggetto root predefinito.

Registrazione di log standard

Specificate se desiderate CloudFront registrare le informazioni su ogni richiesta di un oggetto e memorizzare i file di registro. Puoi attivare o disattivare la registrazione in qualsiasi momento. L'abilitazione della registrazione di log non comporta alcun costo aggiuntivo, ma potrebbero essere addebitati costi per l'archiviazione e l'accesso ai file. Puoi eliminare i log in qualsiasi momento.

CloudFront supporta le seguenti opzioni di registrazione standard:

- Registrazione standard (v2): puoi inviare log a destinazioni di consegna, tra cui Amazon CloudWatch Logs, Amazon Data Firehose e Amazon Simple Storage Service (Amazon S3).
- Registrazione di log standard (legacy): puoi inviare i log solo a un bucket Amazon S3.

Log delle connessioni

Quando attivi l'autenticazione reciproca per la distribuzione, CloudFront fornisce log di connessione che acquisiscono gli attributi relativi alle richieste inviate alle distribuzioni. I log di connessione contengono informazioni come l'indirizzo IP e la porta del client, le informazioni sul certificato del client, i risultati della connessione e i codici TLS utilizzati. Questi log di connessione possono quindi essere utilizzati per esaminare i modelli di richiesta e altre tendenze.

Per ulteriori informazioni sui log di connessione, consulta. Osservabilità utilizzando i log di connessione

Log Prefix (Prefisso log)

(Facoltativo) Se abilitate la registrazione standard (legacy), specificate l'eventuale stringa da aggiungere come prefisso CloudFront ai nomi dei file di registro degli accessi per questa distribuzione, ad esempio. `exampleprefix/` La barra finale (/) è facoltativa ma consigliata per semplificare la navigazione nei file di log. Per ulteriori informazioni, consulta Configurazione della registrazione di log standard (legacy).

Registrazione dei cookie

Se desideri includere CloudFront i cookie nei log di accesso, scegli Attivato. Se scegli di includere i cookie nei CloudFront log, registra tutti i cookie indipendentemente da come configuri i comportamenti della cache per questa distribuzione: inoltra tutti i cookie, non inoltra nessun cookie o inoltra un elenco specifico di cookie all'origine.

Amazon S3 non elabora i cookie, quindi a meno che la tua distribuzione non includa anche un Amazon EC2 o un'altra origine personalizzata, ti consigliamo di scegliere Off per il valore di Cookie Logging.

Per ulteriori informazioni sui cookie, consulta Caching dei contenuti basati su cookie.

Abilita IPv6 (richieste del visualizzatore)

Se desideri rispondere CloudFront alle richieste degli spettatori IPv4 e agli indirizzi IPv6 IP, seleziona Abilita IPv6. Per ulteriori informazioni, consulta Abilita IPv6 per le CloudFront distribuzioni.

Autenticazione reciproca

Opzionale. Puoi scegliere di attivare l'autenticazione reciproca per la tua CloudFront distribuzione. Per ulteriori informazioni, consulta Visualizzatore TLS reciproco (mTLS).

Abilita IPv6 le origini personalizzate (richieste di origine)

Quando utilizzi un'origine personalizzata (escluse le origini Amazon S3 e VPC), puoi personalizzare le impostazioni di origine per la tua distribuzione per scegliere come CloudFront connettersi alla tua origine utilizzando o gli indirizzi. IPv4 IPv6 Per ulteriori informazioni, consulta Abilita IPv6 per le CloudFront distribuzioni.

Comment

Opzionale. Quando crei una distribuzione, puoi includere un commento di 128 caratteri al massimo. Puoi aggiornare il commento in qualsiasi momento.

Distribution State (Stato distribuzione)

Indica se intendi attivare o disattivare la distribuzione implementata:

- Enabled (Attivata) significa che subito dopo l'implementazione della distribuzione, puoi distribuire i collegamenti che utilizzano il nome di dominio della distribuzione e gli utenti possono recuperare

il contenuto. Ogni volta che una distribuzione è attivata, CloudFront accetta e gestisce tutte le richieste utente finale di contenuto che utilizzano il nome di dominio associato a quella distribuzione.

Quando crei, modifichi o elimini una CloudFront distribuzione, ci vuole del tempo prima che le modifiche si propaghino nel database. CloudFront Una richiesta di informazioni immediata su una distribuzione potrebbe non visualizzare la modifica. La propagazione in genere viene completata in pochi minuti, ma una partizione di rete o un carico di sistema elevato potrebbe aumentare il tempo dell'operazione.

- Disabled (Disattivata) significa che anche se la distribuzione è implementata e pronta all'uso, gli utenti non possono utilizzarla. Ogni volta che una distribuzione è disabilitata, CloudFront non accetta alcuna richiesta dell'utente finale che utilizza il nome di dominio associato a quella distribuzione. Fino a che non modifichi lo stato della distribuzione da Disabled (Disattivata) a Enabled (Attivata) (aggiornando la configurazione della distribuzione), nessuno può utilizzare la distribuzione.

Puoi passare da uno stato all'altro della distribuzione tutte le volte che lo desideri. Segui la procedura di aggiornamento della configurazione di una distribuzione. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.

Custom Error Pages and Error Caching (Pagine di errore personalizzate e caching errori)

Puoi CloudFront restituire un oggetto al visualizzatore (ad esempio un file HTML) quando Amazon S3 o l'origine personalizzata restituisce un codice di stato HTTP 4xx o 5xx a. CloudFront Puoi anche specificare per quanto tempo una risposta di errore dall'origine o una pagina di errore personalizzata viene memorizzata nella cache edge. CloudFront Per ulteriori informazioni, consulta Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici.

> **Note**
>
> I seguenti valori non sono inclusi nella procedura guidata per la creazione di una distribuzione, quindi puoi configurare pagine di errore personalizzate solo quando aggiorni una distribuzione.

Argomenti

- Codice di errore HTTP
- Response Page Path (Percorso pagina risposta)
- Codice di risposta HTTP
- Error Caching Minimum TTL (seconds) (TTL minimo caching errori) (secondi)

Codice di errore HTTP

Il codice di stato HTTP per il quale desideri CloudFront restituire una pagina di errore personalizzata. È possibile CloudFront configurare la restituzione di pagine di errore personalizzate per nessuno, alcuni o tutti i codici di stato HTTP memorizzati nella CloudFront cache.

Response Page Path (Percorso pagina risposta)

Il percorso della pagina di errore personalizzata (ad esempio, `/4xx-errors/403-forbidden.html`) che CloudFront deve restituire a un visualizzatore quando la tua origine restituisce il codice di stato HTTP che hai specificato per Error Code (Codice errore), ad esempio 403. Se desideri archiviare gli oggetti e le pagine di errore personalizzate in posizioni differenti, la tua distribuzione deve includere un comportamento cache per il quale le seguenti condizioni sono vere:

- Il valore di Path Pattern (Modello di percorso) corrisponde al percorso dei tuoi messaggi di errore personalizzati. Ad esempio, hai salvato pagine di errore personalizzate per errori 4xx in un bucket Amazon S3 in una directory denominata `/4xx-errors`. La tua distribuzione deve includere un comportamento cache per il quale il modello di percorso instrada le richieste per le pagine di errore personalizzate a quella posizione, ad esempio /4xx-errors/*.
- Il valore di Origin (Origine) specifica il valore di Origin ID (ID origine) per l'origine che contiene le tue pagine di errore personalizzate.

Codice di risposta HTTP

Il codice di stato HTTP che desideri restituire CloudFront al visualizzatore insieme alla pagina di errore personalizzata.

Error Caching Minimum TTL (seconds) (TTL minimo caching errori) (secondi)

La quantità minima di tempo in cui desideri CloudFront memorizzare nella cache le risposte di errore dal server di origine.

Restrizioni geografiche

Se devi impedire agli utenti di determinati paesi di accedere ai tuoi contenuti, puoi configurare la CloudFront distribuzione con una lista consentita o una lista di blocco. Non sono previsti costi aggiuntivi per la configurazione delle restrizioni geografiche. Per ulteriori informazioni, consulta Limitazione della distribuzione geografica del contenuto.

Esecuzione del test di una distribuzione

Dopo aver creato la distribuzione, CloudFront sa dove si trova il server di origine e conosce il nome di dominio associato alla distribuzione. Per eseguire il test della distribuzione, procedi nel seguente modo:

1. Attendi che la distribuzione venga implementata.
   - Visualizza i Dettagli della distribuzione nella console. Quando la distribuzione è stata completata, il campo Ultima modifica cambia da Implementazione in corso a una data e un'ora.
2. Crea collegamenti ai tuoi oggetti con il nome di CloudFront dominio utilizzando la procedura seguente.
3. Provate i collegamenti. CloudFront fornisce gli oggetti alla pagina Web o all'applicazione.

Creazione di link agli oggetti

Utilizzate la procedura seguente per creare collegamenti di prova per gli oggetti nella vostra distribuzione CloudFront web.

Creazione di collegamenti a oggetti in una distribuzione Web

1. Copiate il seguente codice HTML in un nuovo file, *domain-name* sostituitelo con il nome di dominio della vostra distribuzione e *object-name* sostituitelo con il nome dell'oggetto.

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

```
</html>
```

Ad esempio, se il nome di dominio e l'oggetto fossero rispettivamente `d111111abcdef8.cloudfront.net` e `image.jpg`, l'URL per il collegamento sarebbe:

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

Se l'oggetto si trova in una cartella nel tuo server di origine, la cartella deve essere inclusa nell'URL. Ad esempio, se image.jpg si trova nella cartella delle immagini del server di origine, l'URL è:

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

2. Salva il codice HTML in un file con estensione .html.
3. Apri la pagina Web in un browser per assicurarti che l'oggetto sia visibile.

Il browser restituisce la pagina con il file di immagine incorporato, servito dalla posizione periferica CloudFront ritenuta appropriata per servire l'oggetto.

Aggiornamento di una distribuzione

Nella CloudFront console, puoi vedere le CloudFront distribuzioni associate alla tua Account AWS, visualizzare le impostazioni per una distribuzione e aggiornare la maggior parte delle impostazioni. Tieni presente che le modifiche alle impostazioni apportate non avranno effetto fino a quando la distribuzione non si sarà propagata alle posizioni edge di AWS .

Aggiornamento di una distribuzioni nella console

Le seguenti procedure mostrano come aggiornare una CloudFront distribuzione nella console.

Multi-tenant

Come aggiornare una distribuzione multi-tenant

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Cerca e scegli l’ID della distribuzione multi-tenant.
3. Seleziona la scheda relativa alle impostazioni che desideri aggiornare.

4. Effettua gli aggiornamenti, quindi, per salvare le modifiche, scegli Salva modifiche. Per ulteriori informazioni sulle impostazioni che puoi aggiornare, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

Puoi anche aggiornare una distribuzione utilizzando l' CloudFront API:

- Per aggiornare una distribuzione, UpdateDistributionconsulta Amazon CloudFront API Reference.

> **Important**
>
> Quando aggiorni la distribuzione, ricorda che sono necessari alcuni campi aggiuntivi non richiesti quando crei una distribuzione per la prima volta. Per assicurarti che tutti i campi obbligatori siano inclusi quando usi l' CloudFront API per aggiornare una distribuzione, segui i passaggi descritti UpdateDistributionin Amazon CloudFront API Reference.

Per modificare la distribuzione multi-tenant per un tenant di distribuzione, è necessario aggiornare il tenant di distribuzione. È inoltre possibile aggiornare il tenant di distribuzione per aggiornare il relativo dominio, certificato, personalizzazioni o valori dei parametri. Per ulteriori dettagli sull'aggiornamento del certificato del tenant di distribuzione, consulta Aggiunta di un dominio e di un certificato (tenant di distribuzione).

Come aggiornare un tenant di distribuzione

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. In SaaS, scegli Tenant di distribuzione.
3. Cerca il tenant di distribuzione. Utilizza il menu a discesa nella barra di ricerca per filtrare per dominio, nome, ID distribuzione, ID certificato, ID gruppo di connessioni o ID ACL Web.
4. Scegli il nome del tenant di distribuzione.
5. Per aggiornare i dettagli generali, scegli Modifica, effettua gli aggiornamenti e scegli Aggiorna tenant di distribuzione.
6. Scegli la scheda appropriata per tutte le altre impostazioni da aggiornare, effettua gli aggiornamenti e salvali. Per ulteriori informazioni sulle impostazioni del tenant di distribuzione che puoi personalizzare, consulta Personalizzazioni dei tenant di distribuzione.

Standard

Come aggiornare una distribuzione standard

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona l'ID di una distribuzione. L'elenco include tutte le distribuzioni associate all' AWS account utilizzato per accedere alla CloudFront console.
3. Per aggiornare le impostazioni generali, scegli Edit (Modifica). Altrimenti, scegli la scheda per le impostazioni che desideri aggiornare.
4. Esegui gli aggiornamenti, quindi scegli Salva modifiche. Per informazioni sui campi, consulta i seguenti argomenti:
   - General settings (Impostazioni generali: Distribution Settings (Impostazioni distribuzione)
   - Origin settings (Impostazioni di origine: Origin Settings (Impostazioni di origine)
   - Cache behavior settings (Impostazioni del comportamento della cache: Cache Behavior Settings (Impostazioni del comportamento della cache)
5. Se desideri eliminare un'origine nella distribuzione, procedi nel seguente modo:
   a. Scegli Behaviors (Comportamenti) e accertati di aver spostato eventuali comportamenti cache predefiniti associati con l'origine a un'altra origine.
   b. Scegli Origins (Origini), quindi seleziona un'origine.
   c. Scegliere Delete (Elimina).

Puoi anche aggiornare una distribuzione utilizzando l' CloudFront API:

- Per aggiornare una distribuzione, UpdateDistributionconsulta Amazon CloudFront API Reference.

> **Important**
>
> Quando aggiorni la distribuzione, ricorda che sono necessari alcuni campi aggiuntivi non richiesti per creare una distribuzione. Per assicurarti che tutti i campi obbligatori siano inclusi quando usi l' CloudFront API per aggiornare una distribuzione, segui i passaggi descritti UpdateDistributionin Amazon CloudFront API Reference.

Quando salvi le modifiche alla configurazione di distribuzione, CloudFront inizia a propagare le modifiche a tutte le edge location. Le successive modifiche alla configurazione si propagano nel rispettivo ordine. Finché la configurazione viene aggiornata in una edge location, CloudFront continua a servire i tuoi contenuti da quella posizione in base alla configurazione precedente. Quando la configurazione viene aggiornata in una edge location, CloudFront inizia immediatamente a servire i tuoi contenuti da quella posizione in base alla nuova configurazione.

Le modifiche non si propagano contemporaneamente a ogni posizione edge. Durante CloudFront la propagazione delle modifiche, non possiamo determinare se una determinata edge location sta servendo i tuoi contenuti sulla base della configurazione precedente o della nuova configurazione.

> **Note**
>
> In rari casi, quando un host o un link di rete viene interrotto, parte del traffico dei tenant di distribuzione potrebbe essere servito utilizzando configurazioni precedenti per un breve periodo di tempo, fino a quando le modifiche apportate non vengono applicate alla rete.

Per vedere quando le modifiche vengono propagate, visualizza i dettagli della distribuzione nella console. Il campo Ultima modifica cambia da Implementazione in corso a una data e un'ora al termine dell'implementazione.

Tagging di una distribuzione

I tag sono parole o frasi che puoi usare per identificare e organizzare le tue AWS risorse. È possibile aggiungere più tag a ogni risorsa e ogni tag include una chiave e un valore che definisci. Ad esempio, la chiave potrebbe essere "dominio" e il valore potrebbe essere "example.com". Puoi cercare e filtrare le tue risorse in base ai tag che aggiungi.

Puoi utilizzare i tag con CloudFront, ad esempio nei seguenti esempi:

- Applica le autorizzazioni basate su tag alle distribuzioni. CloudFront Per ulteriori informazioni, consulta ABAC con CloudFront.
- Monitora le informazioni di fatturazione in diverse categorie. Quando applichi tag a CloudFront distribuzioni o altre AWS risorse (come EC2 istanze Amazon o bucket Amazon S3) e attivi i tag AWS , genera un report di allocazione dei costi come valore separato da virgole (file CSV) con utilizzo e costi aggregati dai tag attivi.

Puoi applicare i tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari) per organizzare i costi tra più servizi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consultare Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

> **Note**
>
> - Puoi aggiungere dei tag alle distribuzioni, ma non alle identità di accesso origine o agli invalidamenti.
> - Tag Editor e i gruppi di risorse non sono attualmente supportati per. CloudFront
> - Per conoscere il numero massimo corrente relativo al numero di tag che puoi aggiungere a una distribuzione, consulta Quote generali.

Indice

Limitazioni applicate ai tag

Ai tag si applicano le seguenti limitazioni di base:

- Per il numero massimo di tag per distribuzione, consulta Quote generali.
- Lunghezza massima della chiave: 128 caratteri Unicode
- lunghezza massima del valore: 256 caratteri Unicode;
- Valori validi per la chiave e il valore - a-z, A-Z, 0-9, spazi e i seguenti caratteri: _ . : / = + - e @
- Chiavi e valori di tag fanno distinzione tra maiuscole e minuscole
- Non utilizzare `aws:` come prefisso per le chiavi. Questo prefisso è riservato per l'uso di AWS .

Aggiunta, modifica ed eliminazione di tag per distribuzioni

Puoi utilizzare la CloudFront console per gestire i tag per le tue distribuzioni.

Aggiunta, modifica o eliminazione di tag per una distribuzione

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli l'ID della distribuzione che intendi aggiornare.
3. Seleziona la scheda Tag.
4. Scegliere Gestisci tag.
5. Nella pagina Gestisci tag, è possibile:
   - Per aggiungere un tag, inserisci una chiave e, facoltativamente, un valore per il tag. Seleziona Aggiungi nuovo tag per aggiungere altri tag.
   - Per modificare un tag, modificare la chiave del tag o il suo valore o entrambi. Puoi eliminare il valore per un tag, ma la chiave è obbligatoria.
   - Per rimuovere un tag, scegli Rimuovi.
6. Scegli Save changes (Salva modifiche).

Tagging programmatico

Puoi anche utilizzare l' CloudFront API, AWS Command Line Interface (AWS CLI) e AWS Tools for Windows PowerShell per applicare i tag. AWS SDKs Per ulteriori informazioni, consulta i seguenti argomenti:

- CloudFront Operazioni API:
  - ListTagsForResource
  - TagResource
  - UntagResource
- AWS CLI — Vedi cloudfront nel Command Reference AWS CLI
- AWS SDKs — Consulta la documentazione SDK applicabile nella pagina Documentazione AWS
- Strumenti per Windows PowerShell : consulta Amazon CloudFront nella guida di riferimento ai AWS Strumenti per PowerShell cmdlet

Eliminazione di una distribuzione

La procedura seguente elimina una distribuzione utilizzando la CloudFront console. Per informazioni sull'eliminazione con l' CloudFront API, consulta DeleteDistributionAmazon CloudFront API Reference.

Se devi eliminare una distribuzione con un OAC collegato a un bucket S3, consulta Eliminazione di una distribuzione con un OAC collegato a un bucket S3 per dettagli importanti.

⚠ Warning

- Prima di eliminare una distribuzione devi disabilitarla e pertanto è necessaria l'autorizzazione per aggiornare la distribuzione. Una volta eliminata, una distribuzione non può essere recuperata.
- Se disabiliti una distribuzione a cui è associato un nome di dominio alternativo, CloudFront smette di accettare il traffico per quel nome di dominio (ad esempio www.example.com), anche se un'altra distribuzione ha un nome di dominio alternativo con un carattere jolly (*) che corrisponde allo stesso dominio (ad esempio*.example.com).

Multi-tenant

Prima di poter eliminare una distribuzione multi-tenant, è necessario eliminare tutti i tenant di distribuzione associati.

Come eliminare una distribuzione multi-tenant

1. Accedi a e apri la console all'indirizzo. Console di gestione AWS CloudFront https://console.aws.amazon.com/cloudfront/v4/home
2. Nel riquadro destro della CloudFront console, scegli il nome della distribuzione multi-tenant che desideri eliminare.
3. Per Tenant, seleziona ed elimina tutti i tenant di distribuzione associati.
4. Scegli Disabilita per disabilitare la distribuzione e seleziona Disabilita distribuzione per confermare.
5. Attendi fino a quando il nuovo timestamp non viene visualizzato nella colonna Ultima modifica.

- Potrebbero essere necessari alcuni minuti prima che la modifica CloudFront venga propagata in tutte le edge location.

6. Scegli Elimina, Elimina distribuzione.

Come eliminare un tenant di distribuzione

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. In SaaS, scegli Tenant di distribuzione.
3. Cerca il tenant di distribuzione. Utilizza il menu a discesa nella barra di ricerca per filtrare per dominio, nome, ID distribuzione, ID certificato, ID gruppo di connessioni o ID ACL Web.
4. Seleziona il tenant di distribuzione da eliminare.
5. Scegli Elimina tenant, Elimina tenant di distribuzione.

Standard

Come eliminare una distribuzione standard

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro destro della CloudFront console, trova la distribuzione che desideri eliminare.
   - Se la colonna Stato mostra che la distribuzione è già Disabilitata, passa alla fase 6.
   - Se lo Stato mostra Abilitata ma la distribuzione mostra ancora Implementazione in corso nella colonna Ultima modifica, attendi il termine dell'implementazione prima di continuare con la fase 3.
3. Nel riquadro destro della CloudFront console, seleziona la casella di controllo relativa alla distribuzione che desideri eliminare.
4. Fai clic su Disable (Disabilita) per disabilitare la distribuzione e scegli Yes, Disable (Sì, disabilita) per confermare. Quindi seleziona Close (Chiudi).
   - Il valore della colonna Stato cambia immediatamente in Disabilitata.
5. Attendi fino a quando il nuovo timestamp non viene visualizzato nella colonna Ultima modifica.

- Potrebbero essere necessari alcuni minuti prima che la modifica CloudFront venga propagata a tutte le edge location.

6. Seleziona la casella di controllo corrispondente alla distribuzione da eliminare.
7. Scegli Delete (Elimina), poi Delete (Elimina).

   - Se l'opzione Elimina non è disponibile, significa che la modifica CloudFront viene ancora propagata alle posizioni dei bordi. Attendi fino a quando il nuovo timestamp non viene visualizzato nella colonna Ultima modifica, quindi ripeti le fasi 6-7.

Usa origini diverse con le distribuzioni CloudFront

Quando si crea una distribuzione, si specifica l'origine a cui CloudFront inviare le richieste per i file. È possibile utilizzare diversi tipi di origini con CloudFront. Ad esempio, puoi utilizzare un bucket Amazon S3, un MediaStore contenitore, un MediaPackage canale, un Application Load Balancer o l'URL di una funzione. AWS Lambda Quando crei la tua CloudFront distribuzione, configura CloudFront automaticamente la maggior parte delle impostazioni di distribuzione per te, in base al tipo di origine del contenuto. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione preconfigurate.

Se hai un'Application Load Balancer, Network Load Balancer EC2 o un'istanza in una sottorete privata, puoi usarla come origine VPC. Con le origini VPC, è possibile accedere alle applicazioni solo in una sottorete privata con una CloudFront distribuzione, che impedisce all'applicazione di essere accessibile sulla rete Internet pubblica. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso con VPC Origins”.

> **Note**
>
> Puoi utilizzare le funzioni edge per selezionare dinamicamente l’origine appropriata per ogni richiesta. Utilizzando CloudFront Functions o Lambda @Edge, puoi indirizzare le richieste a origini diverse in base a fattori quali la posizione geografica del visualizzatore, le intestazioni della richiesta o i parametri della stringa di query. Per ulteriori informazioni, consulta Personalizzazione a livello di edge con le funzioni.

Argomenti

- Utilizzo di bucket Amazon S3

- Usa un MediaStore contenitore o un canale MediaPackage
- Utilizzo di un Application Load Balancer
- Utilizzo di un Network Load Balancer
- Utilizzo dell'URL di una funzione Lambda
- Usa Amazon EC2 (o un'altra origine personalizzata)
- Usa i gruppi di CloudFront origine
- Utilizzo di Gateway Amazon API

Utilizzo di bucket Amazon S3

I seguenti argomenti descrivono i diversi modi in cui è possibile utilizzare un bucket Amazon S3 come origine per una distribuzione. CloudFront

Argomenti

- Utilizzo di un bucket Amazon S3 standard
- Utilizzo di Lambda per oggetti Amazon S3
- Utilizzo di punti di accesso Amazon S3
- Utilizzo di un bucket Amazon S3 configurato come un endpoint del sito web
- Aggiungi CloudFront a un bucket Amazon S3 esistente
- Sposta un bucket Amazon S3 in un altro Regione AWS

Utilizzo di un bucket Amazon S3 standard

Quando usi Amazon S3 come origine per la tua distribuzione, metti gli oggetti che desideri distribuire in un CloudFront bucket Amazon S3. Puoi utilizzare qualsiasi metodo supportato da Amazon S3 per inserire gli oggetti in Amazon S3. Ad esempio, puoi utilizzare la console di Amazon S3 o l'API o uno strumento di terze parti. Puoi creare una gerarchia nel bucket per archiviare gli oggetti, esattamente come per qualsiasi altro bucket Amazon S3 standard.

L'utilizzo di un bucket Amazon S3 esistente come server di CloudFront origine non modifica in alcun modo il bucket; puoi comunque utilizzarlo come faresti normalmente per archiviare e accedere a oggetti Amazon S3 al prezzo standard di Amazon S3. L'archiviazione di oggetti nel bucket è soggetta ai costi abituali di Amazon S3. Per ulteriori informazioni sui costi da utilizzare CloudFront, consulta la pagina CloudFrontdei prezzi di Amazon. Per ulteriori informazioni sull'utilizzo CloudFront con

un bucket S3 esistente, consulta. the section called “Aggiungi CloudFront a un bucket Amazon S3 esistente”

> **Important**
>
> Affinché il bucket funzioni CloudFront, il nome deve essere conforme ai requisiti di denominazione DNS. Per ulteriori informazioni, consulta Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Quando specifichi un bucket Amazon S3 come origine per CloudFront, ti consigliamo di utilizzare il seguente formato:

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

Quando specifichi il nome di bucket in questo formato, puoi utilizzare le seguenti caratteristiche di CloudFront :

- Configura CloudFront per comunicare con il tuo bucket Amazon S3 tramite SSL/TLS. Per ulteriori informazioni, consulta the section called “Usa HTTPS con CloudFront”.
- Utilizza un controllo dell'accesso all'origine per richiedere che gli spettatori accedano ai tuoi contenuti utilizzando CloudFront URLs e non utilizzando Amazon URLs S3. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.
- Aggiorna il contenuto del tuo bucket inviando POST e richiedendo a. PUT CloudFront Per ulteriori informazioni, consulta the section called “Metodi HTTP” nell'argomento the section called “In che modo CloudFront elabora e inoltra le richieste alla tua origine Amazon S3”.

Non specificare il bucket utilizzando i seguenti formati:

- Lo stile del percorso Amazon S3: s3.amazonaws.com/*bucket-name*
- Il CNAME di Amazon S3

> **Note**
>
> CloudFront supporta S3 Origins utilizzando qualsiasi classe di storage, inclusa S3 Intelligent-Tiering. Quando CloudFront richiede oggetti da un'origine S3, gli oggetti vengono recuperati indipendentemente dal livello di storage in cui risiedono attualmente. L'utilizzo CloudFront

con S3 Intelligent-Tiering non influisce sulle prestazioni o sulla funzionalità della distribuzione. Per ulteriori informazioni, consulta Gestione dei costi di archiviazione con Piano intelligente Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Utilizzo di Lambda per oggetti Amazon S3

Quando crei un punto di accesso Lambda per oggetti, Amazon S3 genera automaticamente un alias univoco per il tuo punto di accesso Lambda per oggetti. Puoi usare questo alias al posto del nome di un bucket Amazon S3 come origine per la tua distribuzione. CloudFront

Quando utilizzi un alias Object Lambda Access Point come origine per CloudFront, ti consigliamo di utilizzare il seguente formato:

alias.s3.*region*.amazonaws.com

Per ulteriori informazioni sull'esito di *alias*, consultare Come utilizzare un'alias stile bucket per il punto di accesso Lambda per oggetti del bucket S3 nella Guida per l'utente di Amazon S3.

Important

Quando si utilizza un punto di accesso Object Lambda come origine per CloudFront, è necessario utilizzare il controllo di accesso all'origine.

Per un caso d'uso di esempio, consulta Usare Amazon S3 Object Lambda con CloudFront Amazon per personalizzare i contenuti per gli utenti finali.

CloudFront tratta l'origine di un punto di accesso Object Lambda allo stesso modo dell'origine di un bucket Amazon S3 standard.

Se utilizzi Lambda per oggetti Amazon S3 come origine per la distribuzione, devi configurare le seguenti quattro autorizzazioni.

Object Lambda Access Point

Come aggiungere le autorizzazioni per il punto di accesso Lambda per oggetti

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/

2. Nel pannello di navigazione, scegli Punti di accesso Lambda dell'oggetto.
3. Scegli il punto di accesso Lambda per oggetti che desideri utilizzare.
4. Scegli la scheda Autorizzazioni.
5. Scegli Modifica nella sezione Policy del punto di accesso per le espressioni Lambda dell'oggetto.
6. Incolla la seguente policy nel campo Policy.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3-object-lambda:Get*",
            "Resource": "arn:aws:s3-object-lambda:us-
east-1:123456789012:accesspoint/Object-Lambda-Access-Point-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-
ID"
                }
            }
        }
    ]
}
```

7. Scegli Save changes (Salva modifiche).

Amazon S3 Access Point

Come aggiungere autorizzazioni per il punto di accesso Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/

2. Nel pannello di navigazione, scegli Punti di accesso.
3. Scegli il Punto di accesso Amazon S3 che desideri utilizzare.
4. Scegli la scheda Autorizzazioni.
5. Scegli Modifica nella sezione Policy del punto di accesso.
6. Incolla la seguente policy nel campo Policy.

   JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name/object/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "s3-object-lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

7. Scegli Save (Salva).

Amazon S3 bucket

Come aggiungere autorizzazioni al bucket Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il bucket Amazon S3 che desideri utilizzare.
4. Scegli la scheda Autorizzazioni.
5. Scegli Modifica nella sezione Policy bucket.
6. Incolla la seguente policy nel campo Policy.

   JSON

```
{
    "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. Scegli Save changes (Salva modifiche).

AWS Lambda function

Come aggiungere autorizzazioni alla funzione Lambda

1. Accedi Console di gestione AWS e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nel riquadro di navigazione, seleziona Funzioni.
3. Scegli la AWS Lambda funzione che desideri utilizzare.
4. Scegli la scheda Configurazione, quindi Autorizzazioni.
5. Scegli Aggiungi autorizzazioni nella sezione Istruzioni di policy basate su risorse.
6. Scegli Account AWS.
7. Inserisci un nome per ID istruzione.
8. Inserisci `cloudfront.amazonaws.com` per Principale.
9. Scegli `lambda:InvokeFunction` dal menu a discesa Operazione.
10. Scegli Save (Salva).

Utilizzo di punti di accesso Amazon S3

Quando utilizzi un punto di accesso S3, Amazon S3 genera automaticamente un alias univoco. Puoi usare questo alias al posto del nome di un bucket Amazon S3 come origine per la tua distribuzione. CloudFront

Quando utilizzi un alias di Amazon S3 Access Point come origine per CloudFront, ti consigliamo di utilizzare il seguente formato:

`alias``.s3.`*`region`*`.amazonaws.com`

Per ulteriori informazioni sulla ricerca dell'*`alias`*, consulta Utilizzo di un alias di tipo bucket per il punto di accesso al bucket S3 nella Guida per l'utente di Amazon S3.

> **Important**
>
> Quando utilizzi un punto di accesso Amazon S3 come origine per CloudFront, devi utilizzare il controllo degli accessi di origine.

CloudFront tratta l'origine di un punto di accesso Amazon S3 allo stesso modo dell'origine di un bucket Amazon S3 standard.

Se utilizzi Lambda per oggetti Amazon S3 come origine per la distribuzione, devi configurare le seguenti due autorizzazioni.

Amazon S3 Access Point

Come aggiungere autorizzazioni per il Punto di accesso Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nel pannello di navigazione, scegli Punti di accesso.
3. Scegli il Punto di accesso Amazon S3 che desideri utilizzare.
4. Scegli la scheda Autorizzazioni.
5. Scegli Modifica nella sezione Policy del punto di accesso.
6. Incolla la seguente policy nel campo Policy.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-Point-name/object/*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-ID"}
            }
```

```
        }
    ]
}
```

7. Scegli Save (Salva).

Amazon S3 bucket

Come aggiungere autorizzazioni al bucket Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il bucket Amazon S3 che desideri utilizzare.
4. Scegli la scheda Autorizzazioni.
5. Scegli Modifica nella sezione Policy bucket.
6. Incolla la seguente policy nel campo Policy.

   JSON

```
{
    "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. Scegli Save changes (Salva modifiche).

Utilizzo di un bucket Amazon S3 configurato come un endpoint del sito web

Puoi utilizzare un bucket Amazon S3 configurato come endpoint del sito Web come origine personalizzata con. CloudFront Quando configuri la CloudFront distribuzione, come origine, inserisci l'endpoint di hosting di siti Web statici Amazon S3 per il tuo bucket. Tale valore viene visualizzato nella console di Amazon S3, nella pagina Properties (Proprietà) nel pannello Static Website Hosting (Hosting sito Web statico). Ad esempio:

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

Per ulteriori informazioni sulla specifica degli endpoint statici di siti Web Amazon S3, consulta Endpoint dei siti Web nella Guida per l'utente di Amazon Simple Storage Service.

Quando specifichi il nome di bucket in questo formato come origine, puoi utilizzare reindirizzamenti di Amazon S3 e documenti di errore personalizzati di Amazon S3. Per ulteriori informazioni, consulta Configurazione di un documento di errore personalizzato e Configurazione di un reindirizzamento nella Guida per l'utente di Amazon Simple Storage Service. (fornisce CloudFront anche pagine di errore personalizzate. Per ulteriori informazioni, vederethe section called “Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici”.)

L'utilizzo di un bucket Amazon S3 come server di CloudFront origine non modifica in alcun modo il bucket. È comunque possibile utilizzarlo come faresti normalmente, sulla base delle normali tariffe Amazon S3. Per ulteriori informazioni sui costi da utilizzare CloudFront, consulta la pagina CloudFront dei prezzi di Amazon.

> **Note**
>
> Se utilizzi l' CloudFront API per creare la tua distribuzione con un bucket Amazon S3 configurato come endpoint del sito Web, devi configurarlo utilizzando`CustomOriginConfig`, anche se il sito Web è ospitato in un bucket Amazon S3. Per ulteriori informazioni sulla creazione di distribuzioni utilizzando l'CloudFront API, consulta CreateDistributionAmazon CloudFront API Reference.

Aggiungi CloudFront a un bucket Amazon S3 esistente

Se memorizzi i tuoi oggetti in un bucket Amazon S3, puoi fare in modo che gli utenti ottengano i tuoi oggetti direttamente da S3 oppure puoi configurare la configurazione CloudFront per ottenere i tuoi oggetti da S3 e poi distribuirli ai tuoi utenti. L'utilizzo CloudFront può essere più conveniente se gli utenti accedono frequentemente ai tuoi oggetti perché, a un utilizzo più elevato, il prezzo del trasferimento CloudFront dei dati è inferiore al prezzo del trasferimento dati di Amazon S3. Inoltre, i download sono più rapidi CloudFront rispetto al solo Amazon S3, perché gli oggetti vengono archiviati più vicino agli utenti.

> **Note**
>
> Se desideri CloudFront rispettare le impostazioni di condivisione delle risorse tra origini diverse di Amazon S3, configura l'inoltro dell'`Origin`intestazione CloudFront ad Amazon S3. Per ulteriori informazioni, consulta the section called “Caching dei contenuti in base alle intestazioni di richiesta”.

Se attualmente distribuisci contenuti direttamente dal tuo bucket Amazon S3 utilizzando il tuo nome di dominio (ad esempio example.com) anziché il nome di dominio del tuo bucket Amazon S3 (ad esempio amzn-s3-demo-bucket. s3.us-west-2.amazonaws.com), puoi aggiungerli senza interruzioni utilizzando la procedura seguente. CloudFront

Da aggiungere CloudFront quando stai già distribuendo i tuoi contenuti da Amazon S3

1. Crea una CloudFront distribuzione. Per ulteriori informazioni, consulta the section called “Creazione di una distribuzione”.

   Quando crei la distribuzione, specifica il nome del tuo bucket Amazon S3 come server di origine.

   > **Important**
   >
   > Affinché il bucket funzioni CloudFront, il nome deve essere conforme ai requisiti di denominazione DNS. Per ulteriori informazioni, consulta Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

   Se usi un CNAME con Amazon S3, specifica anche il CNAME per la tua distribuzione.

2. Crea una pagina Web di test che contenga i link agli oggetti leggibili pubblicamente nel bucket Amazon S3 ed esegui il test dei collegamenti. Per questo test iniziale, utilizzate il nome di CloudFront dominio della vostra distribuzione nell'oggetto URLs, ad esempio. `https://d111111abcdef8.cloudfront.net/images/image.jpg`

   Per ulteriori informazioni sul formato di CloudFront URLs, vederethe section called “Personalizzazione degli URL dei file”.

3. Se utilizzi Amazon S3 CNAMEs, l'applicazione utilizza il tuo nome di dominio (ad esempio, example.com) per fare riferimento agli oggetti nel tuo bucket Amazon S3 anziché utilizzare il nome del tuo bucket (ad esempio, amzn-s3-demo-bucket.s3.amazonaws.com). Per continuare a utilizzare il nome di dominio per fare riferimento agli oggetti anziché utilizzare il nome di CloudFront dominio per la distribuzione (ad esempio, d111111abcdef8.cloudfront.net), devi aggiornare le impostazioni con il tuo provider di servizi DNS.

   Affinché Amazon S3 CNAMEs funzioni, il tuo provider di servizi DNS deve avere un record di risorse CNAME impostato per il tuo dominio che attualmente indirizza le query per il dominio al tuo bucket Amazon S3. Ad esempio, se un utente richiede questo oggetto:

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

   La richiesta viene automaticamente reindirizzata e l'utente vede questo oggetto:

   `https://amzn-s3-demo-bucket.s3.amazonaws.com/images/image.jpg`

   Per indirizzare le query alla tua CloudFront distribuzione anziché al tuo bucket Amazon S3, devi utilizzare il metodo fornito dal tuo provider di servizi DNS per aggiornare il record di risorse CNAME impostato per il tuo dominio. Questo record CNAME aggiornato reindirizza le query DNS dal tuo dominio al nome di dominio per la tua distribuzione. CloudFront Per ulteriori informazioni, consulta la documentazione del tuo fornitore di servizi DNS.

   > **Note**
   >
   > Se usi Route 53 come servizio DNS, puoi utilizzare un set di record di risorse CNAME o un set di record di risorse alias. Per informazioni sulla modifica dei set di record di risorse, consulta Modifica dei set di record. Per informazioni sui set di record di risorse alias, consulta Scelta tra record alias e non alias. Entrambi gli argomenti sono riportati nella Guida per gli sviluppatori di Amazon Route 53.

Per ulteriori informazioni sull'utilizzo di with, consulta. CNAMEs CloudFront the section called "Usa personalizzato URLs"

Dopo aver aggiornato il set di record di risorse CNAME, possono essere necessarie fino a 72 ore affinché la modifica si propaghi per tutto il sistema DNS, anche se in genere i tempi sono più rapidi. Durante questo periodo, alcune richieste per i tuoi contenuti continueranno a essere indirizzate al tuo bucket Amazon S3 e altre verranno indirizzate a. CloudFront

Sposta un bucket Amazon S3 in un altro Regione AWS

Se utilizzi Amazon S3 come origine per una CloudFront distribuzione e sposti il bucket in un'altra Regione AWS, l'aggiornamento dei record per utilizzare la nuova regione CloudFront può richiedere fino a un'ora se si verificano entrambe le seguenti condizioni:

- Stai utilizzando un'identità di accesso all' CloudFront origine (OAI) per limitare l'accesso al bucket.
- Puoi spostare il bucket a una regione Amazon S3 che richiede Signature Version 4 per l'autenticazione

Quando usi OAIs, CloudFront utilizza la regione (tra gli altri valori) per calcolare la firma che usa per richiedere oggetti dal tuo bucket. Per ulteriori informazioni su OAIs, consultathe section called "Utilizzo di un'identità di accesso origine (legacy, non consigliata)". Per un elenco di quelle Regioni AWS che supportano la versione 2 di Signature, consulta la procedura di firma della versione 2 di Signature in Riferimenti generali di Amazon Web Services.

Per forzare un aggiornamento più rapido dei record, puoi aggiornare la tua CloudFront distribuzione, ad esempio, aggiornando il campo Descrizione nella scheda Generale della CloudFront console. CloudFront Quando aggiorni una distribuzione, controlla CloudFront immediatamente la regione in cui si trova il bucket. La propagazione della modifica a tutte le posizioni edge dovrebbe richiedere solo pochi minuti.

Usa un MediaStore contenitore o un canale MediaPackage

Per lo streaming di video CloudFront, puoi configurare un bucket Amazon S3 configurato come MediaStore contenitore o creare un canale e degli endpoint con. MediaPackage Quindi crei e configuri una distribuzione CloudFront per lo streaming del video.

Per ulteriori informazioni e step-by-step istruzioni, consulta i seguenti argomenti:

- the section called “Pubblica video utilizzandolo AWS Elemental MediaStore come origine”
- the section called “Distribuzione di video live formattati con AWS Elemental MediaPackage”

Utilizzo di un Application Load Balancer

È possibile utilizzarlo CloudFront per indirizzare il traffico verso Application Load Balancer interni e collegati a Internet.

Se la tua origine è uno o più server HTTP (S) (server Web) ospitati su una o più EC2 istanze Amazon, puoi scegliere di utilizzare un Application Load Balancer con accesso a Internet per distribuire il traffico alle istanze. Un bilanciatore del carico connesso a Internet ha un nome DNS risolvibile pubblicamente e instrada le richieste dei client verso le destinazioni su Internet.

Per ulteriori informazioni sull'utilizzo di un Application Load Balancer con accesso a Internet come origine CloudFront per, incluso come assicurarsi che gli utenti possano accedere ai server Web solo CloudFront tramite e non accedendo direttamente al load balancer, consulta. the section called “Limitazione dell’accesso ad Application Load Balancer”

In alternativa, puoi utilizzare VPC Origins per distribuire contenuti da applicazioni ospitate con un Application Load Balancer interno nelle sottoreti private del cloud privato virtuale (VPC). VPC Origins impedisce che la applicazione sia accessibile sulla rete Internet pubblica. Per ulteriori informazioni, consulta Limitazione dell’accesso con VPC Origins.

Utilizzo di un Network Load Balancer

Puoi utilizzare Network Load Balancer interni e con accesso a Internet con Amazon. CloudFront È possibile utilizzare Network Load Balancer interni all'interno di sottoreti private CloudFront utilizzando origini VPC. CloudFront Le origini VPC consentono di servire contenuti da applicazioni ospitate in sottoreti VPC private senza esporli alla rete Internet pubblica. Per ulteriori informazioni, consulta Limitazione dell’accesso con VPC Origins.

In alternativa, puoi utilizzarlo anche CloudFront per distribuire traffico da Network Load Balancer con accesso a Internet. Un sistema di bilanciamento del carico connesso a Internet ha un nome DNS risolvibile pubblicamente e può ricevere richieste sia dai client su Internet che dalle distribuzioni. CloudFront

Utilizzo dell'URL di una funzione Lambda

L'URL di una funzione Lambda è un endpoint HTTPS dedicato per una funzione Lambda. Puoi utilizzare l'URL di una funzione Lambda per creare un'applicazione web serverless interamente all'interno di Lambda. È possibile richiamare l'applicazione Web Lambda direttamente tramite l'URL della funzione, senza necessità di integrarsi con API Gateway o Application Load Balancer.

Se crei un'applicazione web serverless utilizzando le funzioni Lambda con URLs funzione, puoi CloudFront aggiungere per ottenere i seguenti vantaggi:

- Accelera la tua applicazione inserendo nella cache i contenuti più vicini ai visualizzatori
- Utilizza un nome di dominio personalizzati per l'applicazione Web
- Indirizza percorsi URL diversi a diverse funzioni Lambda utilizzando CloudFront i comportamenti della cache
- Blocca richieste specifiche utilizzando restrizioni CloudFront geografiche o AWS WAF (o entrambe)
- AWS WAF Usalo con CloudFront per proteggere l'applicazione da bot dannosi, prevenire gli exploit più comuni delle applicazioni e migliorare la protezione dagli DDo attacchi S

Per utilizzare l'URL di una funzione Lambda come origine per una CloudFront distribuzione, specifica il nome di dominio completo dell'URL della funzione Lambda come dominio di origine. Un nome di dominio URL della funzione Lambda utilizza il formato seguente:

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

Quando si utilizza l'URL di una funzione Lambda come origine per una CloudFront distribuzione, l'URL della funzione deve essere accessibile pubblicamente. A tale scopo, usa una delle seguenti opzioni:

- Se utilizzi Origin Access Control (OAC), il `AuthType` parametro dell'URL della funzione Lambda deve utilizzare `AWS_IAM` il valore e consentire `lambda:InvokeFunctionUrl` le autorizzazioni e in una `lambda:InvokeFunction` policy basata sulle risorse. Per ulteriori informazioni sull'utilizzo della funzione Lambda URLs per OAC, vedere. Limitazione dell'accesso all'origine dell'URL di una funzione AWS Lambda
- Se non utilizzi OAC, puoi impostare il parametro `AuthType` della funzione URL su `NONE` e consentire l'autorizzazione `lambda:InvokeFunctionUrl` in una policy basata su risorse.

Puoi anche aggiungere un'intestazione di origine personalizzata alle richieste CloudFront inviate all'origine e scrivere codice di funzione per restituire una risposta di errore se l'intestazione non è presente nella richiesta. Questo aiuta a garantire che gli utenti possano accedere all'applicazione Web solo tramite CloudFront, e non direttamente utilizzando l'URL della funzione Lambda.

Per ulteriori informazioni sulla funzione Lambda URLs, consulta i seguenti argomenti nella Guida per gli AWS Lambda sviluppatori:

- Funzione Lambda URLs: una panoramica generale della funzione Lambda URLs
- Invocare la URLs funzione Lambda: include dettagli sui payload di richiesta e risposta da utilizzare per codificare l'applicazione Web serverless
- Modello di sicurezza e autenticazione per la URLs funzione Lambda: include dettagli sui tipi di autenticazione Lambda

Usa Amazon EC2 (o un'altra origine personalizzata)

Con Amazon puoi utilizzare EC2 istanze interne e con accesso a Internet. CloudFront È possibile utilizzare EC2 istanze interne all'interno di sottoreti private CloudFront utilizzando origini VPC. CloudFront Le origini VPC consentono di servire contenuti da applicazioni ospitate in sottoreti VPC private senza esporli alla rete Internet pubblica. Per ulteriori informazioni, consulta Limitazione dell’accesso con VPC Origins.

Un’origine personalizzata è un server web HTTP(S) con un nome DNS risolvibile pubblicamente che instrada le richieste dei client verso le destinazioni su Internet. Il server HTTP (S) può essere ospitato su, ad AWS esempio, un' EC2 istanza Amazon, o ospitato altrove. Un'origine Amazon S3 configurata come endpoint di un sito Web è considerata anch'essa un'origine personalizzata. Per ulteriori informazioni, consulta the section called “Utilizzo di un bucket Amazon S3 configurato come un endpoint del sito web”.

Quando utilizzi il tuo server HTTP come origine personalizzata, specifichi il nome DNS del server, insieme alle porte HTTP e HTTPS e al protocollo che desideri utilizzare CloudFront per recuperare oggetti dalla tua origine.

La maggior parte delle CloudFront funzionalità è supportata quando si utilizza un'origine personalizzata ad eccezione dei contenuti privati. Sebbene sia possibile utilizzare un URL firmato per distribuire contenuti da un'origine personalizzata, per accedere CloudFront all'origine personalizzata, l'origine deve rimanere accessibile al pubblico. Per ulteriori informazioni, consulta the section called “Limita i contenuti con cookie firmati URLs e firmati”.

Segui queste linee guida per utilizzare EC2 le istanze Amazon e altre origini personalizzate conCloudFront.

- Effettua l'hosting e distribuisci gli stessi contenuti su tutti i server di distribuzione di contenuti per la stessa origine CloudFront. Per ulteriori informazioni, consulta the section called “Origin Settings (Impostazioni di origine)” nell'argomento the section called “Tutte le impostazioni distribuzione”.
- Registra le voci di `X-Amz-Cf-Id` intestazione su tutti i server in caso di necessità Supporto o CloudFront per utilizzare questo valore per il debug.
- Limita le richieste alle porte HTTP e HTTPS sulle quali la tua origine personalizzata è in ascolto.
- Sincronizza gli orologi di tutti i server nella tua implementazione. Tieni presente che CloudFront utilizza il Coordinated Universal Time (UTC) per i cookie firmati URLs e firmati, per i log e i report. Inoltre, se monitori CloudFront l'attività utilizzando le CloudWatch metriche, tieni presente che utilizza CloudWatch anche l'UTC.
- Utilizza server ridondanti per gestire gli errori.
- Per ulteriori informazioni sull'utilizzo di un'origine personalizzata per servire contenuto privato, consulta the section called “Limitazione dell’accesso ai file su origini personalizzate”.
- Per informazioni sul comportamento di richieste e risposte e sui codici di stato HTTP supportati, consulta Comportamento di richieste e risposte.

Se utilizzi Amazon EC2 per un'origine personalizzata, ti consigliamo di fare quanto segue:

- Utilizza Immagine macchina Amazon che installa automaticamente il software per un server Web. Per ulteriori informazioni, consulta la EC2 documentazione di Amazon.
- Usa un load balancer ELB per gestire il traffico su più EC2 istanze Amazon e isolare la tua applicazione dalle modifiche alle istanze Amazon. EC2 Ad esempio, se utilizzi un sistema di bilanciamento del carico, puoi aggiungere ed eliminare EC2 istanze Amazon senza modificare l'applicazione. Per ulteriori informazioni, consulta la documentazione ELB.
- Quando crei la tua CloudFront distribuzione, specifica l'URL del load balancer per il nome di dominio del tuo server di origine. Per ulteriori informazioni, consulta the section called “Creazione di una distribuzione”.

Usa i gruppi di CloudFront origine

È possibile specificare un gruppo di origine per l' CloudFront origine se, ad esempio, si desidera configurare il failover di origine per scenari in cui è necessaria un'elevata disponibilità. Utilizza il

failover di origine per designare un'origine primaria CloudFront più una seconda origine che passa CloudFront automaticamente a quando l'origine primaria restituisce risposte di errore specifiche del codice di stato HTTP.

Per ulteriori informazioni, inclusi i passaggi per la configurazione di un gruppo di origine, consulta the section called “Aumento della disponibilità con il failover di origine”.

Utilizzo di Gateway Amazon API

Puoi utilizzare API Gateway come origine personalizzata per la tua CloudFront distribuzione. Per ulteriori informazioni, consulta i seguenti argomenti:

- Proteggere Amazon API Gateway con cifrari sicuri utilizzando il post del blog di Amazon CloudFront AWS
- Come posso configurare API Gateway con la mia CloudFront distribuzione? AWS re:Post

Abilita IPv6 per le CloudFront distribuzioni

Amazon CloudFront supporta sia IPv4 IPv6 i clienti che le AWS edge location. CloudFront supporta anche la IPv6 connettività dual-stack (IPv4 e IPv6) verso le origini. Questo ti aiuta a raggiungere la consegna. end-to-end IPv6

IPv6 è il protocollo Internet di nuova generazione progettato per sostituire. IPv4 Mentre IPv4 utilizza indirizzi a 32 bit (come 192.0.2.44), IPv6 utilizza indirizzi a 128 bit (come 2001:0 db 8:85 a3: :8a2e: 0370:7334). IPv6 offre uno spazio di indirizzi esteso per ospitare più dispositivi connessi a Internet.

Argomenti

- IPv6 richieste dei visualizzatori
- IPv6 richieste di origine

IPv6 richieste dei visualizzatori

In generale, dovresti IPv6 abilitarla se hai utenti sulle IPv6 reti che desiderano accedere ai tuoi contenuti. Tuttavia, se utilizzi cookie firmati URLs o firmati per limitare l'accesso ai tuoi contenuti e se utilizzi una politica personalizzata che include il `IpAddress` parametro per limitare gli indirizzi IP che possono accedere ai tuoi contenuti, non abilitarli IPv6. Se intendi limitare l'accesso a una parte del tuo contenuto in base all'indirizzo IP e non limitare l'accesso ad altro contenuto (o limitare

l'accesso ma non in base all'indirizzo IP), puoi creare due distribuzioni. Per informazioni sulla creazione di documenti URLs firmati utilizzando una politica personalizzata, consultaCreazione di un URL firmato utilizzando una policy personalizzata. Per informazioni sulla creazione di cookie firmati utilizzando una policy personalizzata, consulta Impostazione di cookie firmati che utilizzano una policy personalizzata.

Se utilizzi un record di risorse alias Route 53 impostato per indirizzare il traffico verso la tua CloudFront distribuzione, devi creare un secondo set di record di risorse alias quando entrambe le seguenti condizioni sono vere:

- Ti abiliti IPv6 per la distribuzione
- Stai usando nomi di dominio alternativi URLs per i tuoi oggetti

Per ulteriori informazioni, consulta Routing del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio nella Amazon Route 53 Developer Guide.

Se hai creato un set di record di risorsa CNAME, con Route 53; o con un altro servizio DNS, non è necessaria alcuna modifica. Un record CNAME instrada il traffico alla distribuzione indipendentemente dal formato dell'indirizzo IP della richiesta visualizzatore.

Se abiliti IPv6 e CloudFront accedi ai log, la `c-ip` colonna include i valori IPv4 e IPv6 il formato. Per ulteriori informazioni, consulta Campi di file di log.

> **Note**
>
> Per mantenere un'elevata disponibilità dei clienti, CloudFront risponde alle richieste degli utenti utilizzando IPv4 se i nostri dati suggeriscono che ciò IPv4 fornirà un'esperienza utente migliore. Per scoprire la percentuale di richieste CloudFront in corso IPv6, abilita la CloudFront registrazione per la tua distribuzione e analizza la `c-ip` colonna, che contiene l'indirizzo IP del visualizzatore che ha effettuato la richiesta. Questa percentuale dovrebbe aumentare nel tempo, ma rimarrà una minoranza del traffico in quanto non IPv6 è ancora supportata da tutte le reti di spettatori a livello globale. Alcune reti di spettatori offrono un IPv6 supporto eccellente, mentre altre non lo supportano IPv6 affatto. (una rete di visualizzatori è analoga all'operatore Internet o wireless).
> Per ulteriori informazioni sulla nostra assistenza per IPv6, consulta le CloudFront domande frequenti. Per informazioni sull'abilitazione di log di accesso, vedi i campi Registrazione di log standard e Log Prefix (Prefisso log).

IPv6 richieste di origine

Quando utilizzi un'origine personalizzata (escluse le origini Amazon S3 e VPC), puoi personalizzare le impostazioni di origine per la tua distribuzione per scegliere come CloudFront connettersi alla tua origine utilizzando o gli indirizzi. IPv4 IPv6 Per le origini personalizzate (escluse le origini Amazon S3 e VPC), sono disponibili le seguenti opzioni di connettività:

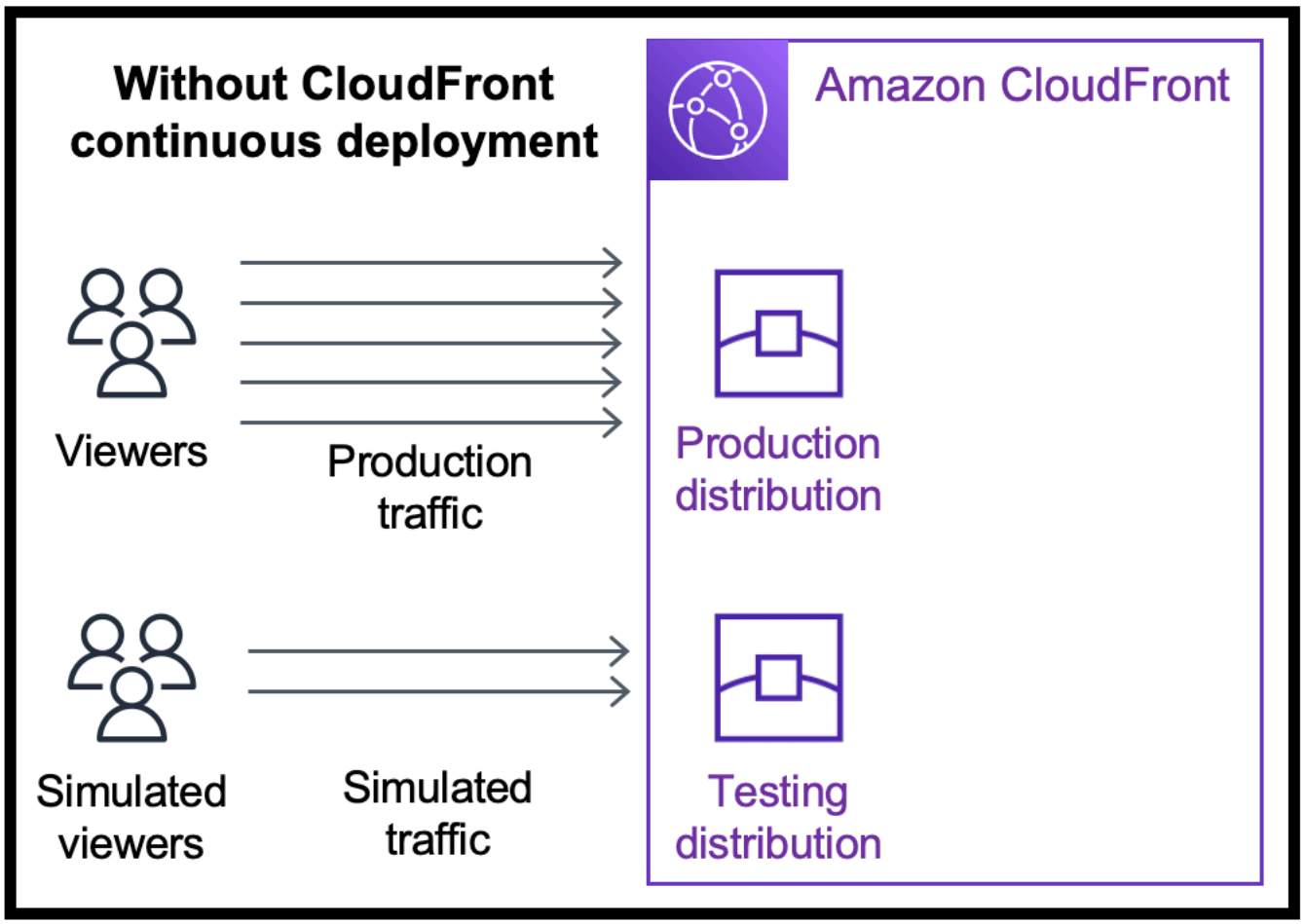
- IPv4 solo (impostazione predefinita): questa è la configurazione predefinita CloudFront utilizzata per connettersi alle origini. IPv4
- IPv6 solo: richiede che il dominio di origine si risolva in un IPv6 indirizzo. CloudFront utilizzerà esclusivamente IPv6 indirizzi per le connessioni di origine.
- Dual-stack: abilita le connessioni su e. IPv4 IPv6 CloudFront sceglie IPv4 automaticamente la nostra connettività di IPv6 origine per dare priorità a prestazioni e disponibilità in modo da poterla utilizzare CloudFront come gateway Internet IPv4 dual-stack per IPv6 le applicazioni Web.

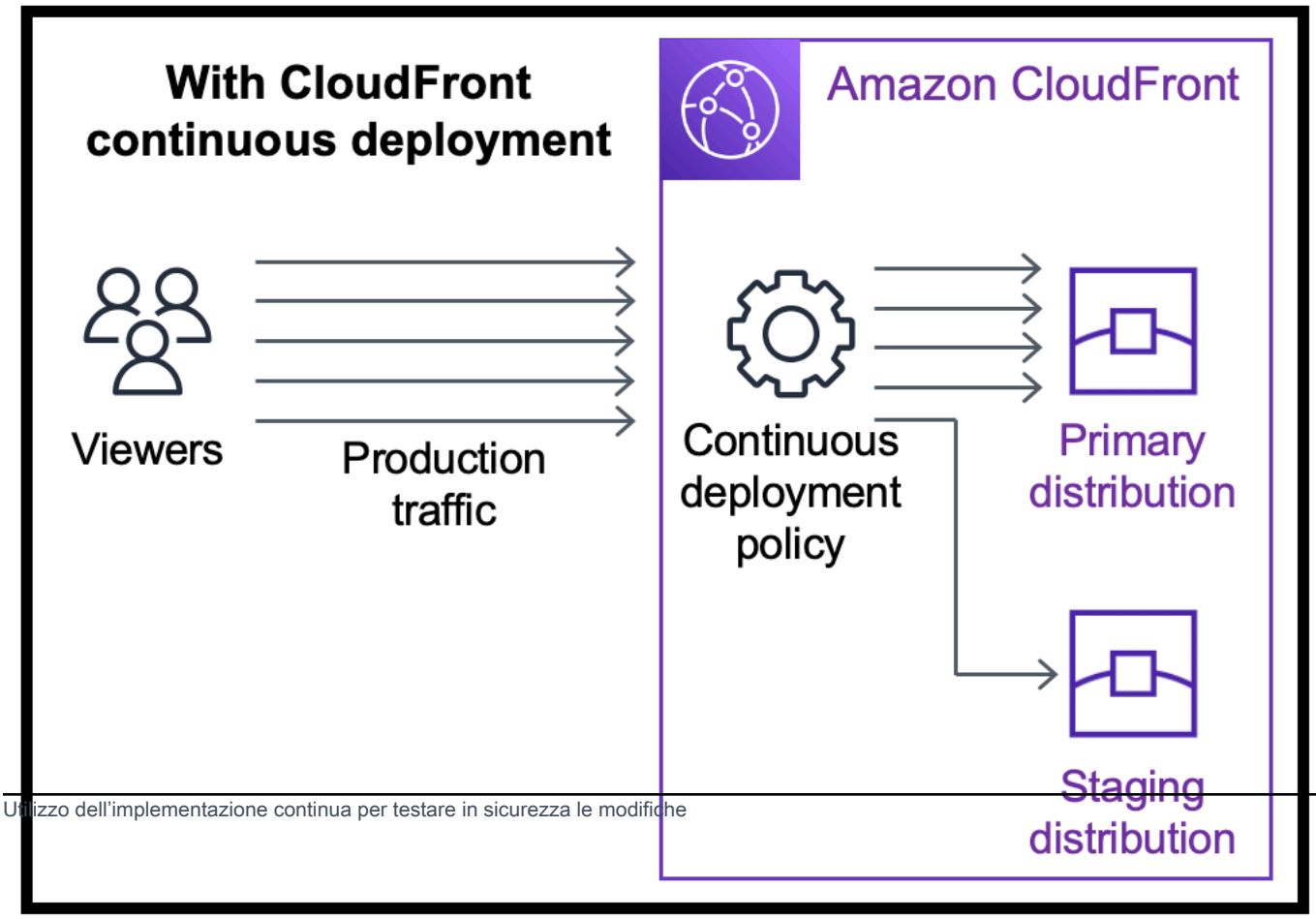
Scegli l'opzione che corrisponde alla configurazione di rete e ai requisiti di connettività dell'origine. Per ulteriori informazioni, consulta Progettazione del DNS e considerazioni sulla sicurezza e il monitoraggio. IPv6 IPv6

Utilizza la distribuzione CloudFront continua per testare in sicurezza le modifiche alla configurazione CDN

Con la distribuzione CloudFront continua di Amazon puoi implementare in sicurezza le modifiche alla tua configurazione CDN testandola prima con un sottoinsieme di traffico di produzione. È possibile utilizzare una distribuzione temporanea e una policy di implementazione continua per inviare parte del traffico da visualizzatori reali (di produzione) alla nuova configurazione CDN e convalidare che funzioni come previsto. È possibile monitorare le prestazioni della nuova configurazione in tempo reale e promuovere la nuova configurazione per servire tutto il traffico tramite la distribuzione principale, una volta pronti.

Il diagramma seguente mostra i vantaggi dell'utilizzo della distribuzione continua. CloudFront Senza di essa, è necessario testare le modifiche alla configurazione CDN con traffico simulato. Con l'implementazione continua è possibile testare le modifiche con un sottoinsieme del traffico di produzione, quindi promuovere le modifiche alla distribuzione principale quando si è pronti.


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

Per ulteriori informazioni sull'utilizzo dell'implementazione continua, consulta gli argomenti seguenti.

Argomenti

CloudFront flusso di lavoro di distribuzione continuo

Il seguente flusso di lavoro di alto livello spiega come testare e implementare in sicurezza le modifiche alla configurazione con CloudFront una distribuzione continua.

1. Scegliere la distribuzione che si desidera utilizzare come distribuzione principale. La distribuzione principale è quella che attualmente serve il traffico di produzione.
2. Dalla distribuzione principale, creare una distribuzione temporanea. Una distribuzione temporanea inizia come una copia della distribuzione principale.
3. Creare una configurazione del traffico all'interno di una policy di implementazione continua e collegarla alla distribuzione principale. Ciò determina il modo in cui CloudFront indirizza il traffico verso la distribuzione temporanea. Per ulteriori informazioni sull'instradamento delle richieste verso una distribuzione temporanea, consulta the section called "Instradamento delle richieste alla distribuzione temporanea".
4. Aggiornare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called "Aggiornamento delle distribuzioni principale e temporanea".
5. Monitorare la distribuzione temporanea per determinare se le modifiche alla configurazione funzionano come previsto. Per ulteriori informazioni sul monitoraggio di una distribuzione temporanea, consulta the section called "Monitoraggio di una distribuzione temporanea".

   Mentre si monitora la distribuzione temporanea è possibile:

   - Aggiornare nuovamente la configurazione della distribuzione temporanea per continuare a testare le modifiche alla configurazione.
   - Aggiornare la policy di implementazione continua (configurazione del traffico) per inviare più o meno traffico alla distribuzione temporanea.

6. Una volta soddisfatti delle prestazioni della distribuzione temporanea, promuovere la configurazione della distribuzione temporanea alla distribuzione principale, che copia la configurazione della distribuzione temporanea nella distribuzione principale. Ciò disabilita anche la politica di distribuzione continua, che significa che CloudFront indirizza tutto il traffico verso la distribuzione primaria.

È possibile creare un'automazione che monitora le prestazioni della distribuzione temporanea (fase 5) e promuova automaticamente la configurazione (fase 6) quando vengono soddisfatti determinati criteri.

Dopo aver promosso una configurazione, è possibile riutilizzare la stessa distribuzione temporanea la prossima volta che si desidera testare una modifica alla configurazione.

Per ulteriori informazioni sull'utilizzo delle distribuzioni temporanee e delle politiche di distribuzione continua nella CloudFront console, nell'API o nell' CloudFront API AWS CLI, consulta la sezione seguente.

Utilizzo di una distribuzione temporanea e di una policy di implementazione continua

È possibile creare, aggiornare e modificare le distribuzioni temporanee e le politiche di distribuzione continua nella CloudFront console, con AWS Command Line Interface (AWS CLI) o con l' CloudFront API.

Creazione di una distribuzione temporanea con una policy di implementazione continua

Nelle procedure seguenti viene illustrato come creare una distribuzione temporanea con una policy di implementazione continua.

Console

Puoi creare una distribuzione temporanea con una policy di implementazione continua utilizzando la Console di gestione AWS.

Creazione di una distribuzione temporanea e di una policy di implementazione continua (console)

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home

2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegliere la distribuzione che si desidera utilizzare come distribuzione principale. La distribuzione principale è quella che attualmente serve il traffico di produzione, quella da cui verrà creata la distribuzione temporanea.
4. Nella sezione Continuous deployment (Implementazione continua), scegliere Create staging distribution (Crea distribuzione temporanea). Si apre la procedura guidata Create staging distribution (Crea distribuzione temporanea).
5. Nella procedura guidata Create staging distribution (Crea distribuzione temporanea), effettuare le seguenti operazioni:

   a. (Facoltativo) Digitare una descrizione per la distribuzione temporanea.

   b. Scegli Next (Successivo).

   c. Modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiornamento delle distribuzioni principale e temporanea”.

      Una volta terminato di modificare la configurazione della distribuzione temporanea, scegliere Next (Avanti).

   d. Utilizzare la console per specificare Traffic configuration (Configurazione del traffico). Ciò determina il modo in cui CloudFront indirizza il traffico verso la distribuzione temporanea. (CloudFront memorizza la configurazione del traffico in una politica di distribuzione continua.)

      Per ulteriori informazioni sulle opzioni in Traffic configuration (Configurazione del traffico) consulta the section called “Instradamento delle richieste alla distribuzione temporanea”.

      Una volta terminato con Traffic configuration (Configurazione del traffico), scegliere Next (Avanti).

   e. Esaminare la configurazione per la distribuzione temporanea, inclusa la configurazione del traffico, quindi scegliere Create staging distribution (Crea distribuzione temporanea).

Al termine della procedura guidata di creazione della distribuzione temporanea nella CloudFront console, CloudFront effettua le seguenti operazioni:

- Crea una distribuzione temporanea con le impostazioni specificate (nella fase 5c)

- Crea una policy di implementazione continua con la configurazione del traffico specificata (nella fase 5d)
- Collega la policy di implementazione continua alla distribuzione principale da cui è stata creata la distribuzione temporanea

Quando la configurazione della distribuzione primaria, con la politica di distribuzione continua allegata, viene distribuita su postazioni periferiche, CloudFront inizia a inviare la parte di traffico specificata alla distribuzione temporanea in base alla configurazione del traffico.

CLI

Per creare una politica di distribuzione temporanea e una politica di distribuzione continua con AWS CLI, utilizza le seguenti procedure.

Creazione di una distribuzione temporanea (CLI)

1. Utilizzare i comandi aws cloudfront get-distribution e grep insieme per ottenere il valore `ETag` della distribuzione che si desidera utilizzare come distribuzione principale. La distribuzione principale è quella che attualmente serve il traffico di produzione, da cui verrà creata la distribuzione temporanea.

   Il comando seguente mostra un esempio. Nell'esempio seguente, sostituiscilo *`primary_distribution_ID`* con l'ID della distribuzione principale.

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

   Copiare il valore `ETag` (servirà nella fase successiva).
2. Utilizzare il comando aws cloudfront copy-distribution per creare una distribuzione temporanea. Il seguente comando di esempio utilizza caratteri di escape (\) e interruzioni di riga per la leggibilità, ma è necessario ometterli dal comando. Nel seguente è un comando di esempio:

   - Sostituisci *`primary_distribution_ID`* con l'ID della distribuzione principale.
   - Sostituisci *`primary_distribution_ETag`* con il `ETag` valore della distribuzione primaria (che hai ottenuto nel passaggio precedente).
   - (Facoltativo) *`CLI_example`* Sostituiscilo con l'ID di riferimento del chiamante desiderato.

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

L'output del comando mostra informazioni sulla distribuzione temporanea e sulla sua configurazione. Copia il nome di CloudFront dominio della distribuzione temporanea perché ti serve per il passaggio successivo.

Creazione di una policy di implementazione continua (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `continuous-deployment-policy.yaml` che contiene tutti i parametri di input per il comando create-continuous-deployment-policy. Il seguente comando utilizza caratteri di escape (\) e interruzioni di riga per la leggibilità, ma è necessario ometterli dal comando.

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

2. Aprire il file `continuous-deployment-policy.yaml` appena creato. Modificare il file per specificare le impostazioni delle policy di implementazione continua desiderate, quindi salvare il file. Quando si modifica il file:

   - Nella sezione `StagingDistributionDnsNames`:
     - Modificare il valore di `Quantity` in `1`.
     - Per`Items`, incolla il nome di CloudFront dominio della distribuzione temporanea (che hai salvato in un passaggio precedente).
   - Nella sezione `TrafficConfig`:
     - Scegliere un `Type`, `SingleWeight` o `SingleHeader`.

- Rimuovere le impostazioni per l'altro tipo. Ad esempio, se si desidera una configurazione del traffico basata sul peso, impostare `Type` su `SingleWeight` e rimuovere le impostazioni `SingleHeaderConfig`.
- Per utilizzare una configurazione del traffico basata sul peso, impostare il valore di `Weight` su un numero decimale compreso tra `.01` (uno percento) e `.15` (quindici percento).

Per ulteriori informazioni su queste opzioni in `TrafficConfig`, consulta the section called “Instradamento delle richieste alla distribuzione temporanea” e the section called “Persistenza della sessione per configurazioni basate sul peso”.

3. Utilizzare il comando seguente per creare la policy dell'implementazione continua utilizzando i parametri di input dal file `continuous-deployment-policy.yaml`.

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

Copiare il valore `Id` nell'output del comando. Questo è l'ID della policy di implementazione continua e serve nella fase successiva.

Collegamento di una policy di implementazione continua a una distribuzione principale (CLI con file di input)

1. Utilizzare il comando seguente per salvare la configurazione della distribuzione principale in un file denominato `primary-distribution.yaml`. Sostituiscilo *`primary_distribution_ID`* con l'ID della distribuzione principale.

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

2. Aprire il file `primary-distribution.yaml` appena creato. Modifica il file apportando le seguenti modifiche:
   - Incollare l'ID della policy di implementazione continua (copiata in una fase precedente) nel campo `ContinuousDeploymentPolicyId`.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione principale e utilizzare la policy di implementazione continua. Sostituisci *primary_distribution_ID* con l'ID della distribuzione principale.

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

Quando la configurazione della distribuzione primaria, con la politica di distribuzione continua allegata, viene implementata su postazioni periferiche, CloudFront inizia a inviare la porzione di traffico specificata alla distribuzione temporanea in base alla configurazione del traffico.

API

Per creare una politica di distribuzione temporanea e di distribuzione continua con l' CloudFront API, utilizza le seguenti operazioni API:

- CopyDistribution
- CreateContinuousDeploymentPolicy

Per ulteriori informazioni sui campi specificati in queste chiamate API, consulta quanto segue:

- the section called “Instradamento delle richieste alla distribuzione temporanea”
- the section called “Persistenza della sessione per configurazioni basate sul peso”
- La documentazione di riferimento sull'API per il tuo AWS SDK o altro client API

Dopo aver creato una distribuzione temporanea e una politica di distribuzione continua, utilizza UpdateDistribution(sulla distribuzione principale) per allegare la politica di distribuzione continua alla distribuzione primaria.

Aggiornamento di una distribuzione temporanea

Nelle procedure seguenti viene illustrato come aggiornare una distribuzione temporanea con una policy di implementazione continua.

Console

Puoi aggiornare determinate configurazioni per le distribuzioni primaria e temporanea. Per ulteriori informazioni, consulta Aggiornamento delle distribuzioni principale e temporanea.

Aggiornamento di una distribuzione temporanea (console)

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegliere la distribuzione principale. Questa è la distribuzione che attualmente serve il traffico di produzione, quella da cui verrà creata la distribuzione temporanea.
4. Scegliere View staging distribution (Visualizza distribuzione temporanea).
5. Utilizzare la console per modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiornamento delle distribuzioni principale e temporanea”.

Non appena la configurazione della distribuzione temporanea viene implementata nelle posizioni edge, ha effetto sul traffico in entrata indirizzato verso la distribuzione temporanea.

CLI

Aggiornamento di una distribuzione temporanea (CLI con file di input)

1. Utilizzare il comando seguente per salvare la configurazione della distribuzione temporanea in un file denominato `staging-distribution.yaml`. Sostituisci *`staging_distribution_ID`* con l'ID della distribuzione temporanea.

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

2. Aprire il file `staging-distribution.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

   - Modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiornamento delle distribuzioni principale e temporanea”.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

Salvare il file al termine.

3. Utilizzare il seguente comando per aggiornare la configurazione della distribuzione temporanea. Sostituisci *staging_distribution_ID* con l'ID della distribuzione temporanea.

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

Non appena la configurazione della distribuzione temporanea viene implementata nelle posizioni edge, ha effetto sul traffico in entrata indirizzato verso la distribuzione temporanea.

API

Per aggiornare la configurazione di una distribuzione temporanea, utilizza UpdateDistribution(sulla distribuzione temporanea) per modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called "Aggiornamento delle distribuzioni principale e temporanea".

Aggiornamento di una policy di implementazione continua

Nelle procedure seguenti viene illustrato come aggiornare una policy di implementazione continua.

Console

Puoi aggiornare la configurazione del traffico della distribuzione aggiornando la policy di implementazione continua.

Aggiornamento di una policy di implementazione continua (console)

1. Apri la console all' CloudFront indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegliere la distribuzione principale. Questa è la distribuzione che attualmente serve il traffico di produzione, quella da cui verrà creata la distribuzione temporanea.
4. Nella sezione Continuous deployment (Implementazione continua), scegliere Edit policy (Modifica policy).

5. Modifica della configurazione del traffico in una policy di implementazione continua. Al termine, scegliere Save changes (Salva le modifiche).

Quando la configurazione della distribuzione primaria con la politica di distribuzione continua aggiornata viene distribuita nelle edge location, CloudFront inizia a inviare traffico alla distribuzione temporanea in base alla configurazione del traffico aggiornata.

CLI

Aggiornamento di una policy di implementazione continua (CLI con file di input)

1. Utilizzare il seguente comando per salvare la configurazione della policy di implementazione continua in un file denominato `continuous-deployment-policy.yaml`. Sostituisci *`continuous_deployment_policy_ID`* con l'ID della politica di distribuzione continua. Il seguente comando utilizza caratteri di escape (\) e interruzioni di riga per la leggibilità, ma è necessario ometterli dal comando.

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

2. Aprire il file `continuous-deployment-policy.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

   - Modificare la configurazione del traffico della policy di implementazione continua come desiderato. Ad esempio, è possibile passare dall'utilizzo di una configurazione di traffico basata sull'intestazione a una basata sul peso oppure puoi modificare la percentuale di traffico (peso) per una configurazione basata sul peso. Per ulteriori informazioni, consultare the section called “Instradamento delle richieste alla distribuzione temporanea” e the section called “Persistenza della sessione per configurazioni basate sul peso”.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare policy di implementazione continua. Sostituisci *`continuous_deployment_policy_ID`* con l'ID della politica di distribuzione continua. Il

seguente comando utilizza caratteri di escape (\) e interruzioni di riga per la leggibilità, ma è necessario ometterli dal comando.

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

Quando la configurazione della distribuzione primaria con la politica di distribuzione continua aggiornata viene distribuita su postazioni periferiche, CloudFront inizia a inviare il traffico alla distribuzione temporanea in base alla configurazione del traffico aggiornata.

API

Per aggiornare una politica di distribuzione continua, usa. UpdateContinuousDeploymentPolicy

Promozione di una configurazione di distribuzione temporanea

Nelle procedure seguenti viene illustrato come promuovere una configurazione di distribuzione temporanea.

Console

Quando promuovi una distribuzione temporanea, CloudFront copia la configurazione dalla distribuzione temporanea alla distribuzione principale. CloudFront disabilita inoltre la politica di distribuzione continua e indirizza tutto il traffico verso la distribuzione primaria.

Dopo aver promosso una configurazione, è possibile riutilizzare la stessa distribuzione temporanea la prossima volta che si desidera testare una modifica alla configurazione.

Promozione della configurazione di una distribuzione temporanea (console)

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegliere la distribuzione principale. Questa è la distribuzione che attualmente serve il traffico di produzione, quella da cui verrà creata la distribuzione temporanea.
4. Nella sezione Continuous deployment (Implementazione continua), scegliere Promote (Promuovi).

5. Digitare **`confirm`** e scegliere Promote (Promuovi).

CLI

Quando promuovi una distribuzione temporanea, CloudFront copia la configurazione dalla distribuzione temporanea alla distribuzione principale. CloudFront disabilita inoltre la politica di distribuzione continua e indirizza tutto il traffico verso la distribuzione primaria.

Dopo aver promosso una configurazione, è possibile riutilizzare la stessa distribuzione temporanea la prossima volta che si desidera testare una modifica alla configurazione.

Promozione di una configurazione di una distribuzione temporanea (CLI)

- Utilizzare il comando aws cloudfront update-distribution-with-staging-config per promuovere la configurazione della distribuzione temporanea alla distribuzione principale. Il seguente comando di esempio utilizza caratteri di escape (\) e interruzioni di riga per la leggibilità, ma è necessario ometterli dal comando. Nel seguente è un comando di esempio:
  - Sostituisci *`primary_distribution_ID`* con l'ID della distribuzione principale.
  - Sostituisci *`staging_distribution_ID`* con l'ID della distribuzione temporanea.
  - Sostituisci *`primary_distribution_ETag`* e *`staging_distribution_ETag`* con i `ETag` valori della distribuzione primaria e della distribuzione temporanea. Assicurarsi che il valore della distribuzione principale sia il primo, come mostrato nell'esempio.

```
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

Per promuovere la configurazione di una distribuzione temporanea alla distribuzione primaria, usa. UpdateDistributionWithStagingConfig

Monitoraggio di una distribuzione temporanea

Per monitorare le prestazioni di una distribuzione temporanea, puoi utilizzare le stesse metriche, log e report disponibili per tutte le CloudFront distribuzioni. Esempio:

- Puoi visualizzare le metriche di CloudFront distribuzione predefinite (come le richieste totali e il tasso di errore) nella CloudFront console e attivare metriche aggiuntive (come la frequenza di accesso alla cache e il tasso di errore per codice di stato) a un costo aggiuntivo. È anche possibile creare degli allarmi in base a tali metriche.
- È possibile visualizzare i log standard e i log di accesso in tempo reale per ottenere informazioni dettagliate sulle richieste ricevute dalla distribuzione temporanea. I log standard contengono i due campi seguenti che consentono di identificare la distribuzione principale a cui è stata originariamente inviata la richiesta prima di CloudFront indirizzarla alla distribuzione temporanea: e. `primary-distribution-id` `primary-distribution-dns-name`
- È possibile visualizzare e scaricare report nella CloudFront console, ad esempio il rapporto sulle statistiche della cache.

Ulteriori informazioni sul funzionamento dell'implementazione continua

I seguenti argomenti spiegano come funziona la distribuzione CloudFront continua.

Argomenti

- Instradamento delle richieste alla distribuzione temporanea
- Persistenza della sessione per configurazioni basate sul peso
- Aggiornamento delle distribuzioni principale e temporanea
- Le distribuzioni principali e temporanee non condividono una cache

Instradamento delle richieste alla distribuzione temporanea

Quando si utilizza la distribuzione CloudFront continua, non è necessario modificare nulla delle richieste dei visualizzatori. I visualizzatori non possono inviare richieste direttamente a una distribuzione temporanea utilizzando un nome DNS, un indirizzo IP o un CNAME. Invece, gli spettatori inviano le richieste alla distribuzione primaria (di produzione) e CloudFront indirizzano alcune di queste richieste alla distribuzione temporanea in base alle impostazioni di configurazione del traffico contenute nella politica di distribuzione continua. Esistono due tipi di configurazioni del traffico:

Basata sul peso

Una configurazione basata sul peso indirizza la percentuale specificata di richieste dei visualizzatori alla distribuzione temporanea. Quando utilizzi una configurazione basata sul peso, puoi anche abilitare la persistenza della sessione, il che aiuta a garantire che le richieste dello stesso visualizzatore vengano CloudFront trattate come parte di una singola sessione. Per ulteriori informazioni, consulta the section called “Persistenza della sessione per configurazioni basate sul peso”.

Basata sull'intestazione

Una configurazione basata sull'intestazione indirizza le richieste alla distribuzione temporanea quando la richiesta del visualizzatore contiene un'intestazione HTTP specifica (si specificano l'intestazione e il valore). Le richieste che non contengono l'intestazione e il valore specificati vengono indirizzate alla distribuzione principale. Questa configurazione è utile per i test locali o quando si ha il controllo sulle richieste dei visualizzatori.

> **Note**
>
> Le intestazioni indirizzate alla distribuzione temporanea devono contenere il prefisso `aws-cf-cd-`.

Persistenza della sessione per configurazioni basate sul peso

Quando utilizzi una configurazione basata sul peso per indirizzare il traffico verso una distribuzione temporanea, puoi anche abilitare la persistenza della sessione, che aiuta a far sì che le richieste dello stesso visualizzatore vengano CloudFront trattate come un'unica sessione. Quando abiliti la persistenza della sessione, CloudFront imposta un cookie in modo che tutte le richieste dello stesso visualizzatore in una singola sessione vengano servite da un'unica distribuzione, principale o temporanea.

Quando si abilita la persistenza della sessione, è anche possibile specificare la durata dell'inattività. Se il visualizzatore è inattivo (non invia richieste) per questo periodo di tempo, la sessione scade e CloudFront considera le richieste future di questo visualizzatore come una nuova sessione. La durata dell'inattività viene specificata in un numero di secondi, da 300 (cinque minuti) a 3.600 (un'ora).

Nei seguenti casi, CloudFront reimposta tutte le sessioni (anche quelle attive) e considera tutte le richieste come una nuova sessione:

- Si disabilita o si abilita la policy di implementazione continua
- Si disabilita o si abilita l'impostazione della persistenza della sessione

Aggiornamento delle distribuzioni principale e temporanea

Quando a una distribuzione principale è associata una policy di implementazione continua, sono disponibili le seguenti modifiche alla configurazione sia per la distribuzione principale che per quella temporanea:

- Tutte le impostazioni del comportamento della cache, incluso il comportamento predefinito della cache
- Tutte le impostazioni di origine (origini e gruppi di origine)
- Risposte agli errori personalizzate (pagine di errore)
- Restrizioni geografiche
- Default Root Object (Oggetto root di default)
- Impostazioni di registrazione
- Descrizione (commento)

Puoi anche aggiornare le risorse esterne a cui si fa riferimento nella configurazione di una distribuzione, come una politica di cache, una politica di intestazioni di risposta, una funzione o una funzione CloudFront Lambda @Edge.

Le distribuzioni principali e temporanee non condividono una cache

Le distribuzioni principali e temporanee non condividono una cache. Quando CloudFront invia la prima richiesta a una distribuzione temporanea, la relativa cache è vuota. Quando le richieste arrivano alla distribuzione temporanea, inizia a memorizzare le risposte nella cache (se configurata per effettuare questa operazione).

Quote e altre considerazioni per l'implementazione continua

CloudFront la distribuzione continua è soggetta alle seguenti quote e ad altre considerazioni.

Quote

- Numero massimo di distribuzioni di staging per: 20 Account AWS
- Numero massimo di politiche di distribuzione continua per Account AWS: 20

- Percentuale massima di traffico che è possibile inviare a una distribuzione temporanea in una configurazione basata sul peso: 15%
- Valori minimi e massimi per la durata di inattività della persistenza della sessione: 300 - 3.600 secondi

Per ulteriori informazioni, consulta Quote.

> **Note**
>
> Quando si utilizza l'implementazione continua e la distribuzione primaria è impostata con OAC per l'accesso al bucket S3, aggiorna la policy di bucket S3 per consentire l'accesso alla distribuzione temporanea. Per le policy di bucket S3 di esempio, consulta the section called "Concedi l' CloudFront autorizzazione per accedere al bucket S3".

AWS WAF web ACLs

Se abiliti l'implementazione continua per la distribuzione, per AWS WAF si applicano le seguenti considerazioni:

- Non è possibile associare una lista di controllo degli accessi AWS WAF Web (ACL) alla distribuzione se è la prima volta che l'ACL viene associata alla distribuzione.
- Non è possibile dissociare un ACL AWS WAF Web dalla distribuzione.

Prima di poter eseguire le operazioni precedenti, è necessario eliminare la policy di implementazione continua per la distribuzione di produzione. Ciò elimina anche la distribuzione temporanea. Per ulteriori informazioni, consulta Utilizzo di protezioni AWS WAF.

Casi in cui CloudFront invia tutte le richieste alla distribuzione primaria

In alcuni casi, ad esempio nei periodi di elevato utilizzo delle risorse, è CloudFront possibile inviare tutte le richieste alla distribuzione primaria indipendentemente da quanto specificato nella politica di distribuzione continua.

CloudFront invia tutte le richieste alla distribuzione principale durante le ore di traffico di punta, indipendentemente da quanto specificato nella politica di distribuzione continua. Il traffico di picco si riferisce al traffico sul CloudFront servizio e non al traffico sulla tua distribuzione.

HTTP/3

Non è possibile utilizzare l'implementazione continua con una distribuzione che supporta HTTP/3.

Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs

Quando crei una distribuzione, CloudFront fornisce un nome di dominio per essa, ad esempio d111111abcdef8.cloudfront.net. Invece di utilizzare questo nome di dominio fornito, puoi utilizzare un nome di dominio alternativo (noto anche come CNAME).

Per ulteriori informazioni su come utilizzare il nome di dominio, ad esempio www.example.com, consulta i seguenti contenuti:

Argomenti

Requisiti per l'utilizzo di nomi di dominio alternativi

Quando aggiungi un nome di dominio alternativo, ad esempio www.example.com, a una distribuzione, i requisiti sono i seguenti: CloudFront

I nomi di dominio alternativi devono essere in lettere minuscole

Tutti i nomi di dominio alternativi () CNAMEs devono essere in minuscolo.

I nomi di dominio alternativi devono essere coperti da un certificato TLS valido

Per aggiungere un nome di dominio alternativo (CNAME) a una CloudFront distribuzione, è necessario allegare alla distribuzione un certificato TLS affidabile e valido che copra il nome di dominio alternativo. Ciò garantisce che solo le persone con accesso al certificato del tuo dominio possano associarsi a CloudFront un CNAME correlato al tuo dominio.

Un certificato affidabile è rilasciato da AWS Certificate Manager (ACM) o da un'altra autorità di certificazione (CA) valida. È possibile utilizzare un certificato autofirmato per convalidare un CNAME esistente, ma non per un nuovo CNAME. CloudFront supporta le stesse autorità di certificazione di Mozilla. Per l'elenco corrente, consulta l'elenco dei certificati CA inclusi in Mozilla. Per informazioni sui certificati intermedi quando si utilizza una CA di terze parti, consulta Certificati intermedi.

Per verificare un nome di dominio alternativo utilizzando il certificato allegato, inclusi nomi di dominio alternativi che includono caratteri jolly, CloudFront verifica il nome alternativo del soggetto (SAN) sul certificato. Il nome di dominio alternativo che stai aggiungendo deve essere coperto dal SAN.

> **Note**
>
> È possibile allegare un solo certificato alla volta a una CloudFront distribuzione.

Puoi verificare di essere autorizzato ad aggiungere un nome di dominio alternativo specifico alla distribuzione in uno dei seguenti modi:

- Collegamento di un certificato che include il nome di dominio alternativo, ad esempio product-name.example.com.
- Collegando un certificato che include un carattere jolly * all'inizio di un nome di dominio, per coprire più sottodomini con un solo certificato. Quando specifichi un carattere jolly, puoi aggiungere più sottodomini come nomi di dominio alternativi in CloudFront.

I seguenti esempi illustrano come l'uso di caratteri jolly in nomi di dominio in un certificato consente di autorizzare l'aggiunta di nomi di dominio alternativi specifici in CloudFront.

- Si desidera aggiungere marketing.example.com come un nome di dominio alternativo. Nel certificato elenca il seguente nome di dominio: *.example.com. Quando alleghi questo certificato a CloudFront, puoi aggiungere qualsiasi nome di dominio alternativo per la tua distribuzione che sostituisca il carattere jolly a quel livello, incluso marketing.example.com. Puoi anche, ad esempio, aggiungere i seguenti nomi di dominio alternativi:
  - product.example.com
  - api.example.com

Tuttavia, non puoi aggiungere nomi di dominio alternativi che sono a livelli più alti o più bassi del carattere jolly. Ad esempio, non è possibile aggiungere i nomi di dominio alternativi example.com o marketing.product.example.com.

- Si desidera aggiungere example.com come un nome di dominio alternativo. A questo scopo, devi elencare il nome di dominio example.com stesso nel certificato che colleghi alla distribuzione.
- Si desidera aggiungere marketing.product.example.com come un nome di dominio alternativo. A questo scopo, puoi elencare *.product.example.com nel certificato o elencare stesso marketing.product.example.com o elencare stesso nel certificato.

Autorizzazione per la modifica della configurazione DNS

Quando aggiungi nomi di dominio alternativi, devi creare record CNAME per indirizzare le query DNS per i nomi di dominio alternativi alla tua distribuzione. CloudFront A questo scopo, devi disporre dell'autorizzazione per creare record CNAME con il provider di servizi DNS per i nomi di dominio alternativi che stai utilizzando. Normalmente questo significa che sei il proprietario dei domini, ma potresti anche sviluppare un'applicazione per il proprietario del dominio.

Nomi di dominio alternativi e HTTPS

Se desideri che i visualizzatori utilizzino HTTPS con il nome di dominio alternativo, devi completare alcune configurazioni aggiuntive. Per ulteriori informazioni, consulta Utilizzo di nomi di dominio alternativi e HTTPS.

Restrizioni sull'utilizzo dei nomi di dominio alternativi

È importante prendere nota delle seguenti imitazioni sull'utilizzo dei nomi di dominio alternativi:

Numero massimo di nomi di dominio alternativi

Per il numero massimo corrente di nomi di dominio alternativi che puoi aggiungere a una distribuzione o per richiedere una quota più elevata (precedentemente nota come limite), consulta Quote generali sulle distribuzioni.

Duplicazione e sovrapposizione dei nomi di dominio alternativi

Non puoi aggiungere un nome di dominio alternativo a una CloudFront distribuzione se lo stesso nome di dominio alternativo esiste già in un'altra CloudFront distribuzione, anche se l'altra distribuzione è di tua proprietà. Account AWS

Tuttavia, puoi aggiungere un nome di dominio alternativo con carattere jolly, ad esempio *.example.com, che includa (in sovrapposizione) un nome di dominio alternativo senza carattere jolly, ad esempio www.example.com. Se hai nomi di dominio alternativi sovrapposti in due distribuzioni, CloudFront invia la richiesta alla distribuzione con il nome più specifico, indipendentemente dalla distribuzione a cui punta il record DNS. Ad esempio, marketing.domain.com è più specifico di *.domain.com.

Se disponi di una voce DNS wildcard esistente che punta a una CloudFront distribuzione e ricevi un errore DNS configurato in modo errato quando tenti di aggiungere un nuovo CNAME con un nome più specifico, vedi. CloudFront restituisce un errore di record DNS configurato in modo errato quando tento di aggiungere un nuovo CNAME

Domain Fronting

CloudFront è protetto contro il fronting dei domini che si verificano tra diversi. Account AWS Si tratta di uno scenario in cui un client non standard crea una connessione TLS/SSL a un nome di dominio in un nome di dominio e quindi effettua una Account AWS richiesta HTTPS per un nome di dominio non correlato in un altro. Account AWS

Ad esempio, la connessione TLS potrebbe connettersi a www.example.com e quindi effettuare una richiesta per www.example.org.

Per determinare se una richiesta è indirizzata al dominio, esegue i seguenti controlli: CloudFront

- L'estensione SNI è uguale all'intestazione `Host` della richiesta HTTP
- Il certificato appartiene alla Account AWS stessa distribuzione della richiesta
- La richiesta HTTP `Host` è coperta dal certificato fornito durante l'handshake TLS

Se nessuna di queste condizioni è soddisfatta, CloudFront determina che la richiesta è il domain fronting. CloudFront rifiuterà la richiesta con una risposta di errore HTTP 421.

> **Note**
>
> Se il client non fornisce l'estensione SNI e ottiene invece un certificato *.cloudfront.net predefinito, accetterà le richieste in arrivo. CloudFront

Come identifica la distribuzione per una richiesta CloudFront

CloudFront identifica una distribuzione per una richiesta HTTP in base all'`Host`intestazione. CloudFront non dipende dall'indirizzo CloudFront IP a cui ti stai connettendo o dall'handshake SNI fornito durante l'handshake TLS.

Quando CloudFront riceve una richiesta, utilizzerà il valore dell'`Host`intestazione per abbinare la richiesta alla distribuzione specifica.

Ad esempio, si supponga di avere due distribuzioni e di aver aggiornato la configurazione DNS in modo che i nomi di dominio alternativi vengano instradati ai seguenti endpoint:

- primary.example.com punta a d111111primary.cloudfront.net
- secondary.example.com punta a d222222secondary.cloudfront.net

Se effettui una richiesta https://primary.example.com ma specifichi l'`Host`intestazione come secondary.example.com, ad esempio`curl https://primary.example.com -H "Host: secondary.example.com"`, la richiesta verrà indirizzata invece alla distribuzione secondaria.

Aggiunta di un nome di dominio alternativo al nodo di primo livello (apex di zona) per un dominio

Quando aggiungi un nome di dominio alternativo a una distribuzione, in genere crei un record CNAME nella configurazione DNS per indirizzare le query DNS relative al nome di dominio alla tua distribuzione. CloudFront Tuttavia, non potrai creare un record CNAME per il nodo di primo livello di uno spazio dei nomi DNS, noto anche come apex di zona; il protocollo DNS non lo consente. Ad esempio, se registri il nome DNS esempio.com, l'apex di zona è esempio.com. Non puoi creare un record CNAME per example.com, ma puoi creare più record CNAME per www.example.com, newproduct.example.com e così via.

Se usi Route 53 come servizio DNS, puoi creare un set di record di risorse alias che ha i due vantaggi seguenti rispetto ai record CNAME:

- Puoi creare un set di record di risorse alias per un nome di dominio al nodo di primo livello (example.com).
- Puoi creare un record HTTPS per un nome di dominio alternativo per consentire la negoziazione del protocollo come parte della ricerca DNS, se il client lo supporta. Per ulteriori informazioni, consulta Create alias resource record set.
- Non paghi per le query Route 53 quando utilizzi un set di record di risorse alias.

> **Note**
>
> Se abiliti IPv6, devi creare due set di record di risorse alias: uno per instradare il IPv4 traffico (un record A) e uno per instradare il IPv6 traffico (un record AAAA). Per ulteriori informazioni, consulta Abilita IPv6 (richieste del visualizzatore) nell'argomento Riferimento a tutte le impostazioni di distribuzione.

Per ulteriori informazioni, consulta Routing del traffico verso una distribuzione CloudFront web Amazon utilizzando il tuo nome di dominio nella Amazon Route 53 Developer Guide.

Se non utilizzi Route 53 per il tuo DNS, puoi richiedere indirizzi IP statici Anycast per indirizzare domini apex come example.com verso. CloudFront Per ulteriori informazioni, consulta Richiedi Anycast static da utilizzare IPs per l'elenco delle autorizzazioni.

Aggiunta di un nome di dominio alternativo

Il seguente elenco di attività descrive come utilizzare la CloudFront console per aggiungere un nome di dominio alternativo alla distribuzione in modo da poter utilizzare il proprio nome di dominio nei collegamenti anziché il nome di CloudFront dominio. Per informazioni sull'aggiornamento della distribuzione tramite l' CloudFront API, consultaConfigurazione delle distribuzioni.

> **Note**
>
> Se desideri che i visualizzatori utilizzino HTTPS con il tuo nome di dominio alternativo, consulta Utilizzo di nomi di dominio alternativi e HTTPS.

Prima di iniziare: assicurati di eseguire le operazioni seguenti prima di aggiornare la distribuzione per aggiungere un nome di dominio alternativo:

- Registra il nome di dominio con Route 53 o un altro registrar di domini.
- Ottieni un certificato TLS da un'autorità di certificazione (CA) autorizzata che copre il nome di dominio. Aggiungi il certificato alla distribuzione per verificare che si è autorizzati a utilizzare il dominio. Per ulteriori informazioni, consulta Requisiti per l'utilizzo di nomi di dominio alternativi.

Aggiunta di un nome di dominio alternativo

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli l'ID della distribuzione che intendi aggiornare.
3. Nella scheda Generale, scegli Aggiungi un dominio.
4. Inserisci fino a cinque domini da servire.
5. Scegli Next (Successivo).
6. Per quanto riguarda il certificato TLS, se non CloudFront riesci a trovare un certificato AWS Certificate Manager (ACM) esistente per il tuo dominio Account AWS nel `us-east-1` Regione AWS, puoi scegliere di creare automaticamente un certificato o crearlo manualmente in ACM.
7. Una volta effettuato il provisioning del certificato, devi aggiornare i record DNS con il provider DNS per dimostrare la proprietà del dominio. Le immissioni che devi inserire nei tuoi record DNS vengono fornite automaticamente nella console. CloudFront
8. Dopo aver aggiornato i record DNS, scegli Convalida certificato.
9. Quando il certificato viene convalidato, scegli Avanti.
10. Rivedi le modifiche e scegli Aggiungi domini.
11. Nella scheda General (Generale) della distribuzione, conferma che Distribution Status (Stato distribuzione) è stato modificato in Deployed (Implementato). Se tenti di utilizzare un nome di dominio alternativo prima che gli aggiornamenti per la distribuzione siano stati implementati, i collegamenti creati nella procedura seguente potrebbero non funzionare.
12. Configura il servizio DNS per il nome di dominio alternativo (ad esempio www.example.com) per indirizzare il traffico verso il nome di dominio per la tua distribuzione (ad esempio CloudFront d111111abcdef8.cloudfront.net). Il metodo utilizzato dipende dall'utilizzo di Route 53 come provider di servizi DNS per il dominio o di un altro provider. Per ulteriori informazioni, consulta Aggiungi un dominio alla tua distribuzione CloudFront standard.

    Percorso 53

    Crea un set di record di risorse alias. Con un set di record di risorse alias, non hai alcun addebito per le query Route 53. Puoi anche creare un set di record di risorse alias per il nome di dominio principale (example.com), cosa che il DNS non consente. CNAMEs Per istruzioni sulla creazione di un set di record di risorse alias, consulta Routing del traffico verso una distribuzione CloudFront web Amazon utilizzando il tuo nome di dominio nella Amazon Route 53 Developer Guide.

Facoltativamente, puoi creare un record HTTPS per un nome di dominio alternativo per consentire la negoziazione del protocollo come parte della ricerca DNS, se supportato dal client.

Come creare un set di record di risorse alias con un record HTTPS (opzionale)

1. Abilita HTTP/2 o HTTP/3 nelle impostazioni di distribuzione. CloudFront Per ulteriori informazioni, consultare Versioni HTTP supportate e Aggiornamento di una distribuzione.
2. Nella console Route 53, crea un set di record di risorse alias. Segui la procedura di routing del traffico verso una distribuzione CloudFront web Amazon utilizzando la procedura del nome di dominio.
3. Durante la creazione del set di record di risorse alias, crea un record alias con il tipo di record HTTPS.

Un altro fornitore di servizi DNS

Utilizzare il metodo fornito dal provider di servizi DNS per aggiungere un record CNAME per il dominio. Questo nuovo record CNAME reindirizzerà le query DNS dal tuo nome di dominio alternativo (ad esempio, www.example.com) al nome di dominio per la tua distribuzione (ad esempio, CloudFront d111111abcdef8.cloudfront.net). Per ulteriori informazioni, consulta la documentazione del tuo fornitore di servizi DNS.

> **Important**
>
> Se disponi già di un record CNAME per il tuo nome di dominio alternativo, aggiorna quel record o sostituiscilo con uno nuovo che punti al nome di dominio della tua distribuzione. CloudFront

13. Utilizzando `dig` o uno strumento DNS simile, conferma che la configurazione DNS creata nella fase precedente punti al nome di dominio della tua distribuzione.

L'esempio seguente mostra una richiesta `dig` per il dominio www.example.com e la parte pertinente della risposta.

```
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 sezione delle risposte mostra un record CNAME che indirizza le query relative a www.example.com al nome di dominio di distribuzione d111111abcdef8.cloudfront.net. CloudFront Se il nome sulla destra di è il nome di dominio della tua distribuzione, il record CNAME è configurato correttamente. `CNAME` CloudFront Se è un qualsiasi altro valore, ad esempio, il nome di dominio del bucket Amazon S3, il record CNAME non è stato configurato correttamente. In questo caso, torna alla fase 7 e correggi il record CNAME in modo che punti al nome di dominio della tua distribuzione.

14. Prova il nome di dominio alternativo inserendo il tuo nome URLs di dominio anziché il nome di CloudFront dominio utilizzato per la tua distribuzione.
15. Nell'applicazione, modificate l'impostazione URLs degli oggetti in modo da utilizzare il nome di dominio alternativo anziché il nome di dominio della distribuzione. CloudFront

Spostamento di un nome di dominio alternativo

Se tenti di aggiungere un nome di dominio alternativo a una distribuzione standard o a un tenant di distribuzione e il nome di dominio alternativo è già associato a una risorsa diversa, verrà visualizzato un messaggio di errore.

Ad esempio, riceverai il messaggio di `CNAMEAlreadyExists` errore (uno o più dei CNAMEs dati forniti sono già associati a una risorsa diversa) quando tenti di aggiungere www.example.com a un tenant di distribuzione o distribuzione standard, ma quel nome di dominio alternativo è già associato a una risorsa diversa.

In tal caso, potrebbe essere necessario spostare il nome di dominio alternativo esistente da una risorsa all'altra. Questa è la distribuzione di origine e la distribuzione di destinazione. È possibile spostare nomi di dominio alternativi tra i tenant di distribuzione standard di entrambe le distribuzioni. and/or

Per spostare il nome di dominio alternativo, consulta i seguenti argomenti:

Argomenti

Configurazione della distribuzione standard di destinazione o del tenant di distribuzione

Prima di poter spostare un nome di dominio alternativo, devi impostare la risorsa di destinazione. Si tratta della distribuzione standard di destinazione o del tenant di distribuzione in cui stai trasferendo il nome di dominio alternativo.

Standard distribution

Come impostare una distribuzione standard di destinazione

1. Richiedi un certificato TLS. Questo certificato include il nome di dominio alternativo come Subject o Subject Alternative Domain (SAN) oppure un carattere jolly (*) che copre il nome di dominio alternativo che stai spostando. Se non ne possiedi uno, puoi richiederlo ad AWS Certificate Manager (ACM) o ad un'altra autorità di certificazione (CA) e importarlo in ACM.

   > **Note**
   >
   > Devi richiedere o importare il certificato nella Regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

   Per ulteriori informazioni, consulta Richiesta di un certificato pubblico utilizzando la console e Importazione di un certificato in AWS Certificate Manager nella Guida per l'utente di AWS Certificate Manager .
2. Se non hai ancora creato la distribuzione standard di destinazione, creane una adesso. Come parte della creazione della distribuzione standard, associa il certificato a questa distribuzione standard. Per ulteriori informazioni, consulta Creazione di una distribuzione.

   Se disponi già di una distribuzione standard di destinazione, associa il certificato alla distribuzione standard. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.

3. Se stai spostando nomi di dominio alternativi all'interno dello stesso Account AWS, salta questo passaggio.

   Per spostare un nome di dominio alternativo da uno Account AWS all'altro, devi creare un record TXT nella configurazione DNS. Questa fase di verifica aiuta a prevenire trasferimenti di dominio non autorizzati. CloudFront utilizza questo record TXT per convalidare la proprietà del nome di dominio alternativo.

   Nella configurazione DNS, crea un record TXT DNS che associ il nome di dominio alternativo alla distribuzione standard di destinazione. Il formato del record TXT può variare a seconda del tipo di dominio.

   - Per i sottodomini, specificare un trattino basso (_) davanti al nome di dominio alternativo. Di seguito è riportato un esempio di record TXT.

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

   - Per un apex (o dominio root), specifica un trattino basso e un punto (_.) davanti al nome di dominio. Di seguito è riportato un esempio di record TXT.

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

Distribution tenant

Come configurare il tenant di distribuzione di destinazione

1. Richiedi un certificato TLS. Questo certificato include il nome di dominio alternativo come Subject o Subject Alternative Domain (SAN) oppure un carattere jolly (*) che copre il nome di dominio alternativo che stai spostando. Se non ne possiedi uno, puoi richiederlo ad AWS Certificate Manager (ACM) o ad un'altra autorità di certificazione (CA) e importarlo in ACM.

   > **Note**
   >
   > Devi richiedere o importare il certificato nella Regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

   Per ulteriori informazioni, consulta Richiesta di un certificato pubblico utilizzando la console e Importazione di un certificato in AWS Certificate Manager nella Guida per l'utente di AWS Certificate Manager .

2. Se non hai ancora creato il tenant di distribuzione di destinazione, creane uno adesso. Come parte della creazione del tenant di distribuzione, associa il certificato al tenant di distribuzione. Per ulteriori informazioni, consulta Creazione di una distribuzione.

   Se disponi già di un tenant di distribuzione di destinazione, associa il certificato al tenant di distribuzione. Per ulteriori informazioni, consulta Aggiunta di un dominio e di un certificato (tenant di distribuzione).

3. Se stai spostando nomi di dominio alternativi all'interno dello stesso Account AWS, salta questo passaggio.

   Per spostare un nome di dominio alternativo da uno Account AWS all'altro, devi creare un record TXT nella configurazione DNS. Questa fase di verifica aiuta a prevenire trasferimenti di dominio non autorizzati e CloudFront utilizza questo record TXT per convalidare la proprietà del nome di dominio alternativo.

   Nella configurazione DNS, crea un record TXT DNS che associ il nome di dominio alternativo al tenant di distribuzione di destinazione. Il formato del record TXT può variare a seconda del tipo di dominio.

   - Per i sottodomini, specificare un trattino basso (_) davanti al nome di dominio alternativo. Di seguito è riportato un esempio di record TXT.

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

   - Per un apex (o dominio root), specifica un trattino basso e un punto (_.) davanti al nome di dominio. Di seguito è riportato un esempio di record TXT.

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

Successivamente, consulta l’argomento seguente per individuare la distribuzione standard di origine o il tenant di distribuzione già associato al nome di dominio alternativo.

Individuazione della distribuzione standard di origine o del tenant di distribuzione

Prima di poter spostare un nome di dominio alternativo da una distribuzione (standard o tenant) a un’altra, individua la distribuzione di origine. Questa è la risorsa a cui è già associato il nome di dominio alternativo. Una volta che conosci l' Account AWS ID delle risorse di distribuzione di origine e di destinazione, puoi determinare come spostare il nome di dominio alternativo.

> **Note**
>
> - Ti consigliamo di utilizzare l'operazione ListDomainConflictsAPI, poiché supporta sia le distribuzioni standard che i tenant di distribuzione.
> - L'operazione ListConflictingAliasesAPI supporta solo distribuzioni standard.

Segui questi esempi per trovare la distribuzione di origine (standard o tenant).

list-domain-conflicts

> **Tip**
>
> - Per una distribuzione standard, è necessario disporre delle autorizzazioni `cloudfront:GetDistribution` e `cloudfront:ListDomainConflicts`.
> - Per un tenant di distribuzione, è necessario disporre delle autorizzazioni `cloudfront:GetDistributionTenant` e `cloudfront:ListDomainConflicts`.

Come utilizzare **`list-domain-conflicts`** per trovare la distribuzione standard di origine e il tenant di distribuzione

1. Usa il comando `list-domain-conflicts` come mostrato nell'esempio seguente.

   a. Sostituisci *`www.example.com`* con il nome di dominio.

   b. Per `domain-control-validation-resource`, specifica l'ID della distribuzione standard di destinazione o del tenant di distribuzione impostato in precedenza. È necessario disporre di una distribuzione standard o di un tenant di distribuzione associato a un certificato che copra il dominio specificato.

   c. Esegui questo comando utilizzando le credenziali che si trovano nella distribuzione Account AWS standard o nel tenant di distribuzione di destinazione.

   Richiesta

   In questo esempio viene specificato un tenant di distribuzione.

   ```
   aws cloudfront list-domain-conflicts \
   ```

```
--domain www.example.com \
--domain-control-validation-resource
 "DistributionTenantId=dt_2x9GhoK0TZRsohWzv1b9It8JABC"
```

Risposta

Per ogni nome di dominio nell'output del comando, puoi vedere le informazioni seguenti:

- Il tipo di risorsa a cui è associato il dominio
- L'ID della risorsa
- L' Account AWS ID che possiede la risorsa

L'ID risorsa e l'ID account sono parzialmente nascosti. Ciò consente di identificare la distribuzione standard o il tenant di distribuzione appartenente all'account e contribuisce a proteggere le informazioni di quelli di cui non si è proprietari.

```
{
    "DomainConflicts": [
        {
            "Domain": "www.example.com",
            "ResourceType": "distribution-tenant",
            "ResourceId": "***************ohWzv1b9It8JABC",
            "AccountId": "******112233"
        }
    ]
}
```

Nella risposta vengono elencati tutti i nomi di dominio che sono in conflitto o si sovrappongono a quello specificato.

Esempio

- Se lo specifichi*tenant1.example.com*, la risposta include tenant1.example.com e il nome di dominio alternativo con caratteri jolly sovrapposti (*.example.com se esiste).
- Se lo specifichi**.tenant1.example.com*, la risposta include *.tenant1.example.com e tutti i nomi di dominio alternativi coperti da tale wildcard (ad esempio, test.tenant1.example.com, dev.tenant1.example.com e così via).

2. Nella risposta, trova la distribuzione standard di origine o il tenant di distribuzione per il nome di dominio alternativo che stai trasferendo e annota l'ID. Account AWS

3. Confronta l'ID account della distribuzione standard di origine o il tenant di distribuzione con l'ID account in cui hai creato la distribuzione standard di destinazione o il tenant di destinazione nella fase precedente. Puoi quindi determinare se l'origine e la destinazione si trovano nello stesso Account AWS. In questo modo è possibile determinare come spostare il nome di dominio alternativo.

   Per ulteriori informazioni, vedi il comando list-domain-conflicts nel Riferimento dell'AWS Command Line Interface .

list-conflicting-aliases (standard distributions only)

> **Tip**
>
> È necessario disporre delle autorizzazioni `cloudfront:GetDistribution` e `cloudfront:ListConflictingAliases` sulla distribuzione standard di destinazione.

Come usare **`list-conflicting-aliases`** per trovare la distribuzione standard di origine

1. Usa il comando `list-conflicting-aliases` come mostrato nell'esempio seguente.

   a. Sostituiscilo *`www.example.com`* con il nome di dominio alternativo e *`EDFDVBD6EXAMPLE`* con l'ID della distribuzione standard di destinazione che hai impostato in precedenza.

   b. Esegui questo comando utilizzando le credenziali che si trovano nello stesso Account AWS della distribuzione standard di destinazione.

   Richiesta

   In questo esempio viene specificata una distribuzione standard.

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

   Risposta

Per ogni nome di dominio alternativo nell'output del comando, puoi visualizzare l'ID della distribuzione standard a cui è associato e l'ID dell' Account AWS che possiede la distribuzione standard. La distribuzione standard e l'account IDs sono parzialmente nascosti, il che ti consente di identificare le distribuzioni standard e gli account di tua proprietà e aiuta a proteggere le informazioni di quelli che non possiedi.

```
{
    "ConflictingAliasesList": {
        "MaxItems": 100,
        "Quantity": 1,
        "Items": [
            {
                "Alias": "www.example.com",
                "DistributionId": "*******EXAMPLE",
                "AccountId": "******112233"
            }
        ]
    }
}
```

Nella risposta vengono elencati i nomi di dominio alternativi che sono in conflitto o si sovrappongono a quello specificato.

Esempio

- Se lo specifichi*www.example.com*, la risposta include www.example.com e il nome di dominio alternativo con caratteri jolly sovrapposti (*.example.com), se esiste.
- Se lo specifichi**.example.com*, la risposta include *.example.com e tutti i nomi di dominio alternativi coperti da quella wildcard (ad esempio, www.example.com, test.example.com, dev.example.com e così via).

2. Trova la distribuzione standard per il nome di dominio alternativo che stai trasferendo e annota l'ID. Account AWS Confronta questo ID account con l'ID dell'account in cui è stata creata la distribuzione standard di destinazione nella fase precedente. Potrai quindi determinare se queste due distribuzioni standard coincidono Account AWS e come spostare il nome di dominio alternativo.

   Per ulteriori informazioni, vedi il comando list-conflicting-aliases nel Riferimento dell'AWS Command Line Interface .

Successivamente, consulta il seguente argomento per spostare il nome di dominio alternativo.

Spostamento del nome di dominio alternativo

A seconda della situazione, scegli una delle seguenti modalità per spostare il nome di dominio alternativo:

Le distribuzioni di origine e di destinazione (standard o tenant) si trovano nello stesso Account AWS

Utilizza il comando update-domain-association nella AWS Command Line Interface (AWS CLI) per spostare il nome di dominio alternativo.

Questo comando funziona per tutti gli spostamenti dello stesso account, incluso quando il nome di dominio alternativo è un dominio apex (chiamato anche dominio root, come example.com).

Le distribuzioni di origine e di destinazione (standard o tenant) si trovano in Account AWS diversi

Se hai accesso alla distribuzione standard di origine o al tenant di distribuzione, il nome di dominio alternativo non è un dominio apex e non stai già utilizzando un carattere jolly che si sovrappone a tale nome di dominio alternativo, utilizza un carattere jolly per spostare il nome di dominio alternativo. Per ulteriori informazioni, consulta the section called “Utilizzo di un carattere jolly per spostare un nome di dominio alternativo”.

Se non hai accesso a Account AWS quello che ha la distribuzione standard di origine o il tenant di distribuzione, puoi provare a utilizzare il update-domain-association comando per spostare il nome di dominio alternativo. Prima di poter spostare il nome di dominio alternativo, è necessario disabilitare la distribuzione standard di origine o il tenant di distribuzione. Per ulteriori informazioni, consulta the section called “Contatta Supporto AWS per spostare un nome di dominio alternativo”.

> **Note**
>
> Puoi utilizzare il comando associate-alias, anche se supporta solo le distribuzioni standard. Vedi AssociateAliasnell'Amazon CloudFront API Reference.

update-domain-association (standard distributions and distribution tenants)

Come utilizzare **`update-domain-association`** per spostare un nome di dominio alternativo

1. Utilizza il comando `update-domain-association` come visualizzato nell'esempio seguente.

   a. Sostituiscilo *`example.com`* con il nome di dominio alternativo e specifica l'ID della distribuzione standard o del tenant di distribuzione di destinazione.

   b. Esegui questo comando utilizzando le credenziali che si trovano nello stesso Account AWS della distribuzione standard di destinazione o del tenant di distribuzione.

> Prendi nota delle seguenti limitazioni
>
> - Oltre all'autorizzazione `cloudfront:UpdateDomainAssociation`, è necessario disporre dell'autorizzazione `cloudfront:UpdateDistribution` per aggiornare una distribuzione standard. Per aggiornare un tenant di distribuzione, è necessario disporre dell'autorizzazione `cloudfront:UpdateDistributionTenant`.
> - Se le distribuzioni di origine e di destinazione (standard o tenant) sono diverse Account AWS, è necessario disabilitare l'origine prima di poter spostare il dominio.
> - La distribuzione di destinazione deve essere configurata nel modo descritto in the section called "Configurazione della distribuzione standard di destinazione o del tenant di distribuzione".

Richiesta

```
aws cloudfront update-domain-association \
  --domain "www.example.com" \
  --target-resource DistributionTenantId=dt_9Fd3xTZq7Hl2KABC \
  --if-match E3UN6WX5ABC123
```

Risposta

```
{
    "ETag": "E7Xp1Y3N9DABC",
```

```
    "Domain": "www.example.com",
    "ResourceId": "dt_9Fd3xTZq7Hl2KABC"
}
```

Questo comando rimuove il nome di dominio alternativo dalla distribuzione standard di origine o dal tenant di distribuzione e lo aggiunge alla distribuzione standard di destinazione o al tenant di distribuzione.

2. Una volta completata la distribuzione di destinazione, aggiorna la configurazione DNS per indirizzare il nome di dominio verso l'endpoint di routing. CloudFront Ad esempio, il tuo record DNS indirizzerà il tuo nome di dominio alternativo (`www.example.com`) al nome di dominio fornito d111111abcdef8.cloudfront.net. CloudFront Se la destinazione è un tenant di distribuzione, specifica l'endpoint del gruppo di connessioni. Per ulteriori informazioni, consulta Indirizza i domini a CloudFront.

associate-alias (standard distributions only)

Come utilizzare **`associate-alias`** per spostare un nome di dominio alternativo

1. Utilizza il comando `associate-alias` come visualizzato nell'esempio seguente.

   a. Sostituiscilo *`www.example.com`* con il nome di dominio alternativo e con l'ID di distribuzione standard di destinazione. *`EDFDVBD6EXAMPLE`*

   b. Esegui questo comando utilizzando le credenziali che si trovano nello stesso Account AWS della distribuzione standard di destinazione.

   > Prendi nota delle seguenti limitazioni
   >
   > - È necessario disporre delle autorizzazioni `cloudfront:AssociateAlias` e `cloudfront:UpdateDistribution` sulla distribuzione standard di destinazione.
   > - Se la distribuzione standard di origine e quella di destinazione coincidono Account AWS, è necessario disporre dell'`cloudfront:UpdateDistribution`autorizzazione per la distribuzione standard di origine.
   > - Se la distribuzione standard di origine e la distribuzione standard di destinazione sono diverse Account AWS, è necessario prima disabilitare la distribuzione standard di origine.

- La distribuzione standard di destinazione deve essere configurata come descritto in the section called “Configurazione della distribuzione standard di destinazione o del tenant di distribuzione”.

Richiesta

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

Questo comando rimuove il nome di dominio alternativo dalla distribuzione standard di origine e lo sposta nella distribuzione standard di destinazione.

2. Dopo che la distribuzione standard di destinazione è stata completamente distribuita, aggiornare la configurazione DNS in modo da puntare il record DNS del nome di dominio alternativo al nome del dominio di distribuzione della distribuzione standard di destinazione. Ad esempio, il record DNS indicherebbe il nome di dominio alternativo (`www.example.com`) al nome di dominio CloudFront fornito d111111abcdef8.cloudfront.net.

Per ulteriori informazioni, consulta il comando associate-alias nel Riferimento ai comandi AWS CLI .

Utilizzo di un carattere jolly per spostare un nome di dominio alternativo

Se la distribuzione di origine è in una distribuzione Account AWS diversa da quella di destinazione e la distribuzione dell'origine è abilitata, puoi utilizzare un jolly per spostare il nome di dominio alternativo.

> **Note**
>
> Non puoi usare un carattere jolly per spostare un dominio apex (come example.com). Per spostare un dominio apex quando le distribuzioni di origine e di destinazione si trovano in Account AWS diversi, contatta il Supporto. Per ulteriori informazioni, consulta the section called “Contatta Supporto AWS per spostare un nome di dominio alternativo”.

Come utilizzare un carattere jolly per spostare un nome di dominio alternativo

> **Note**
>
> Questo processo comporta più aggiornamenti alle distribuzioni. Attendere che ogni distribuzione implementi completamente l'ultima modifica prima di procedere con il passaggio successivo.

1. Aggiornare la distribuzione di destinazione per aggiungere un nome di dominio alternativo con caratteri jolly che copra il nome di dominio alternativo che si sta spostando. Ad esempio, se il nome di dominio alternativo che si sta spostando è www.example.com, aggiungere il nome di dominio alternativo *.example.com alla distribuzione di destinazione. A tale scopo, il SSL/TLS certificato sulla distribuzione di destinazione deve includere il nome di dominio wildcard. Per ulteriori informazioni, consulta the section called “Aggiornamento di una distribuzione”.
2. Aggiornare le impostazioni DNS per il nome di dominio alternativo in modo che punti al nome di dominio della distribuzione di destinazione. Ad esempio, se il nome di dominio alternativo che si sta spostando è www.example.com, aggiornare il record DNS di www.example.com per instradare il traffico al nome di dominio della distribuzione di destinazione (ad esempio d111111abcdef8.cloudfront.net).

   > **Note**
   >
   > Anche dopo aver aggiornato le impostazioni DNS, il nome di dominio alternativo viene comunque servito dalla distribuzione di origine poiché è lì che è attualmente configurato il nome di dominio alternativo.

3. Aggiornare la distribuzione di origine per rimuovere il nome di dominio alternativo. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
4. Aggiornare la distribuzione di destinazione per aggiungere il nome di dominio alternativo. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
5. Utilizza dig (o uno strumento di query DNS simile) per verificare che il record DNS per il nome di dominio alternativo venga risolto nel nome di dominio della distribuzione di destinazione.
6. (Facoltativo) Aggiornare la distribuzione di destinazione per rimuovere il nome di dominio alternativo con carattere jolly.

Contatta Supporto AWS per spostare un nome di dominio alternativo

Se le distribuzioni di origine e di destinazione sono diverse Account AWS e non hai accesso alla distribuzione di origine Account AWS o non puoi disabilitarla, puoi contattare Supporto per spostare il nome di dominio alternativo.

A cui rivolgersi Supporto per spostare un nome di dominio alternativo

1. Impostare una distribuzione di destinazione, incluso il record TXT DNS che punta alla distribuzione di destinazione. Per ulteriori informazioni, consulta Configurazione della distribuzione standard di destinazione o del tenant di distribuzione.
2. Contattaci Supporto per richiedere che verifichino che il dominio sia di tua proprietà e trasferisca il dominio nella nuova CloudFront distribuzione per te.
3. Dopo che la distribuzione di destinazione è stata completamente distribuita, aggiornare la configurazione DNS in modo da puntare il record DNS del nome di dominio alternativo al nome del dominio di distribuzione della distribuzione di destinazione.

Rimozione di un nome di dominio alternativo

Se desideri interrompere il routing del traffico di un dominio o sottodominio verso una CloudFront distribuzione, segui i passaggi di questa sezione per aggiornare sia la configurazione DNS che la distribuzione. CloudFront

È importante rimuovere i nomi di dominio alternativi dalla distribuzione e aggiornare la configurazione DNS. Questo aiuta a prevenire problemi in un secondo momento se desideri associare il nome di dominio a un'altra distribuzione. CloudFront Se un nome di dominio alternativo è già associato a una distribuzione, non può essere configurato con un'altra.

> **Note**
>
> Se desideri rimuovere il nome di dominio alternativo da questa distribuzione in modo da aggiungerlo a un'altra, segui la procedura descritta in Spostamento di un nome di dominio alternativo. Se invece segui i passaggi indicati qui (per rimuovere un dominio) e poi aggiungi il dominio a un'altra distribuzione, passerà un periodo di tempo durante il quale il dominio non si collegherà alla nuova distribuzione perché CloudFront si sta propagando agli aggiornamenti nelle edge location.

Per rimuovere un nome di dominio alternativo da una distribuzione

1. Per iniziare, indirizza il traffico Internet del tuo dominio verso un'altra risorsa diversa dalla tua CloudFront distribuzione, ad esempio un sistema di bilanciamento del carico ELB. Oppure puoi eliminare il record DNS verso cui indirizza il traffico. CloudFront

   Scegli una delle seguenti operazioni, a seconda del servizio DNS del dominio:

   - Se stai utilizzando Route 53, aggiorna o elimina i record di alias o i record CNAME. Per ulteriori informazioni, consulta Modifica di record o Eliminazione di record.
   - Se stai utilizzando un altro fornitore di servizi DNS, usa il metodo fornito dal fornitore di servizi DNS per aggiornare o eliminare il record CNAME che indirizza il traffico a CloudFront. Per ulteriori informazioni, consulta la documentazione del tuo fornitore di servizi DNS.
2. Dopo aver aggiornato i record DNS del dominio, attendi fino a quando le modifiche non si sono propagate e i resolver DNS esegue il routing del traffico verso la nuova risorsa. È possibile controllare il completamento di questa operazione creando alcuni link che utilizzano il tuo dominio nell'URL.
3. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home e aggiorna la CloudFront distribuzione per rimuovere il nome di dominio procedendo come segue:

   a. Scegli l'ID della distribuzione che intendi aggiornare.
   b. Nella scheda General (Generale), seleziona Edit (Modifica).
   c. In Alternate Domain Names (CNAMEs), rimuovi il nome di dominio alternativo (o i nomi di dominio) che non desideri più utilizzare per la tua distribuzione.
   d. Seleziona Yes, Edit (Sì, modifica).

Utilizzo di caratteri jolly nei nomi di dominio alternativi

Quando aggiungi nomi di dominio alternativi, puoi utilizzare il carattere jolly* all'inizio di un nome di dominio invece di aggiungere i singoli sottodomini. Ad esempio, con un nome di dominio alternativo di *.example.com, puoi utilizzare qualsiasi nome di dominio che termina con example.com nel tuo, ad esempio www.example.com, product-name.example.com URLs, marketing.product-name.example.com e così via. Il percorso di un oggetto è lo stesso indipendentemente dal nome di dominio, ad esempio:

- www.example. com/images/image.jpg

- nome del prodotto.esempio. com/images/image.jpg
- marketing.nome-prodotto.esempio. com/images/image.jpg

Segui questi requisiti per i nomi di dominio alternativi che includono caratteri jolly:

- Il nome di dominio alternativo deve iniziare con un asterisco e un punto (*.).
- Non puoi utilizzare un carattere jolly per sostituire parte di un nome di sottodominio, come *domain.example.com.
- Non puoi sostituire un sottodominio nel mezzo di un nome di dominio, come ad esempio subdomain.*.example.com.
- Tutti i nomi di dominio alternativi, inclusi i nomi di dominio alternativi che utilizzano caratteri jolly, devono essere coperti dal nome di oggetto alternativo (SAN) sul certificato.

Un nome di dominio alternativo con carattere jolly, ad esempio *.example.com, può includere un altro nome di dominio alternativo in uso, ad esempio example.com.

Utilizzare WebSockets con le distribuzioni CloudFront

Amazon CloudFront supporta l'utilizzo WebSocket di un protocollo basato su TCP utile quando sono necessarie connessioni bidirezionali di lunga durata tra client e server. Una connessione permanente è spesso un requisito con applicazioni in tempo reale. Gli scenari in cui potresti utilizzare WebSockets includono piattaforme di social chat, spazi di lavoro per la collaborazione online, giochi multigiocatore e servizi che forniscono feed di dati in tempo reale come piattaforme di trading finanziario. I dati tramite una WebSocket connessione possono fluire in entrambe le direzioni per una comunicazione full-duplex.

WebSocket la funzionalità viene abilitata automaticamente per funzionare con qualsiasi distribuzione. Per WebSockets utilizzarla, configura uno dei seguenti comandi nel comportamento della cache associato alla tua distribuzione:

- Inoltra tutte le intestazioni di richiesta visualizzatore all'origine. Puoi utilizzare la policy di richiesta di origine AllViewer gestita.
- Inoltra specificatamente le intestazioni di richiesta `Sec-WebSocket-Key` e `Sec-WebSocket-Version` nella policy di richiesta origine.

Come funziona il WebSocket protocollo

Il WebSocket protocollo è un protocollo indipendente basato su TCP che consente di evitare il sovraccarico e il potenziale aumento della latenza di HTTP.

Per stabilire una WebSocket connessione, il client invia una richiesta HTTP regolare che utilizza la semantica di aggiornamento di HTTP per modificare il protocollo. Il server può quindi completare l'handshake. La WebSocket connessione rimane aperta e il client o il server possono scambiarsi frame di dati senza dover stabilire nuove connessioni ogni volta.

Per impostazione predefinita, il WebSocket protocollo utilizza la porta 80 per WebSocket le connessioni regolari e la porta 443 per WebSocket le connessioni tramite TLS. Le opzioni che scegli per te Protocollo (solo origini personalizzate) si applicano alle WebSocket connessioni CloudFront Viewer Protocol Policy (Policy protocollo visualizzatore) e anche al traffico HTTP.

Requisiti WebSocket

WebSocket le richieste devono essere conformi alla RFC 6455 nei seguenti formati standard.

Example Esempio di richiesta 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
```

Example Esempio di risposta del server

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+xOo=
Sec-WebSocket-Protocol: chat
```

Se la WebSocket connessione viene interrotta dal client o dal server o a causa di un'interruzione della rete, è previsto che le applicazioni client riavviino la connessione con il server.

Intestazioni consigliate WebSocket

Per evitare problemi imprevisti relativi alla compressione durante l'utilizzo WebSockets, ti consigliamo di includere le seguenti intestazioni in una policy di richiesta di origine:

- `Sec-WebSocket-Key`
- `Sec-WebSocket-Version`
- `Sec-WebSocket-Protocol`
- `Sec-WebSocket-Accept`
- `Sec-WebSocket-Extensions`

> **Note**
>
> Attualmente, supporta CloudFront solo WebSocket connessioni tramite il protocollo HTTP/1.1.

Richiedi Anycast static da utilizzare IPs per l'elenco delle autorizzazioni

Puoi richiedere Anycast static IPs da utilizzare con le tue CloudFront distribuzioni. Gli elenchi IP statici Anycast possono contenere solo indirizzi IPv4 IP o entrambi IPv4 e IPv6 indirizzi IP. Questi indirizzi IP sono dedicati all'utente Account AWS e sono distribuiti in diverse aree geografiche.

Puoi richiedere 21 indirizzi IP statici anycast da inserire nella lista dei consentiti con provider di rete, in modo da poter rinunciare agli addebiti dei dati per i visualizzatori che accedono all'applicazione. In alternativa, è possibile utilizzare questi dispositivi statici IPs all'interno dei firewall di sicurezza in uscita per controllare lo scambio di traffico con applicazioni approvate. Gli elenchi di IP statici anycast possono essere utilizzati con una o più distribuzioni.

Se desideri abilitare il routing dei domini apex (come example.com) direttamente verso le tue CloudFront distribuzioni, puoi richiedere 3 indirizzi IP statici Anycast per questo caso d'uso. Quindi, aggiungi i record A nel tuo DNS a cui indirizzare il dominio apex. CloudFront

Anycast static IPs funziona con Server Name Indication (SNI). Per ulteriori informazioni, consulta Utilizzo di SNI per servire le richieste HTTPS (funziona per la maggior parte dei client).

Prerequisiti

Per utilizzare gli elenchi IP statici Anycast con la CloudFront distribuzione, è necessario selezionare Usa tutte le edge location per la classe di prezzo della distribuzione. Per ulteriori informazioni sui prezzi, consulta Prezzi di CloudFront .

Richiesta di un elenco di IP statici anycast

Richiedete un elenco di IP statici Anycast da utilizzare con la vostra CloudFront distribuzione.

Come richiedere un elenco di IP statici anycast

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione a sinistra, scegli Statico IPs.
3. Per Richiesta, scegli il link per contattare l' CloudFront assistenza tecnica.
4. Fornisci le informazioni sul carico di lavoro (byte di richiesta al secondo e richieste al secondo).
5. CloudFront support engineering esamina la tua richiesta. Il processo di revisione può richiedere fino a due giorni.

Dopo che la richiesta è stata approvata, puoi creare un elenco di IP statici anycast e associarlo a una o più distribuzioni.

Creazione di un elenco di IP statici anycast

Prima di iniziare, richiedi un elenco di IP statici anycast come spiegato nella sezione precedente.

Come creare un elenco di IP statici anycast

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione a sinistra, scegli Statico IPs.
3. Scegli Crea elenco di IP anycast.
4. In Nome, immetti un nome.
5. Per Casi d’uso di IP statici, seleziona il caso d’uso appropriato.
6. Per il tipo di indirizzo IP, specifica una delle seguenti opzioni:

- IPv4— Assegna un elenco di soli indirizzi IPv4
- Dualstack: assegna un elenco di entrambi gli indirizzi IPv4 IPv6

7. Rivedi i termini e i prezzi del servizio e scegli Invia.

Dopo aver creato l'elenco di IP statici, puoi visualizzare gli indirizzi IP allocati nella pagina dei dettagli dell'elenco di IP statici. Puoi anche associare le distribuzioni all'elenco di IP statici.

Associazione di un elenco di IP statici anycast a una distribuzione esistente

Prima di iniziare, richiedi e crea un elenco di IP statici anycast come spiegato nelle sezioni precedenti.

Verificate che le seguenti impostazioni di distribuzione siano compatibili con l'elenco di IP statici Anycast:

- Price Class (Categoria prezzo)ha l'impostazione Usa tutte le edge location (migliori prestazioni).
- Se IPv6è abilitata, è possibile associare un elenco IP statico Anycast dualstack. Un elenco di IP statici Anycast che contiene solo IPv4 indirizzi non può essere associato alle distribuzioni se abilitato. IPv6

Come associare un elenco di IP statici anycast a una distribuzione esistente

- Esegui una delle seguenti operazioni:
  - Associa l'elenco di IP statici dalla pagina di dettaglio dell'elenco di IP statici:
    1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
    2. Scegli Statico IPs nel riquadro di navigazione a sinistra.
    3. Seleziona il nome dell'elenco di IP statici.
    4. Scegli Associa distribuzioni.
    5. Seleziona una o più distribuzioni e scegli Associa distribuzioni.
  - Associa l'elenco di IP statici dalla pagina dei dettagli della distribuzione:
    1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Nel riquadro di navigazione a sinistra, scegli Distribuzioni.

3. Scegli il nome della distribuzione.
4. Nel riquadro Generale, in Impostazioni, scegli Modifica.
5. Per Elenco di IP anycast, seleziona l'elenco di IP statici anycast da utilizzare con questa distribuzione.
6. Scegli Save changes (Salva modifiche).

Associazione di un elenco di IP statici anycast a una nuova distribuzione

Prima di iniziare, richiedi e crea un elenco di IP statici anycast come spiegato nelle sezioni precedenti.

Come associare un elenco di IP statici anycast a una nuova distribuzione

- Creare una nuova distribuzione . Per ulteriori informazioni, consulta Crea una CloudFront distribuzione nella console. Per Impostazioni, è necessario effettuare le seguenti selezioni per utilizzare l'elenco di IP statici anycast:
  - Per Elenco di IP anycast, seleziona l'elenco di IP statici anycast dall'elenco a discesa.
  - Per Classe di prezzo, seleziona Utilizza tutte le posizioni edge (prestazioni migliori).
  - Nota: se il tuo IP statico Anycast utilizza solo IPv4 e non dualstack, per IPv6, seleziona Off.

Completa la creazione della distribuzione. Puoi scegliere qualsiasi altra impostazione e configurazione non richiesta per gli elenchi di IP statici anycast in base alle tue esigenze.

Per ulteriori informazioni sulle quote relative agli elenchi di IP statici Anycast, consulta Amazon CloudFront endpoints and quotas nel. Riferimenti generali di AWS

Associa un elenco di IP statici Anycast a un gruppo di connessioni

Prima di iniziare, richiedi e crea un elenco di IP statici Anycast come spiegato nelle sezioni precedenti.

Per associare un elenco IP statico Anycast a un nuovo gruppo di connessioni

1. Assicurati di aver abilitato i gruppi di connessione in Impostazioni.
2. Crea un gruppo di connessione. Per ulteriori informazioni, consulta Creare un gruppo di connessione personalizzato.

3. Per le Impostazioni, è necessario effettuare le seguenti selezioni per utilizzare l'elenco di IP statici Anycast.
   - Per Elenco di IP anycast, seleziona l'elenco di IP statici anycast dall'elenco a discesa.
4. Completate la creazione del gruppo di connessione.

> **Note**
>
> Se il tuo IP statico Anycast utilizza solo il dualstack IPv4 e non lo utilizza, per IPv6, seleziona Off.

Per ulteriori informazioni sulle quote relative agli elenchi di IP statici Anycast, consulta Amazon CloudFront endpoints and quotas nel. Riferimenti generali di Amazon Web Services

Aggiornare un elenco di IP statici Anycast

Dopo aver creato l'indirizzo IP statico Anycast e averlo associato a una distribuzione, è possibile modificare il tipo di indirizzo IP dell'elenco IP statico Anycast.

Per aggiornare un elenco di IP statici Anycast

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione a sinistra, scegli Statico IPs.
3. Seleziona il nome dell'elenco di IP statici.
4. Scegli Modifica.
5. Per il tipo di indirizzo IP, specifica una delle seguenti opzioni:
   - IPv4— Assegna un elenco di soli indirizzi IPv4
   - Dualstack: assegna un elenco di entrambi gli indirizzi IPv4 IPv6

> **Note**
>
> Non puoi scegliere IPv4se la distribuzione associata è già abilitata. IPv6 A tale scopo, disattivate IPv6 prima di poter aggiornare il tipo di indirizzo IP per il vostro IP statico Anycast. Per ulteriori informazioni, consulta Abilita IPv6 per le CloudFront distribuzioni.

6. Scegliete Invia per salvare le modifiche e aggiornare l'elenco degli IP statici di Anycast.

Implementa il tuo IP all' CloudFront utilizzo di IPAM

Questo tutorial mostra come utilizzare IPAM per gestire il BYOIP per gli elenchi di IP CIDRs statici di Anycast. CloudFront

Argomenti

Cos'è BYOIP per Anycast Static? IPs

CloudFront supporta l'invio dei propri IPv4 indirizzi tramite BYOIP di IPAM per servizi globali. Tramite l'interfaccia unificata di IPAM, i clienti possono creare pool di indirizzi IP dedicati utilizzando i propri indirizzi IP (BYOIP) e assegnarli alle CloudFront distribuzioni, sfruttando al contempo la rete AWS mondiale di distribuzione dei contenuti per fornire applicazioni e contenuti. I tuoi indirizzi IP vengono pubblicizzati da più edge location contemporaneamente utilizzando il routing anycast. CloudFront

Perché usare questa funzionalità?

Controlla l'accesso alla rete negli elenchi consentiti per:

- Consenti agli operatori di rete di inserire gli indirizzi IP nell'elenco degli indirizzi IP in modo da esonerare gli addebiti relativi ai dati per gli utenti approvati
- Configura i firewall di sicurezza in uscita per limitare il traffico solo alle applicazioni approvate

Semplifica le operazioni e le migrazioni

- Indirizza i domini apex (example.com) direttamente a destinazione CloudFront aggiungendo record A che rimandano ai tuoi dati statici IPs
- Esegui la migrazione da altri CDNs senza aggiornare l'infrastruttura IP o le configurazioni del firewall
- Mantieni le liste di autorizzazione IP esistenti con partner e clienti
- Condividi un unico elenco di IP statici Anycast su più distribuzioni CloudFront

Branding coerente

- Mantieni lo spazio di indirizzo IP esistente per un branding coerente quando passi a AWS

Prerequisiti

Per utilizzare gli elenchi IP statici Anycast con la CloudFront distribuzione, è necessario selezionare Usa tutte le edge location per la classe di prezzo per la distribuzione. Per ulteriori informazioni sui prezzi, consulta Prezzi di CloudFront. Per Bring Your Own IP (BYOIP), è inoltre necessario disabilitarlo IPv6 per il gruppo di distribuzione o di connessione.

Completa questi passaggi prima di iniziare:

- Configurazione IPAM: vedi Integrazione di IPAM con gli account e Creazione di un IPAM.
- Verifica del dominio: verifica il controllo del dominio.
- Crea un pool di primo livello: segui i passaggi da 1 a 2 in Porta il tuo IPv4 CIDR in IPAM.
- Crea un pool IPAM con impostazioni locali globali da utilizzare. CloudFront Per ulteriori informazioni, consulta Bring your own IP to CloudFront use IPAM.

> **Note**
>
> Richiede tre blocchi IPv4 CIDR /24.

Fase 1: Richiedere un elenco IP statico Anycast

Richiedete un elenco di IP statici Anycast da utilizzare con la vostra CloudFront distribuzione.

Come richiedere un elenco di IP statici anycast

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione a sinistra, scegli Statico IPs.
3. Per Richiesta, scegli il link per contattare l' CloudFront assistenza tecnica.
4. Fornisci le informazioni sul carico di lavoro (byte di richiesta al secondo e richieste al secondo).
5. CloudFront support engineering esamina la tua richiesta. Il processo di revisione può richiedere fino a due giorni.
6. Dopo che la richiesta è stata approvata, puoi creare un elenco di IP statici anycast e associarlo a una o più distribuzioni.

Fase 2: Creare un elenco di IP statici Anycast

Prima di iniziare, richiedi un elenco di IP statici anycast come spiegato nella sezione precedente.

Come creare un elenco di IP statici anycast

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione a sinistra, scegli Statico IPs.
3. Scegli Crea elenco di IP anycast.
4. In Nome, immetti un nome.
5. Per i casi d'uso di IP statico, seleziona BYOIP come caso d'uso.

I passaggi seguenti differiscono dal processo BYOIP regionale standard e stabiliscono il modello per i servizi globali:

AWS CLI

Installazione o aggiornamento alla versione più recente della AWS CLI. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface.

1. Recupera il IpamPoolArn pool IPAM in cui sono stati forniti i blocchi CIDR. Per ulteriori informazioni, consulta Portare il proprio IPv4 CIDR pubblico su IPAM utilizzando solo la CLI AWS.
2. Crea un elenco di IP Anycast con i tuoi blocchi CIDR e la configurazione IPAM:

```
aws cloudfront create-anycast-ip-list \
    --name byoip-aip-1 \
    --ip-count 3 \
    --region us-east-1 \
    --ip-address-type ipv4 \
    --ipam-cidr-configs
 '[{"Cidr":"1.1.1.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"2.2.2.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"3.3.3.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"}]'
```

> **Note**
>
> Non è possibile selezionare l'indirizzo IP specifico dal pool. CloudFront lo farà automaticamente.

Fase 3: Creare una CloudFront distribuzione

Infatti CloudFront, puoi seguire le istruzioni per creare una distribuzione standard o utilizzare distribuzioni multi-tenant.

Fase 4: Associarsi alle risorse CloudFront

- Associa un elenco di IP statici Anycast a una distribuzione esistente
- Associa un elenco IP statico Anycast a una nuova distribuzione
- Associa un elenco IP statico Anycast a un gruppo di connessioni

Fase 5: Prepararsi alla migrazione

Per ulteriori informazioni, consulta la Fase 4: Preparazione alla migrazione nella Amazon VPC User Guide.

Passaggio 6: pubblicizza CIDR a livello globale

Per ulteriori informazioni, consulta la Fase 5: Pubblicizzare CIDR a livello globale nella Amazon VPC User Guide.

Usare gRPC con le distribuzioni CloudFront

Amazon CloudFront supporta gRPC, un framework RPC (Remote Procedure Call) open source basato su HTTP/2. gRPC offre streaming bidirezionale e protocollo binario che bufferizza i payload, rendendolo adatto per applicazioni che richiedono comunicazioni a bassa latenza.

CloudFront riceve le tue richieste gRPC e le invia direttamente alle tue origini. È possibile utilizzare CloudFront per eseguire il proxy di quattro tipi di servizi gRPC:

- RPC unario
- Streaming del server RPC
- Streaming del client RPC
- Streaming bidirezionale RPC

Come funziona gRPC in CloudFront

Per configurare gRPC in CloudFront, imposta un'origine che fornisca un servizio gRPC come origine della distribuzione. È possibile utilizzare origini che forniscono servizi non gRPC e gRPC. CloudFront determina se la richiesta in arrivo è una richiesta gRPC o una richiesta HTTP/HTTPS in base all'intestazione. `Content-Type` Se l'`Content-Type`intestazione di una richiesta ha il valore di`application/grpc`, la richiesta viene considerata una richiesta gRPC CloudFront e invierà la richiesta come proxy alla tua origine.

> **Note**
>
> Per consentire a una distribuzione di gestire le richieste gRPC, includi HTTP/2 come una delle versioni HTTP supportate e consenti i metodi HTTP, incluso `POST`. L'endpoint di origine gRPC deve essere configurato per supportare HTTPS, poiché supporta CloudFront solo

connessioni gRPC sicure (basate su HTTPS). gRPC supporta solo HTTPS. end-to-end Se utilizzi un'origine personalizzata, verifica che le impostazioni Protocollo supportino HTTPS.

Per abilitare il supporto gRPC per la distribuzione, completa le seguenti fasi:

1. Aggiorna il comportamento cache della distribuzione per consentire i metodi HTTP, incluso il metodo `POST`.
2. Dopo aver selezionato il metodo `POST`, seleziona la casella di controllo gRPC che viene visualizzata.
3. Specifica HTTP/2 come una delle versioni HTTP supportate.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Consentire richieste gRPC su HTTP/2
- GrpcConfignell'Amazon CloudFront API Reference

Poiché gRPC è utilizzato solo per traffico API non memorizzabile nella cache, le configurazioni della cache non influiranno sulle richieste gRPC. Puoi usare una policy di richiesta di origine per aggiungere intestazioni personalizzate alle richieste gRPC inviate alla all'origine gRPC. È possibile utilizzare AWS WAF with CloudFront per gestire l'accesso alla distribuzione gRPC, controllare i bot e proteggere le applicazioni gRPC dagli exploit web. CloudFront gRPC supporta CloudFront le funzioni.

Oltre allo stato HTTPS, riceverai grpc-status insieme alla risposta gRPC. Per un elenco dei valori possibili per grpc-status, consulta Codici di stato e loro utilizzo in gRPC.

Note

gRPC non supporta le seguenti funzionalità: CloudFront

- Risposte di errore personalizzate
- Il failover di Origin non è supportato con gRPC, poiché gRPC utilizza il metodo. `POST` CloudFront esegue il failover sull'origine secondaria solo quando il metodo HTTP della richiesta del visualizzatore è`GET`, `HEAD` o. `OPTIONS`
- CloudFront invia le richieste gRPC direttamente all'origine e ignora la Regional Edge Cache (REC). Poiché gRPC aggira il REC, gRPC non supporta Lambda@Edge o Origin Shield.

- gRPC non supporta le regole di ispezione dell'organismo AWS WAF su richiesta. Se hai abilitato queste regole sull'ACL Web per una distribuzione, qualsiasi richiesta che utilizza gRPC ignorerà le regole di ispezione del corpo della richiesta. Tutte le altre regole AWS WAF continueranno ad essere applicate. Per ulteriori informazioni, consulta Abilitazione di AWS WAF per le distribuzioni.

Utilizzo di risorse condivise in CloudFront

Amazon CloudFront si integra con AWS Resource Access Manager (AWS RAM) per consentire la condivisione delle risorse. AWS RAM ti consente di condividere alcune CloudFront risorse con altri Account AWS o tramite AWS Organizations. Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori includono:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Questo argomento spiega come condividere le risorse che possiedi e come utilizzare le risorse condivise con te.

Indice

Prerequisiti per la condivisione delle risorse

- È necessario disporre della politica AWSRAMDefaultPermissionCloudFront gestita per concedere l'accesso in sola lettura alla condivisione delle risorse. Per ulteriori informazioni, consulta AWSRAMDefaultPermissionCloudFront.

- Per condividere un'origine VPC, devi possederla nel tuo. Account AWS Ciò significa che la risorsa deve essere allocata o fornita nel tuo account. Non puoi condividere una risorsa che è stata condivisa con te.
- Per condividere una risorsa con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Condivisione di un'origine VPC

> **Note**
>
> Attualmente, CloudFront supporta la condivisione delle origini VPC. Se non ne hai già creato uno, vediLimitazione dell'accesso con VPC Origins.

Quando condividi un'origine VPC di tua proprietà con altri Account AWS, consenti loro di utilizzare quella risorsa come origine per le loro CloudFront distribuzioni.

Per condividere un'origine VPC, è necessario aggiungerla a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che consente di condividere le risorse tra Account AWS.

Una condivisione di risorse specifica quanto segue:

- Le risorse che desideri condividere
- I consumatori con cui vengono condivise
- La politica gestita del servizio che determina le autorizzazioni per le risorse

Quando condividi un'origine VPC utilizzando la CloudFront console, la aggiungi a una condivisione di risorse esistente. Se non disponi già di una condivisione di risorse, puoi crearne una quando condividi un'origine VPC dalla CloudFront console. Puoi anche utilizzare la AWS RAM console o AWS CLI crearne una separatamente.

Puoi condividere le origini del VPC con altri Account AWS e. AWS Organizations

- Se condividi la risorsa con un' AWS organizzazione, a tutti i consumatori di quella specifica organizzazione è consentito l'accesso all'origine del VPC.

- Se condividi con un'organizzazione Account AWS o con un'organizzazione di cui non fai parte, i consumatori riceveranno un invito ad accettare la condivisione delle risorse. Una volta accettati, possono utilizzare l'origine VPC.

Puoi condividere un'origine VPC di tua proprietà utilizzando la CloudFront console, la AWS RAM console o il. AWS CLI

Per creare una condivisione di risorse utilizzando la console CloudFront

1. Aprire la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Origini VPC.
3. Seleziona una o più risorse e scegli Condividi origine VPC.
4. Seleziona Crea condivisione risorse.
5. In Nome, inserisci un nome per la condivisione di risorse.
6. Per Tipo principale, selezionare una delle seguenti opzioni:

   - Account AWS— Concedi l'accesso a uno specifico Account AWS.
   - Unità organizzativa: concede l'accesso a un'unità organizzativa (OU) specifica.
   - Organizzazione: concedi l'accesso all'intera organizzazione, compresi i suoi figli OUs e Account AWS.

   a. Se hai scelto Account AWS, inserisci il numero ID dell'account. Puoi scegliere Aggiungi nuovo account per aggiungerne fino a 5 Account AWS.
   b. Se hai scelto Unità organizzativa, inserisci l'ARN dell'unità organizzativa. È possibile inserire solo 1 unità organizzativa.
   c. Se hai scelto Organizzazione, inserisci l'ARN dell'organizzazione. Puoi inserire solo 1 organizzazione.
7. Scegli Condividi risorse.

   Per impostazione predefinita, CloudFront applica la politica AWSRAMDefaultPermissionCloudFront AWS gestita alla condivisione delle risorse. Questa politica consente azioni di sola lettura sulla condivisione di risorse, in modo che gli account utente non possano aggiornare o eliminare la risorsa condivisa. Non puoi modificare o rimuovere questa politica dalla condivisione delle risorse.

> **Tip**
>
> Dopo aver creato la condivisione di risorse, puoi aggiungerne altre Account AWS dalla AWS RAM console. Per ulteriori informazioni, consulta Aggiornare una condivisione di risorse nella AWS RAM nella Guida AWS RAM per l'utente.

Per condividere un'origine VPC di tua proprietà utilizzando la console CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Origini VPC.
3. Seleziona una risorsa e scegli Condividi origine VPC.
4. Nella pagina Condividi origine VPC, puoi selezionare una condivisione di risorse esistente a cui desideri aggiungere questa origine VPC.
5. Scegli Condividi risorsa.

   Nella pagina dei dettagli della risorsa, in Condiviso con, puoi vedere che l'origine del tuo VPC è condivisa con i seguenti dettagli:

   - Nomi di condivisione delle risorse
   - Condividi lo stato
   - Data dell'ultima modifica

Dopo aver creato e condiviso la condivisione di risorse con gli account consumatori, questi hanno 12 ore di tempo per accettare l'invito. Per ulteriori informazioni, consulta Accettazione e rifiuto degli inviti alla condivisione di risorse nella Guida per l'AWS RAM utente.

> **Important**
>
> Per consentire agli account utente di utilizzare la tua origine VPC per la loro CloudFront distribuzione, devi anche fornire loro l'endpoint ELB o Amazon dell'origine VPC. EC2

Per condividere un'origine VPC di tua proprietà utilizzando la console AWS RAM

Crea una condivisione di risorse e poi scegli le CloudFront risorse che desideri aggiungervi. Per ulteriori informazioni, consulta Creazione di una condivisione di risorse nella Guida AWS RAM per l'utente.

Per condividere un'origine VPC di tua proprietà utilizzando AWS CLI

Utilizza il comando create-resource-share.

Utilizzo di un'origine VPC condivisa

Per utilizzare un'origine VPC condivisa, l'account che riceve l'invito deve accettare la condivisione di risorse. Puoi farlo accedendo alla AWS Resource Access Manager console nella regione Stati Uniti orientali (Virginia settentrionale) e accettando eventuali richieste in sospeso nella scheda In sospeso. Per ulteriori informazioni, consulta Accettazione di risorse condivise nella Guida per l'utente.AWS RAM

Dopo aver accettato la condivisione di risorse, puoi utilizzare l'origine VPC come origine per le tue CloudFront distribuzioni.

Per utilizzare un'origine VPC condivisa

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, per Distribuzioni, esegui una delle seguenti operazioni:
   - Per una nuova distribuzione, scegli Crea distribuzione.
   - Per una distribuzione esistente, scegli l'ID di distribuzione.
3. Per il tipo di origine, scegli Origine VPC, quindi specifica l'origine VPC che è stata condivisa con te.
4. Per l'endpoint di origine VPC, inserisci il nome DNS privato dell' EC2 istanza Amazon o del load balancer ELB o il dominio di origine. Se non disponi già di questo valore, devi ottenerlo da chi possiede Account AWS l'origine del VPC. Se non disponi già di questo endpoint, puoi ottenerlo da chi possiede Account AWS l'origine del VPC.
5. Segui gli altri passaggi della console per creare o aggiornare la tua distribuzione.

Identificazione di un'origine VPC condivisa

I proprietari e i consumatori possono identificare le origini VPC condivise utilizzando la CloudFront console e. AWS CLI

Per identificare un'origine VPC condivisa utilizzando la console CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Origini VPC. Puoi utilizzare la colonna Owner ID per identificare a Account AWS chi appartiene la risorsa.
3. Selezionare una risorsa.
4. Nella pagina dei dettagli della risorsa, in Condiviso con, puoi vedere che l'origine del tuo VPC è condivisa con i seguenti dettagli:
   - Nomi di condivisione delle risorse
   - Condividi lo stato
   - Data dell'ultima modifica

Annullamento della condivisione di un'origine VPC condivisa

Quando annulli la condivisione di una risorsa, gli Account AWS (account di consumo) non possono più utilizzare quella risorsa per nuove distribuzioni o aggiornare le distribuzioni esistenti.

> **Note**
>
> Se annulli la condivisione di una risorsa, le distribuzioni esistenti che utilizzano ancora quella risorsa rimangono attive e continueranno a servire il traffico. Tuttavia, queste distribuzioni non possono essere modificate finché la risorsa non condivisa non viene rimossa come origine. Ti consigliamo di assicurarti che tutti gli account consumatori smettano di utilizzare la risorsa non condivisa prima di annullarne la condivisione.

Per annullare la condivisione di un'origine VPC condivisa di tua proprietà, devi rimuoverla dalla condivisione di risorse. Puoi farlo utilizzando la CloudFront console, AWS RAM la console o il. AWS CLI

Per annullare la condivisione di un'origine VPC condivisa di tua proprietà utilizzando la console CloudFront

1. Apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Nel riquadro di navigazione, scegli Origini VPC.

3. Seleziona una risorsa e scegli Annulla condivisione.
4. Controlla i dettagli nella finestra di dialogo Annulla condivisione della risorsa, quindi scegli Annulla condivisione. I principali elencati non avranno più accesso alla tua risorsa condivisa.

Per annullare la condivisione di un'origine VPC condivisa di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per annullare la condivisione di un'origine VPC condivisa di tua proprietà, utilizza AWS CLI

Utilizza il comando disassociate-resource-share.

Responsabilità e autorizzazioni per le origini VPC condivise

Autorizzazioni per i proprietari

In qualità di account proprietario della risorsa, assicurati che tutti gli account consumatori smettano di utilizzare la risorsa prima di annullarne la condivisione o eliminarla.

Autorizzazioni per gli utenti

Gli account che utilizzano possono utilizzare risorse condivise come origini per le proprie CloudFront distribuzioni, ma non possono modificare o eliminare le risorse. Per impostazione predefinita, la politica AWSRAMDefaultPermissionCloudFront AWS gestita viene applicata alla condivisione di risorse nell'account di condivisione (l'account proprietario della risorsa).

AWSRAMDefaultPermissionCloudFront

Quando si crea una condivisione di risorse in CloudFront, CloudFront utilizza la politica AWSRAMDefaultPermissionCloudFront AWS gestita e la applica alla condivisione di risorse. Questa politica concede autorizzazioni di sola lettura alle CloudFront risorse che possono essere condivise dal proprietario della risorsa all'account utente.

Per ulteriori informazioni sulla gestione delle autorizzazioni in AWS RAM, vedere Gestione delle autorizzazioni nella Guida per l'utente. AWS RAMAWS Resource Access Manager

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione delle origini VPC con altri. Account AWS I costi di utilizzo del traffico per una distribuzione che utilizza un'origine VPC condivisa andranno all'account utente proprietario della distribuzione.

Quote di risorse condivise

CloudFront utilizza le stesse quote di condivisione delle risorse specificate da. AWS RAM Dalla CloudFront console è possibile aggiungere fino a 5 Account AWS, 1 unità organizzativa o 1 organizzazione. Per aggiungerne altre, usa la AWS RAM console o l' AWS RAM API.

Per maggiori informazioni, consulta Service Quotas di AWS RAM nella Guida per l'utente di AWS RAM .

Caching e disponibilità

Puoi utilizzare CloudFront per ridurre il numero di richieste a cui il server di origine deve rispondere direttamente. Con il caching CloudFront, più oggetti vengono serviti dalle edge location CloudFront, che sono più vicine agli utenti. Questo riduce il carico e la latenza sul server di origine.

Maggiore è il numero di richieste che CloudFront può servire dalle cache edge, minori sono le richieste del visualizzatore che CloudFront deve inoltrare all'origine per ottenere l'ultima versione o una versione univoca di un oggetto. Per ottimizzare CloudFront per effettuare il minor numero possibile di richieste alla tua origine, considera l'utilizzo di Origin Shield di CloudFront. Per ulteriori informazioni, consulta Usa Amazon CloudFront Origin Shield.

La proporzione di richieste che vengono servite direttamente dalla cache CloudFront rispetto a tutte le richieste è chiamata percentuale di riscontri nella cache. Nella console CloudFront è possibile visualizzare la percentuale di richieste dei visualizzatori che sono hit, errori e mancanze. Per ulteriori informazioni, consulta Visualizzazione dei report sulle statistiche della cache di CloudFront.

La percentuale di riscontri nella cache è influenzata da diversi fattori. Puoi modificare la configurazione di distribuzione CloudFront per migliorare la percentuale di riscontri nella cache seguendo le indicazioni in Aumento della percentuale di richieste eseguite direttamente dalle cache CloudFront (percentuale di riscontri nella cache).

Per ulteriori informazioni sull'aggiunta e la rimozione di contenuti che desideri vengano serviti da CloudFront, consulta Aggiunta, rimozione o sostituzione di contenuti distribuiti da CloudFront.

Argomenti

Aumento della percentuale di richieste eseguite direttamente dalle cache CloudFront (percentuale di riscontri nella cache)

È possibile migliorare le prestazioni aumentando la percentuale di richieste dei visualizzatori che vengono servite direttamente dalla cache CloudFront anziché rivolgersi ai server di origine per i contenuti. Questo è noto come miglioramento del tasso di occorrenza nella cache.

Le seguenti sezioni illustrano come migliorare il tuo numero di riscontri nella cache.

Argomenti

Specifica della durata di tempo in cui CloudFront memorizza nella cache gli oggetti

Per incrementare il numero di riscontri nella cache, puoi configurare il server di origine per aggiungere una direttiva Cache-Control max-age ai tuoi oggetti e specificare il valore pratico più lungo per `max-age`. Più breve è la durata cache, più frequentemente CloudFront invia le richieste all'origine per determinare se un oggetto è stato modificato e per ottenere la versione più recente. È possibile integrare `max-age` con le direttive `stale-while-revalidate` e `stale-if-error` per migliorare ulteriormente il rapporto di occorrenza nella cache in determinate condizioni. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Utilizzo di Origin Shield

Origin Shield di CloudFront può contribuire a migliorare la percentuale di riscontri nella cache della distribuzione CloudFront, poiché fornisce un ulteriore livello di caching davanti all'origine. Quando usi Origin Shield, tutte le richieste provenienti da tutti i livelli di caching di CloudFront all'origine provengono da un'unica posizione. CloudFront può recuperare ogni oggetto utilizzando una singola

richiesta origine da Origin Shield e tutti gli altri livelli della cache CloudFront (posizioni edge e cache edge regionali) possono recuperare l'oggetto da Origin Shield.

Per ulteriori informazioni, consulta Usa Amazon CloudFront Origin Shield.

Caching Basato su parametri della stringa di query

Se si configura CloudFront per la memorizzazione nella cache in base ai parametri delle stringhe di query, è possibile migliorare la memorizzazione nella cache se si eseguono le seguenti operazioni:

- Configura CloudFront per inoltrare solo i parametri della stringa di query per i quali l'origine restituirà oggetti univoci.
- Utilizza la stessa combinazione di maiuscole e minuscole per tutte le istanze dello stesso parametro. Ad esempio, se una richiesta contiene `parameter1=A` e un'altra contiene `parameter1=a`, CloudFront inoltra richieste separate all'origine quando una richiesta contiene `parameter1=A` e quando una richiesta contiene `parameter1=a`. CloudFront quindi memorizza separatamente nella cache gli oggetti corrispondenti restituiti dall'origine separatamente anche se gli oggetti sono identici. Se utilizzi solo `A` o `a`, CloudFront inoltra un numero minore di richieste al server di origine.
- Elenca i parametri nello stesso ordine. Come per le differenze tra maiuscola e minuscola, se una richiesta per un oggetto contiene la stringa di query `parameter1=a&parameter2=b` e un'altra richiesta per lo stesso oggetto contiene `parameter2=b&parameter1=a`, CloudFront inoltra entrambe le richieste al server di origine e memorizza nella cache gli oggetti separatamente anche se sono identici. Se utilizzi sempre lo stesso ordine per i parametri, CloudFront inoltra un numero minore di richieste al server di origine.

Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query. Se desideri esaminare le stringhe di query che CloudFront inoltra all'origine, esamina i valori nella colonna `cs-uri-query` dei file di log CloudFront. Per ulteriori informazioni, consulta Registri di accesso (registri standard).

Caching in base ai valori dei cookie

Se configuri CloudFront per la memorizzazione nella cache in base ai valori dei cookie, puoi migliorare il caching nel seguente modo:

- Configura CloudFront per inoltrare solo i cookie specificati invece di inoltrare tutti i cookie. Per i cookie configurati per l'inoltro all'origine da parte di CloudFront, CloudFront inoltra tutte le

combinazioni di nome e valore dei cookie. Quindi memorizza nella cache separatamente gli oggetti restituiti dall'origine, anche se sono tutti identici.

Ad esempio, supponiamo che i visualizzatori includano due cookie in ogni richiesta, che ogni cookie abbia a disposizione tre valori possibili e che siano possibili tutte le combinazioni dei valori dei cookie. CloudFront inoltra fino a nove diverse richieste al server di origine per ogni oggetto. Se il server di origine restituisce versioni differenti di un oggetto in base a uno solo dei cookie, allora CloudFront inoltra più richieste al server di origine del necessario e memorizza inutilmente nella cache più versioni identiche dell'oggetto.

- Crea comportamenti cache separati per i contenuti statici e dinamici e configura CloudFront in modo che inoltri i cookie al tuo server di origine solo per i contenuti dinamici.

  Ad esempio, supponiamo che tu disponga di un solo comportamento cache per la tua distribuzione e che tu stia utilizzando la distribuzione sia per i contenuti dinamici, ad esempio i file `.js`, sia per i file `.css` che cambiano raramente. CloudFront memorizza nella cache le versioni separate dei file `.css` in base ai valori dei cookie, perciò ogni edge location CloudFront inoltra una richiesta al server di origine per ogni nuovo valore di cookie o combinazione di valori di cookie.

  Se crei un comportamento cache per il quale il modello di percorso è `*.css` e per il quale CloudFront non esegue la memorizzazione nella cache in base ai valori dei cookie, CloudFront inoltra le richieste per i file `.css` all'origine solo per la prima richiesta che una posizione edge riceve per un determinato file `.css` e per la prima richiesta dopo la scadenza di un file `.css`.
- Se possibile, crea comportamenti cache separati per i contenuti dinamici per cui i valori dei cookie sono univoci per ogni utente (ad esempio un ID utente) e per contenuti dinamici che variano in base a un numero minore di valori univoci.

Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie. Se desideri esaminare i cookie che CloudFront inoltra all'origine, esamina il valori nella colonna `cs(Cookie)` dei file di log CloudFront. Per ulteriori informazioni, consulta Registri di accesso (registri standard).

Caching in base alle intestazioni di richiesta

Se configuri CloudFront per la memorizzazione nella cache in base alle intestazioni di richiesta, puoi migliorare il caching nel seguente modo:

- Configura CloudFront per inoltrare e memorizzare nella cache solo le intestazioni specificate invece di inoltrare e memorizzare nella cache tutte le intestazioni. Per le intestazioni specificate,

CloudFront inoltra ogni combinazione di nome e di valore di intestazione. Quindi memorizza nella cache separatamente gli oggetti restituiti dall'origine, anche se sono tutti identici.

> **Note**
>
> CloudFront inoltra sempre al server di origine le intestazioni specificate nei seguenti argomenti:
>
> - Come CloudFront elabora e inoltra le richieste al server di origine Amazon S3 > Intestazioni di richiesta HTTP che rimuovono o aggiornano CloudFront
> - Come CloudFront elabora e inoltra le richieste al server di origine personalizzato > Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

Quando configuri CloudFront per la memorizzazione nella cache in base alle intestazioni di richiesta, non modifichi le intestazioni che CloudFront inoltra, solo se CloudFront memorizza nella cache gli oggetti in base ai valori dell'intestazione.

- Prova a evitare la memorizzazione nella cache in base alle intestazioni delle richieste che dispongono di un numero elevato di valori univoci.

  Ad esempio, se desideri servire diversi formati di un'immagine in base al dispositivo dell'utente, non configurare CloudFront per la memorizzazione nella cache in base all'intestazione `User-Agent` che ha un numero enorme di valori possibili. Configurare invece CloudFront per la cache in base alle intestazioni di tipo dispositivo CloudFront `CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer` e `CloudFront-Is-Tablet-Viewer`. Inoltre, se restituisci la stessa versione dell'immagine per tablet e computer desktop, allora inoltra solo l'intestazione `CloudFront-Is-Tablet-Viewer` e non l'intestazione `CloudFront-Is-Desktop-Viewer`.

Per ulteriori informazioni, consulta Caching dei contenuti in base alle intestazioni di richiesta.

Rimuovere l'intestazione **`Accept-Encoding`** quando la compressione non è necessaria

Se la compressione non è abilitata perché l'origine non la supporta, CloudFront non la supporta o il contenuto non è comprimibile, puoi aumentare l'indice di occorrenze nella cache associando un

comportamento della cache nella distribuzione a un'origine che imposta Custom Origin Header come segue:

- Nome intestazione: `Accept-Encoding`
- Header value (Valore intestazione): (Lasciare vuoto)

Quando si utilizza questa configurazione, CloudFront rimuove l'intestazione `Accept-Encoding` dalla chiave cache e non include l'intestazione nelle richieste di origine. Questa configurazione si applica a tutti i contenuti forniti da CloudFront con la distribuzione da tale origine.

Distribuire contenuti multimediali tramite HTTP

Per ulteriori informazioni su come ottimizzare i contenuti video on demand (VOD) e in streaming, consulta Video on demand e video in streaming live con CloudFront.

Usa Amazon CloudFront Origin Shield

CloudFront Origin Shield è un livello aggiuntivo dell'infrastruttura di CloudFront caching che aiuta a ridurre al minimo il carico dell'origine, a migliorarne la disponibilità e a ridurne i costi operativi. Con lo scudo di origine CloudFront ottieni i seguenti vantaggi:

Miglior rapporto di occorrenza nella cache

Origin Shield può aiutarti a migliorare il rapporto di accesso alla cache della tua CloudFront distribuzione perché fornisce un ulteriore livello di caching davanti all'origine. Quando usi Origin Shield, tutte le richieste provenienti da tutti i livelli CloudFront di caching alla tua origine passano attraverso Origin Shield, aumentando la probabilità che si verifichi un errore nella cache. CloudFrontpuoi recuperare ogni oggetto con una singola richiesta di origine da Origin Shield all'origine e tutti gli altri livelli della CloudFront cache (edge location e cache edge regionali) possono recuperare l'oggetto da Origin Shield.

Carico di origine ridotto

Origin Shield può ridurre ulteriormente il numero di richieste simultanee inviate all'origine per lo stesso oggetto. Le richieste di contenuto che non si trova nella cache dello scudo di origine vengono consolidate con altre richieste per lo stesso oggetto, con il risultato che solo una richiesta va alla tua origine. La gestione di un minor numero di richieste all'origine può preservare la disponibilità dell'origine durante i picchi di carico o i picchi di traffico imprevisti e può ridurre i

costi per attività come la creazione di just-in-time pacchetti, le trasformazioni delle immagini e il trasferimento dei dati (DTO).

Migliori prestazioni di rete

Quando attivi Origin Shield nella AWS regione con la latenza più bassa rispetto all'origine, puoi ottenere prestazioni di rete migliori. Per le origini in una AWS regione, il traffico di CloudFront rete rimane sulla CloudFront rete ad alto throughput fino all'origine. Per le origini esterne AWS, il traffico di CloudFront rete rimane sulla CloudFront rete fino a Origin Shield, che ha una connessione a bassa latenza con la tua origine.

Incorrono costi aggiuntivi per l'utilizzo di Origin Shield. Per ulteriori informazioni, consultare Prezzi di CloudFront .

> **Note**
>
> Origin Shield non è supportato con le richieste gRPC. Se Origin Shield è abilitato in una distribuzione che supporta gRPC, le richieste gRPC continueranno a funzionare. Tuttavia, le richieste saranno inoltrate direttamente all'origine gRPC senza passare attraverso Origin Shield. Per ulteriori informazioni, consulta Usare gRPC con le distribuzioni CloudFront .

Argomenti

Casi d'uso per Origin Shield

CloudFront Origin Shield può essere utile per molti casi d'uso, inclusi i seguenti:

- Visualizzatori che sono distribuiti in diverse regioni geografiche
- Origins che forniscono just-in-time imballaggi per lo streaming live o on-the-fly l'elaborazione di immagini

- Origini locali con vincoli di capacità o larghezza di banda
- Carichi di lavoro che utilizzano più reti di distribuzione dei contenuti () CDNs

Origin Shield potrebbe non essere adatto in altri casi, ad esempio un contenuto dinamico che viene inoltrato tramite proxy all'origine, un contenuto con scarsa memorizzazione nella cache o un contenuto richiesto raramente.

Le sezioni seguenti illustrano i vantaggi di Origin Shield per i seguenti casi d'uso.

Casi d'uso

- Visualizzatori in diverse regioni geografiche
- Molteplici CDNs

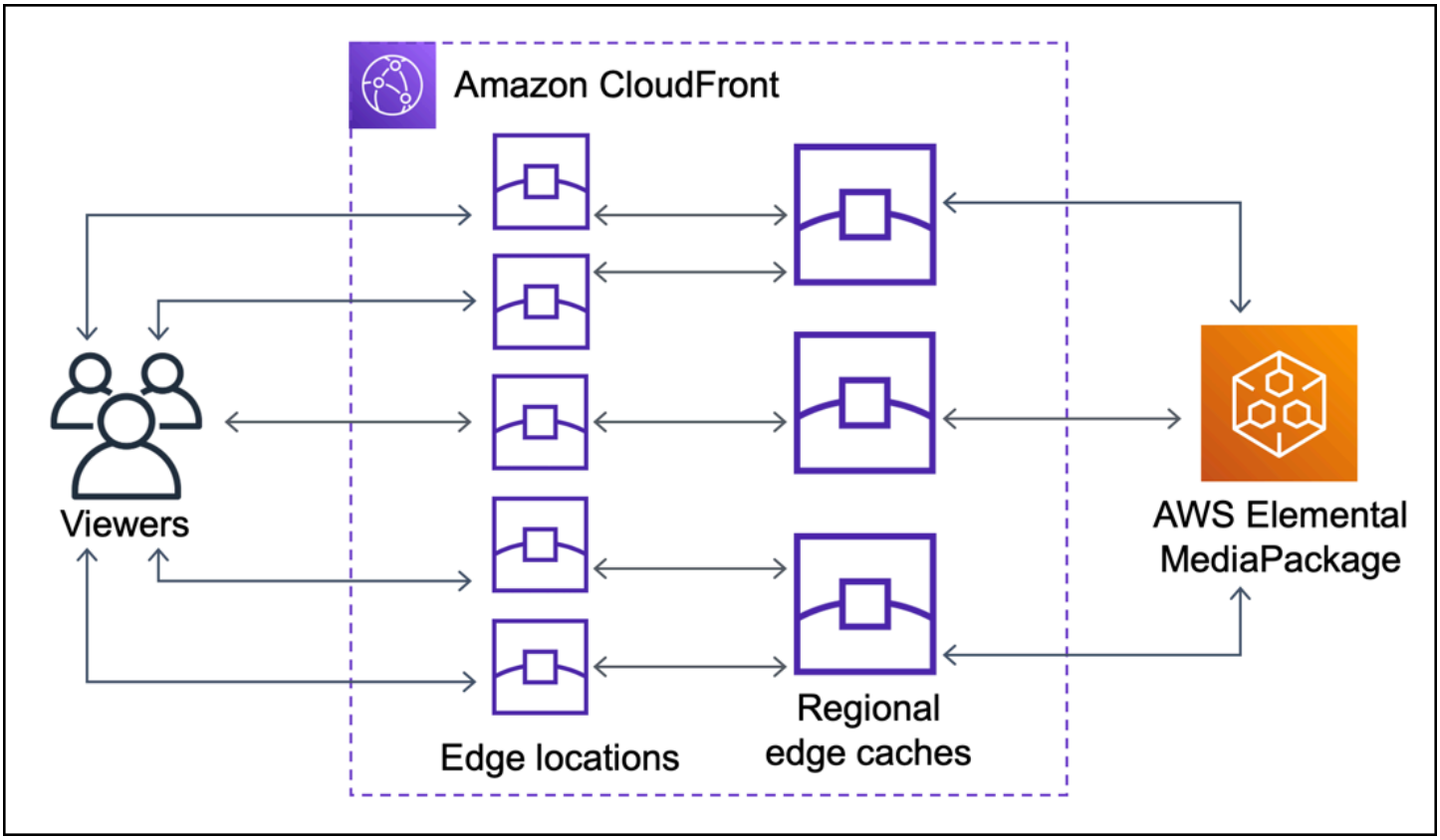
Visualizzatori in diverse regioni geografiche

Con Amazon CloudFront, ottieni intrinsecamente un carico ridotto sulla tua origine perché le richieste che CloudFront possono essere inviate dalla cache non arrivano alla tua origine. Oltre alla rete globale CloudFront di edge location, le cache edge regionali fungono da livello di caching di livello intermedio per fornire accessi alla cache e consolidare le richieste di origine per gli spettatori nelle aree geografiche vicine. Le richieste del visualizzatore vengono instradate prima a una edge location CloudFront vicina e, se l'oggetto non è memorizzato nella cache in tale posizione, la richiesta viene inviata a una cache edge regionale.

Quando i visualizzatori si trovano in regioni geografiche diverse, le richieste possono essere instradate attraverso cache edge diverse, ognuna delle quali può inviare una richiesta all'origine per lo stesso contenuto. Ma con Origin Shield, ottieni un ulteriore livello di memorizzazione nella cache tra le cache edge regionali e la tua origine. Tutte le richieste provenienti da tutte le cache edge regionali passano attraverso Origin Shield, riducendo ulteriormente il carico sulla tua origine. I seguenti diagrammi illustrano tutto questo. Nei seguenti diagrammi, l'origine è AWS Elemental MediaPackage.

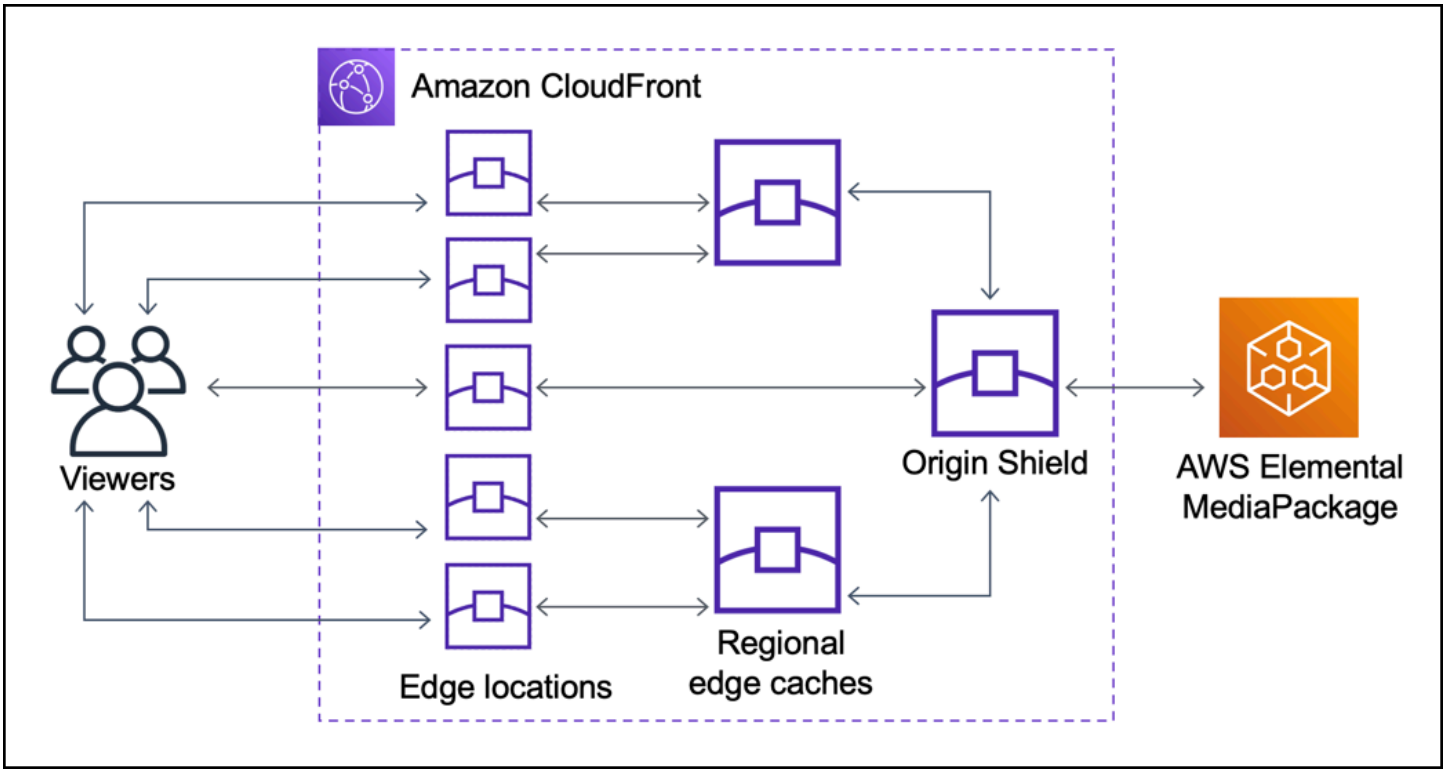
Senza scudo di origine

Senza Origin Shield, l'origine potrebbe ricevere richieste duplicate per lo stesso contenuto, come illustrato nel diagramma seguente.



Con lo scudo di origine

L'utilizzo di Origin Shield consente di ridurre il carico sull'origine, come illustrato nel diagramma seguente.



Molteplici CDNs

Per offrire eventi video in diretta o contenuti on-demand popolari, puoi utilizzare più reti di distribuzione dei contenuti (CDNs). L'utilizzo di più contenuti CDNs può offrire alcuni vantaggi, ma significa anche che l'origine potrebbe ricevere molte richieste duplicate per lo stesso contenuto, ognuna proveniente da posizioni diverse CDNs o diverse all'interno dello stesso CDN. Queste richieste ridondanti potrebbero influire negativamente sulla disponibilità dell'origine o causare costi operativi aggiuntivi per processi come l' just-in-timeimballaggio o il trasferimento dei dati (DTO) su Internet.

Combinando Origin Shield con l'utilizzo della tua CloudFront distribuzione come origine per altri CDNs, puoi ottenere i seguenti vantaggi:

- Meno richieste ridondanti ricevute all'origine, il che aiuta a ridurre gli effetti negativi dell'utilizzo di più richieste. CDNs
- Una chiave di cache comune e una gestione centralizzata delle funzionalità rivolte all'origine. CDNs
- Prestazioni di rete migliorate. Il traffico di rete proveniente da altri utenti CDNs viene interrotto presso una CloudFront edge location vicina, il che potrebbe causare un impatto dalla cache locale. Se l'oggetto richiesto non si trova nella cache dell'edge location, la richiesta all'origine rimane sulla CloudFront rete fino a Origin Shield, che fornisce un throughput elevato e una bassa latenza

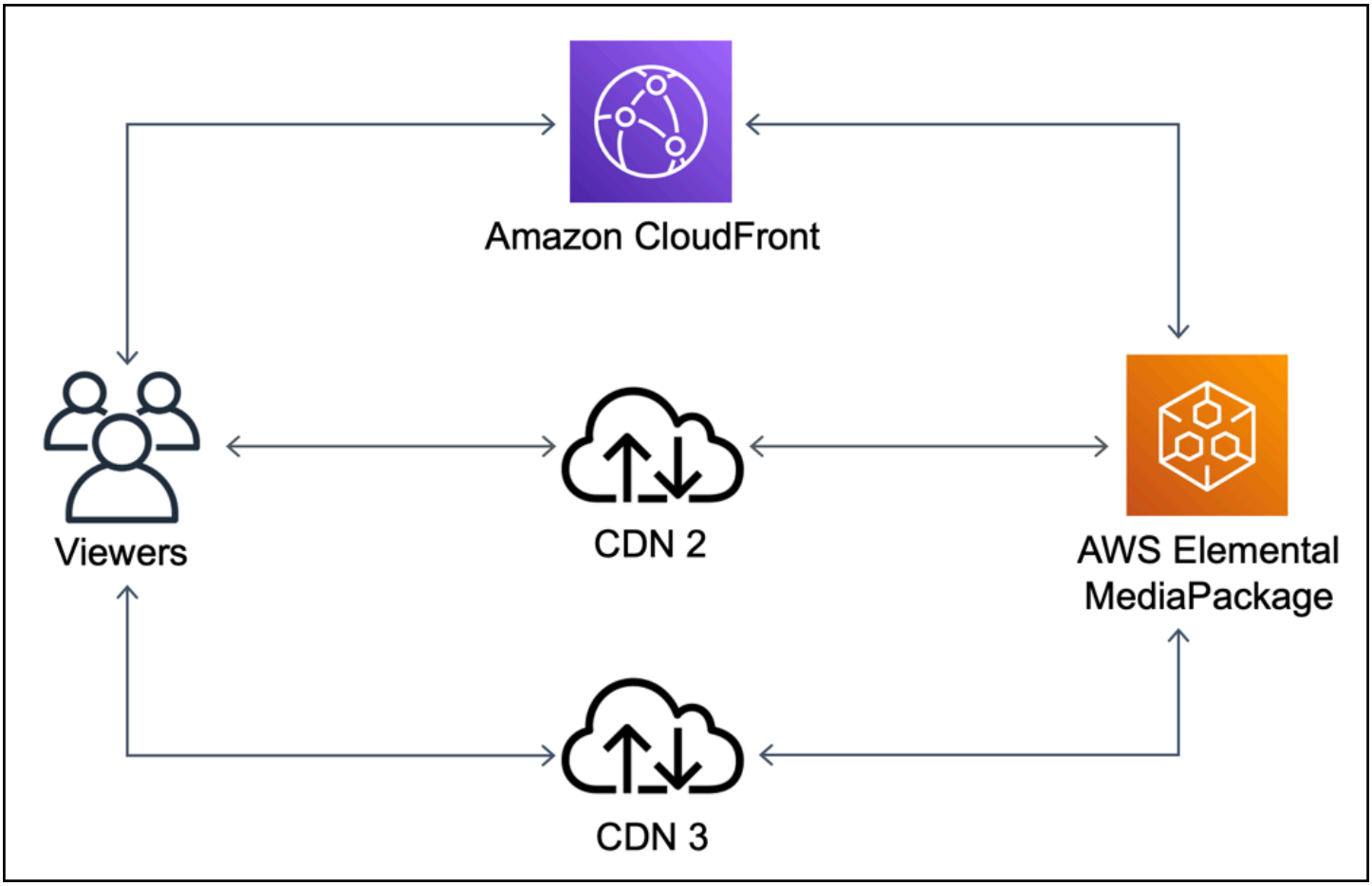
all'origine. Se l'oggetto richiesto si trova nella cache dello scudo di origine, la richiesta all'origine viene evitata completamente.

> **Important**
>
> Se sei interessato a utilizzare Origin Shield in un'architettura multi-CDN e hai prezzi scontati, contatta noi o il tuo rappresentante di AWS vendita per ulteriori informazioni. Potrebbero essere applicati costi aggiuntivi.

I seguenti diagrammi mostrano in che modo questa configurazione può aiutare a ridurre al minimo il carico sull'origine quando si organizzano eventi video live popolari con più eventi. CDNs Nei diagrammi seguenti, l'origine è. AWS Elemental MediaPackage

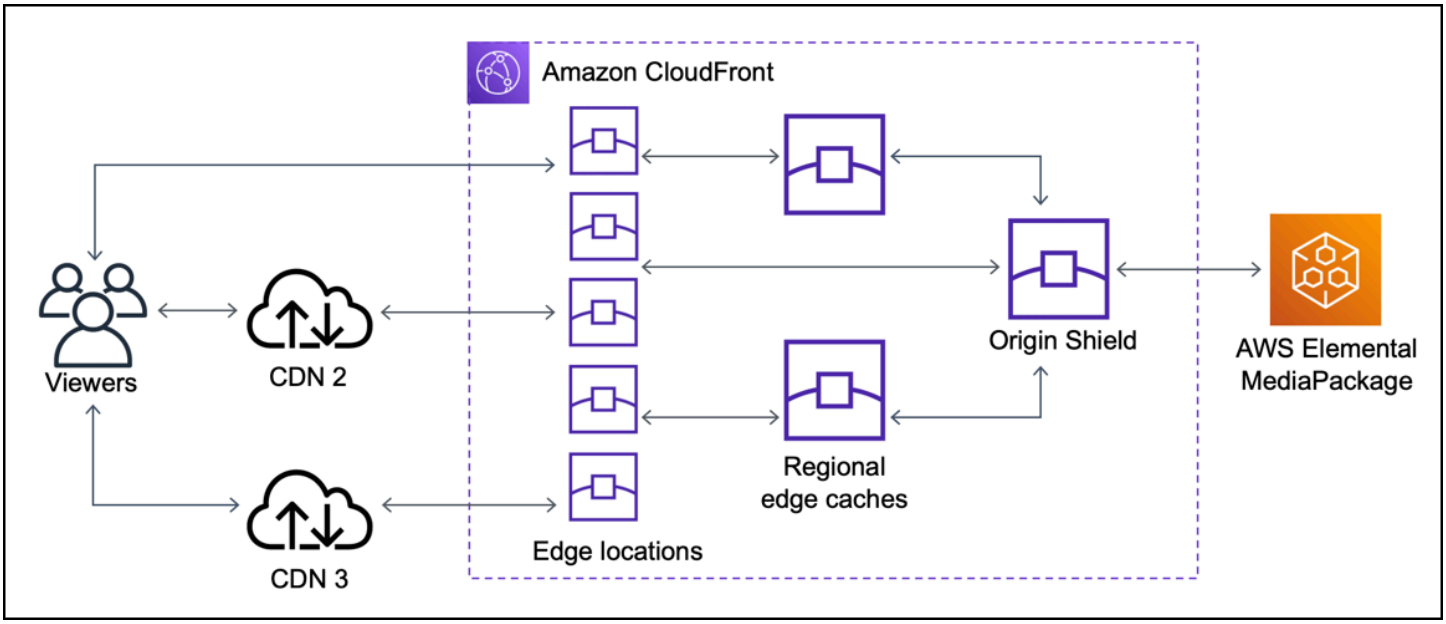
Senza Origin Shield (multiplo CDNs)

Senza Origin Shield, l'origine potrebbe ricevere molte richieste duplicate per lo stesso contenuto, ognuna proveniente da un CDN diverso, come mostrato nel diagramma seguente.



Con Origin Shield (multiplo CDNs)

Usare Origin Shield, con CloudFront come origine per gli altri CDNs, può aiutarti a ridurre il carico sull'origine, come mostrato nel diagramma seguente.



Scegli la AWS regione per Origin Shield

Amazon CloudFront offre Origin Shield nelle AWS regioni in cui CloudFront è presente una cache edge regionale. Quando attivi Origin Shield, scegli la AWS regione per Origin Shield. Si consiglia vivamente di scegliere la regione AWS che ha la latenza più bassa rispetto alla propria origine. Puoi usare Origin Shield con origini che si trovano in una AWS regione e con origini che non lo sono AWS.

Per le origini in una regione AWS

Se sei originario di una AWS regione, verifica innanzitutto se proviene da una regione in cui CloudFront è disponibile Origin Shield. CloudFront offre Origin Shield nelle seguenti AWS regioni.

- Stati Uniti orientali (Ohio) – `us-east-2`
- Stati Uniti orientali (Virginia settentrionale) – `us-east-1`
- Stati Uniti occidentali (Oregon) – `us-west-2`
- Asia Pacifico (Mumbai) – `ap-south-1`
- Asia Pacifico (Seul) - `ap-northeast-2`
- Asia Pacifico (Singapore) – `ap-southeast-1`
- Asia Pacifico (Sydney) - `ap-southeast-2`
- Asia Pacifico (Tokyo) - `ap-northeast-1`
- Europe (Francoforte) – `eu-central-1`
- Europa (Irlanda) – `eu-west-1`

- Europe (Londra) – `eu-west-2`
- Sud America (San Paolo) – `sa-east-1`
- Medio Oriente (EAU) — `me-central-1`

Se sei originario di una AWS regione in cui è disponibile CloudFront Origin Shield

Se sei originario di una AWS regione che CloudFront offre Origin Shield (vedi l'elenco precedente), abilita Origin Shield nella stessa regione in cui sei originario.

Se non sei originario di una AWS regione in cui è disponibile CloudFront Origin Shield

Se il tuo paese di origine non è in una AWS regione in cui è CloudFront disponibile Origin Shield, consulta la tabella seguente per determinare in quale regione abilitare Origin Shield.

Se l'origine è in...	Attivare lo scudo di origine in...
Stati Uniti occidentali (California settentrionale) – `us-west-1`	Stati Uniti occidentali (Oregon) – `us-west-2`
Africa (Città del Capo) – `af-south-1`	Europa (Irlanda) – `eu-west-1`
Asia Pacific (Hong Kong) – `ap-east-1`	Asia Pacifico (Singapore) – `ap-southeast-1`
Canada (Central) – `ca-central-1`	Stati Uniti orientali (Virginia settentrionale) – `us-east-1`
Europe (Milan) – `eu-south-1`	Europe (Francoforte) – `eu-central-1`
Europe (Paris) – `eu-west-3`	Europe (Londra) – `eu-west-2`
Europe (Stockholm) – `eu-north-1`	Europe (Londra) – `eu-west-2`
Middle East (Bahrain) – `me-south-1`	Asia Pacifico (Mumbai) – `ap-south-1`

Per origini al di fuori di AWS

È possibile utilizzare Origin Shield con un'origine locale o non presente in una regione AWS . In questo caso, abilita Origin Shield nella AWS regione con la latenza più bassa rispetto all'origine. Se

non sei sicuro di quale AWS regione abbia la latenza più bassa rispetto alla tua origine, puoi usare i seguenti suggerimenti per aiutarti a fare una scelta.

- È possibile consultare la tabella precedente per un'approssimazione circa quale regione AWS potrebbe avere la latenza più bassa rispetto alla propria origine, in base alla posizione geografica dell'origine.
- Puoi avviare EC2 istanze Amazon in alcune AWS regioni diverse geograficamente vicine alla tua origine ed eseguire alcuni test per `ping` misurare le latenze di rete tipiche tra tali regioni e la tua origine.

Abilitazione di Origin Shield

Origin Shield può essere abilitato per migliorare il tasso di occorrenza nella cache, ridurre il carico sull'origine e migliorare le prestazioni. Per abilitare Origin Shield, modifica le impostazioni di origine in una CloudFront distribuzione. Origin Shield è una proprietà dell'origine. Per ogni origine nelle tue CloudFront distribuzioni, puoi abilitare Origin Shield separatamente nella AWS regione che offre le migliori prestazioni per quell'origine.

Puoi abilitare Origin Shield nella CloudFront console CloudFormation, con o con l' CloudFrontAPI.

Console

Per abilitare Origin Shield per un'origine esistente (console)

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere la distribuzione con l'origine che si desidera aggiornare.
3. Seleziona la scheda Origins (Origini).
4. Scegliere l'origine da aggiornare, quindi scegliere Edit (Modifica).
5. Per Enable Origin Shield (Abilita scudo di origine), scegliere Yes (Sì).
6. Per Origin Shield Region (Regione scudo di origine), scegliere la regione AWS in cui si desidera abilitare lo scudo di origine. Per informazioni sulla scelta di una regione, vedere Scegli la AWS regione per Origin Shield.
7. Scegli Save changes (Salva modifiche).

Quando lo stato di distribuzione è Deployed (Distribuito), Origin Shield è pronto. Ci vogliono pochi minuti.

Per abilitare Origin Shield per una nuova origine (console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Per creare la nuova origine in una distribuzione esistente, effettuare le seguenti operazioni:

   1. Scegliere la distribuzione in cui si desidera creare l'origine.
   2. Scegliere Create Origin (Crea origine), quindi procedere al passaggio 3.

   Per creare la nuova origine in una nuova distribuzione, effettua le seguenti operazioni:

   1. Segui le fasi per creare una distribuzione standard nella console. Per ulteriori informazioni, consulta Crea una CloudFront distribuzione nella console.
   2. Nella sezione Impostazioni, seleziona Personalizza impostazioni origine. Procedi al passaggio 3.
3. Per Enable Origin Shield (Abilita scudo di origine), scegliere Yes (Sì).
4. Per Origin Shield Region (Regione scudo di origine), scegliere la regione AWS in cui si desidera abilitare lo scudo di origine. Per informazioni sulla scelta di una regione, vedere Scegli la AWS regione per Origin Shield.
5. Segui le fasi indicate nella console per completare la creazione dell'origine o della distribuzione.

Quando lo stato di distribuzione è Deployed (Distribuito), Origin Shield è pronto. Ci vogliono pochi minuti.

CloudFormation

Per abilitare Origin Shield con CloudFormation, usa la `OriginShield` proprietà nel tipo di `Origin` proprietà in una `AWS::CloudFront::Distribution` risorsa. È possibile aggiungere la proprietà `OriginShield` a una `Origin` esistente, o includerla quando si crea una nuova `Origin`.

Nell'esempio seguente viene illustrata la sintassi, in formato YAML, per l'abilitazione di `OriginShield` nella regione US West (Oregon) (`us-west-2`). Per informazioni sulla

scelta di una regione, vedere the section called “Scegli la AWS regione per Origin Shield”. In questo esempio viene visualizzato solo il tipo di proprietà `Origin` e non l'intera risorsa `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
```

Per ulteriori informazioni, consulta AWS::CloudFront::Distribution Origin nella sezione di riferimento alle risorse e alle proprietà della Guida AWS CloudFormation per l'utente.

API

Per abilitare Origin Shield con l' CloudFront API utilizzando AWS SDKs or AWS Command Line Interface (AWS CLI), usa il `OriginShield` tipo. È possibile specificare `OriginShield` in un `Origin`, in un oggetto `DistributionConfig`. Per informazioni sul `OriginShield` tipo, consulta le seguenti informazioni nell'Amazon CloudFront API Reference.

- OriginShield(tipo)
- Origin (tipo)
- DistributionConfig(tipo)
- UpdateDistribution(operazione)
- CreateDistribution(operazione)

La sintassi specifica per l'utilizzo di questi tipi e operazioni varia in base al client SDK, CLI o API. Per ulteriori informazioni, vedere la documentazione di riferimento per SDK, CLI o client.

Stima dei costi di Origin Shield

I costi di Origin Shield vengono addebitati in base al numero di richieste che vanno allo scudo di origine come livello incrementale.

Per le richieste dinamiche (non memorizzabili nella cache) che vengono inoltrate tramite proxy all'origine, Origin Shield è sempre un livello incrementale. Le richieste dinamiche utilizzano i metodi HTTP `PUT`, `POST`, `PATCH` e `DELETE`.

Le richieste `GET` e `HEAD` con un'impostazione TTL (time to live) inferiore a 3600 secondi sono considerate richieste dinamiche. Inoltre, anche le richieste `GET` e `HEAD` che hanno disabilitato la cache sono considerate richieste dinamiche.

Per stimare gli addebiti relativi a Origin Shield per le richieste dinamiche, usa la seguente formula:

Numero totale di richieste dinamiche x addebito Origin Shield per 10.000 richieste / 10.000

Per le richieste non dinamiche con i metodi HTTP `GET`, `HEAD` e `OPTIONS`, Origin Shield è talvolta un livello incrementale. Quando attivi Origin Shield, scegli Origin Shield. Regione AWS Per le richieste che vengono indirizzate naturalmente alla cache edge regionale nella stessa Regione di Origin Shield, Origin Shield non costituisce un livello incrementale. Per queste richieste non si accumulano addebiti per Origin Shield. Per le richieste che vengono indirizzate a una cache edge regionale in una Regione diversa da Origin Shield e quindi a Origin Shield, Origin Shield costituisce un livello incrementale. Per queste richieste si accumulano addebiti per Origin Shield.

Per stimare gli addebiti relativi a Origin Shield per le richieste dinamiche, usare la seguente formula:

Numero totale di richieste memorizzabili nella cache x (1 - tasso di occorrenza nella cache) x percentuale di richieste che vanno a Origin Shield da una cache edge regionale in una regione diversa x addebito dello scudo di origine per 10.000 richieste / 10.000

Per ulteriori informazioni sull'addebito per 10.000 richieste per lo scudo di origine, vedere Prezzi di CloudFront .

Alta disponibilità di Origin Shield.

Origin Shield sfrutta la funzionalità di cache edge CloudFront regionali. Ognuna di queste cache edge è integrata in una AWS regione che utilizza almeno tre zone di disponibilità con flotte di istanze Amazon con scalabilità automatica. EC2 Le connessioni da posizioni CloudFront allo scudo di origine utilizzano inoltre il rilevamento degli errori attivo per ogni richiesta per instradare automaticamente la richiesta a una posizione secondaria dello scudo di origine se la posizione principale non è disponibile.

In che modo Origin Shield interagisce con altre funzionalità CloudFront

Le sezioni seguenti spiegano il modo in cui lo scudo di origine interagisce con altre funzioni CloudFront.

Origin Shield e CloudFront registrazione

Per vedere quando Origin Shield ha gestito una richiesta, è necessario abilitare una delle seguenti opzioni:

- CloudFront registri standard (registri di accesso). I registri standard sono forniti gratuitamente.
- CloudFront registri di accesso in tempo reale. L'utilizzo dei log di accesso in tempo reale comporta costi aggiuntivi. Vedi i CloudFrontprezzi di Amazon.

Gli accessi alla cache di Origin Shield vengono visualizzati come `OriginShieldHit` nel `x-edge-detailed-result-type` campo CloudFront dei log. Origin Shield sfrutta le cache edge regionali CloudFront di Amazon. Se una richiesta viene instradata da un' CloudFront edge location alla cache edge regionale che funge da Origin Shield, viene riportata come a `Hit` nei log, non come. `OriginShieldHit`

Origin Shield e gruppi di origine

Lo scudo di origine è compatibile con i gruppi di origine CloudFront . Poiché Origin Shield è una proprietà dell'origine, le richieste viaggiano sempre attraverso Origin Shield per ogni origine anche quando l'origine fa parte di un gruppo di origine. Per una determinata richiesta, CloudFront indirizza la richiesta all'origine primaria nel gruppo di origine tramite Origin Shield dell'origine primaria. Se la richiesta ha esito negativo (in base ai criteri di failover del gruppo di origine), CloudFront indirizza la richiesta all'origine secondaria tramite Origin Shield dell'origine secondaria.

Origin Shield e Lambda@Edge

Origin Shield non influisce sulla funzionalità delle funzioni Lambda@Edgema può influire sulla AWS regione in cui vengono eseguite tali funzioni.

Quando usi Origin Shield con Lambda @Edge, i trigger rivolti all'origine (richiesta di origine e risposta all'origine) vengono eseguiti nella regione in AWS cui Origin Shield è abilitato. Se la sede principale di Origin Shield non è disponibile e CloudFront indirizza le richieste a una sede Origin Shield secondaria, anche i trigger di origine di Lambda @Edge passeranno a utilizzare la posizione Origin Shield secondaria.

I trigger rivolti al visualizzatore non sono interessati.

Ottimizzazione dell'elevata disponibilità con il failover di origine CloudFront

È anche possibile configurare CloudFront con il failover di origine per scenari che richiedono elevata disponibilità. Per iniziare, è necessario creare un gruppo di origine con due origini: una primaria e una secondaria. Se l'origine primaria non è disponibile o restituisce codici di stato di risposta HTTP specifici che indicano un errore, CloudFront passa automaticamente all'origine secondaria.

Per configurare il failover di origine, è necessario disporre di una distribuzione con almeno due origini. In seguito, viene creato un gruppo di origine per la distribuzione che include le due origini, impostandone una come primaria. Infine, è possibile creare o aggiornare un comportamento della cache per utilizzare il gruppo di origine.

Per vedere i passaggi per la configurazione dei gruppi di origine con le opzioni specifiche di failover di origine, consulta Creazione di un gruppo di origine.

Dopo aver configurato il failover di origine per un comportamento cache, CloudFront procede come segue per le richieste dei visualizzatori:

- Quando si verifica un'occorrenza nella cache, CloudFront restituisce l'oggetto richiesto.
- Quando si verifica un mancato riscontro della cache, CloudFront instrada la richiesta all'origine primaria nel gruppo di origine.
- Quando l'origine primaria restituisce un codice di stato non configurato per il failover, ad esempio un codice di stato HTTP 2xx o 3xx, CloudFront invia l'oggetto richiesto al visualizzatore.
- Quando si verifica una delle seguenti condizioni:
  - L'origine primaria restituisce un codice di stato HTTP configurato per il failover
  - CloudFront non riesce a connettersi all'origine primaria (quando 503 è impostato come codice di failover)
  - La risposta dall'origine primaria richiede troppo tempo (timeout) (quando 504 è impostato come codice di failover)

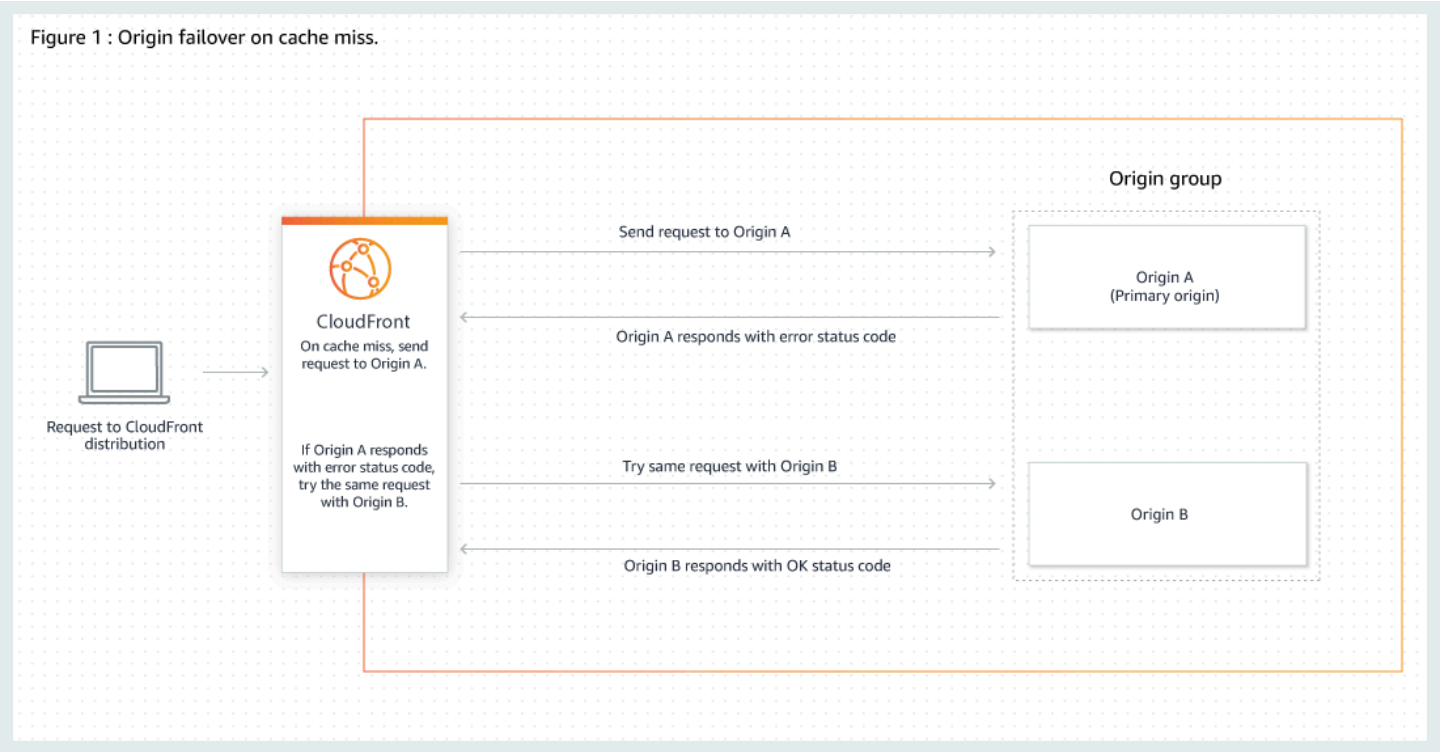
  Quindi, CloudFront instrada la richiesta all'origine secondaria nel gruppo di origine.

> **Note**
>
> Per alcuni casi d'uso, come lo streaming di contenuti video, potrebbe essere necessario per CloudFront eseguire rapidamente il failover all'origine secondaria. Per regolare la velocità di failover di CloudFront all'origine secondaria, consulta Controllo dei timeout e dei tentativi di origine.

CloudFront instrada tutte le richieste in entrata all'origine primaria, anche quando una richiesta precedente all'origine secondaria ha avuto esito negativo. CloudFront invia le richieste all'origine secondaria solo dopo che una richiesta all'origine primaria ha esito negativo.

CloudFront esegue il failover sull'origine secondaria solo quando il metodo HTTP della richiesta del visualizzatore è `GET`, `HEAD` o `OPTIONS`. CloudFront non esegue il failover quando il visualizzatore invia un metodo HTTP diverso (ad esempio `POST`, `PUT` e così via).

Il diagramma seguente illustrato il funzionamento del failover di origine.



Argomenti

- Creazione di un gruppo di origine

- Controllo dei timeout e dei tentativi di origine
- Utilizzo del failover di origine con le funzioni Lambda@Edge
- Utilizzo di pagine di errore personalizzate con failover di origine

Creazione di un gruppo di origine

Per creare un gruppo di origine

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli la distribuzione per la quale desideri creare il gruppo di origine.
3. Seleziona la scheda Origins (Origini).
4. Assicurati che la distribuzione abbia più di un'origine. In caso contrario, aggiungi una seconda origine.
5. Nella scheda Origini, nel pannello Gruppi di origine, scegli Crea gruppo di origine.
6. Scegli le origini per il gruppo di origine. Dopo aver aggiunto le origini, utilizza le frecce per impostare la priorità, ovvero quale origine è primaria e quale secondaria.
7. Digitare un nome per il gruppo di origine.
8. Scegli i codici di stato HTTP da utilizzare come criteri di failover. È possibile scegliere qualsiasi combinazione dei seguenti codici di stato: 400, 403, 404, 416, 500, 502, 503 o 504. Quando CloudFront riceve una risposta con uno dei codici di stato specificati, viene eseguito il failover sull'origine secondaria.

   > **Note**
   >
   > CloudFront esegue il failover sull'origine secondaria solo quando il metodo HTTP della richiesta del visualizzatore è `GET`, `HEAD` o `OPTIONS`. CloudFront non esegue il failover quando il visualizzatore invia un metodo HTTP diverso (ad esempio `POST`, `PUT` e così via).

9. In Criteri di selezione origine, specifica come vengono selezionate le origini quando la distribuzione instrada le richieste. Puoi scegliere le seguenti opzioni.

   Predefinita

   CloudFront utilizzerà la priorità di origine predefinita specificata nella pagina Impostazioni.

Punteggio di qualità multimediale

CloudFront tiene traccia e utilizza questo punteggio per determinare la prima origine a cui inoltrare la richiesta. Ciò autorizza inoltre CloudFront a effettuare richieste `HEAD` asincrone all'origine alternativa nel gruppo di origine per determinarne il punteggio di qualità multimediale. Puoi scegliere questa opzione solo per le origini AWS Elemental MediaPackage v2. Per ulteriori informazioni, consulta MQAR (Media Quality-Aware Resiliency).

10. Scegliere Crea un gruppo di origine.

Assicurati di assegnare il gruppo di origine come origine per il comportamento della cache della distribuzione. Per ulteriori informazioni, consulta Name.

Controllo dei timeout e dei tentativi di origine

Per impostazione predefinita, CloudFront tenta di connettersi all'origine primaria in un gruppo di origine per 30 secondi (3 tentativi di connessione di 10 secondi ciascuno) prima di eseguire il failover sull'origine secondaria. Per alcuni casi d'uso, come lo streaming di contenuti video, è possibile chiedere a CloudFront di eseguire il failover sull'origine secondaria più rapidamente. È possibile modificare le impostazioni seguenti in modo da influire sulla velocità con cui CloudFront esegue il failover all'origine secondaria. Se l'origine è un'origine secondaria o un'origine che non fa parte di un gruppo di origine, queste impostazioni influiscono sulla rapidità con cui CloudFront restituisce una risposta HTTP 504 al visualizzatore.

Per eseguire il failover più rapidamente, specificare un timeout di connessione più breve, un minor numero di tentativi di connessione o entrambi. Per le origini personalizzate (incluse le origini del bucket Amazon S3 che sono configurate con l'hosting di siti web statici), è inoltre possibile regolare il timeout di risposta all'origine.

Timeout connessione origine

L'impostazione del timeout della connessione di origine influisce sulla durata dell'attesa di CloudFront quando tenta di stabilire una connessione all'origine. Per impostazione predefinita, CloudFront attende 10 secondi per stabilire una connessione, ma è possibile specificare 1-10 secondi (estremi inclusi). Per ulteriori informazioni, consulta Timeout di connessione.

Tentativi di connessione all'origine

L'impostazione dei tentativi di connessione di origine influisce sul numero di tentativi di CloudFront di eseguire una connessione all'origine. Per impostazione predefinita, CloudFront tenta 3 volte

di connettersi, ma è possibile specificare 1-3 (estremi inclusi). Per ulteriori informazioni, consulta Tentativi di connessione.

Per un'origine personalizzata (incluso un bucket Amazon S3 configurato con hosting di siti web statici), questa impostazione influisce anche sul numero di tentativi di CloudFront di ottenere una risposta dall'origine nel caso di un timeout di risposta di origine.

Timeout di risposta origine

Il timeout di risposta dell'origine, noto anche come timeout di lettura dell'origine, influisce sul tempo di attesa di CloudFront per ricevere una risposta (o per ricevere la risposta completa) dall'origine. Per impostazione predefinita, CloudFront attende 30 secondi, ma è possibile specificare da 1 a 120 secondi (estremi inclusi). Per ulteriori informazioni, consulta Timeout di risposta.

Come modificare queste impostazioni

Per modificare queste impostazioni nella console CloudFront

- Per una nuova origine o una nuova distribuzione, è necessario specificare questi valori quando si crea la risorsa.
- Per un'origine esistente in una distribuzione esistente, è necessario specificare questi valori quando si modifica l'origine.

Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.

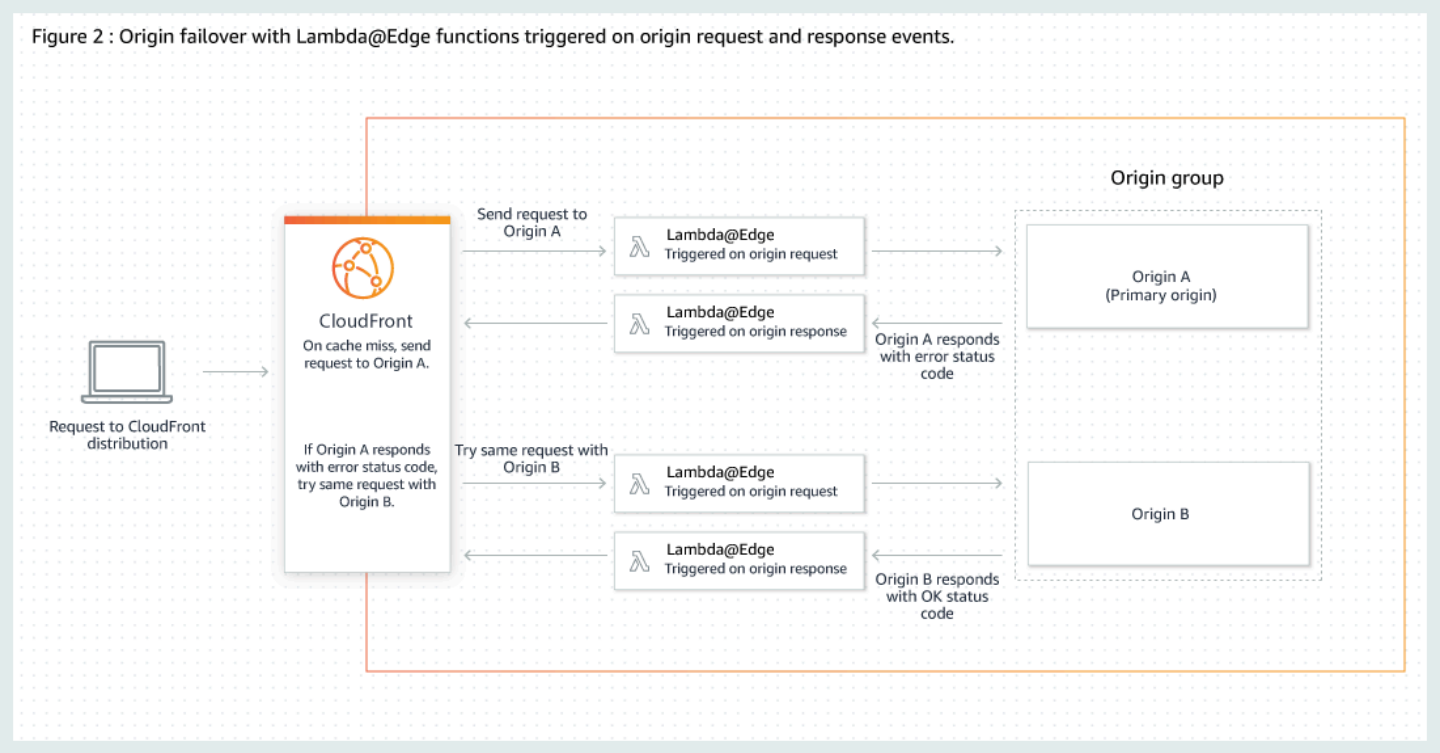
Utilizzo del failover di origine con le funzioni Lambda@Edge

È possibile utilizzare le funzioni Lambda@Edge con le distribuzioni CloudFront che hai impostato con i gruppi di origine. Per utilizzare una funzione Lambda, specificarla in una richiesta di origine o in un trigger di risposta di origine per un gruppo di origine quando si crea il comportamento della cache. Quando utilizzi una funzione Lambda@Edge con un gruppo di origine, la funzione può essere attivata due volte per una singola richiesta del visualizzatore. Considera ad esempio questo scenario:

1. Crei una funzione Lambda@Edge con un trigger di richiesta di origine.
2. La funzione Lambda viene attivata una volta quando CloudFront invia una richiesta all'origine primaria (su una mancanza di cache).
3. L'origine primaria risponde con un codice di stato HTTP configurato per il failover.

4. La funzione Lambda viene attivata nuovamente quando CloudFront invia la stessa richiesta all'origine secondaria.

Il seguente diagramma mostra il modo in cui il failover di origine funziona quando si include una funzione Lambda@Edge in un trigger di richiesta o di risposta origine.



Per ulteriori informazioni sull'utilizzo dei trigger Lambda@Edge, consulta the section called "Aggiunta di trigger per una funzione Lambda@Edge".

Per ulteriori informazioni sulla gestione del failover DNS, consulta Configurazione di un failover DNS nella Guida per gli sviluppatori di Amazon Route 53.

Utilizzo di pagine di errore personalizzate con failover di origine

È possibile utilizzare le pagine di errore personalizzate con i gruppi di origine in modo analogo a come si utilizzano con le origini che non sono impostate per il failover di origine.

Quando usi il failover di origine, CloudFront può essere configurato per restituire una pagina di errore personalizzata per l'origine primaria o secondaria (o entrambe):

- Restituisce una pagina di errore personalizzata per l'origine primaria: se l'origine primaria restituisce un codice di stato HTTP non configurato per il failover, CloudFront restituisce la pagina di errore personalizzata ai visualizzatori.
- Restituisce una pagina di errore personalizzata per l'origine secondaria: se CloudFront riceve un codice di stato di errore dall'origine secondaria, CloudFront restituisce la pagina di errore personalizzata.

Per ulteriori informazioni sull'utilizzo di pagine di errore personalizzate con CloudFront, consulta Generazione di risposte di errore personalizzate.

Gestione della durata di permanenza dei contenuti nella cache (scadenza)

Puoi controllare per quanto tempo i file rimangono in una cache CloudFront prima che CloudFront inoltri un'altra richiesta all'origine. Riducendo la durata, puoi distribuire contenuti dinamici. Aumentando la durata, gli utenti otterranno prestazioni migliori, poiché è più probabile che i file vengano distribuiti direttamente dalla cache edge. Una durata maggiore riduce anche il carico sul server di origine.

In genere, CloudFront distribuisce un file da una posizione edge fino alla scadenza della durata della cache indicata, cioè fino alla scadenza del file. Dopo la scadenza, la volta successiva in cui la posizione edge riceve una richiesta per il file da parte di un utente, CloudFront inoltra la richiesta all'origine per verificare che la cache contenga l'ultima versione del file. La risposta dall'origine dipende dall'eventuale modifica del file:

- Se la cache di CloudFront ha già l'ultima versione, l'origine restituisce il codice di stato `304 Not Modified`.
- Se la cache di CloudFront non ha l'ultima versione, l'origine restituisce un codice di stato `200 OK` e l'ultima versione del file.

Se un file in una posizione edge non viene richiesto frequentemente, CloudFront potrebbe eliminarlo, ovvero cancellarlo prima della sua data di scadenza, per fare spazio a file richiesti più di recente.

Ti consigliamo di gestire la durata della cache aggiornando la policy della cache della distribuzione. Se scegli di non utilizzare una policy della cache, il TTL (Time to Live) predefinito è di 24 ore, ma puoi aggiornare le seguenti impostazioni per sovrascrivere il valore predefinito:

- Per cambiare la durata della cache di tutti i file con lo stesso modello di percorso, puoi modificare le impostazioni di CloudFront per Minimum TTL (TTL minimo), Maximum TTL (TTL massimo) e Default TTL (TTL predefinito) per un comportamento cache. Per ulteriori informazioni sulle singole impostazioni, consulta Minimum TTL (TTL minimo), Maximum TTL (TTL massimo) e Default TTL (TTL di default).
- Per modificare la durata della cache per un singolo file, puoi configurare l'origine e aggiungere un'intestazione `Cache-Control` con la direttiva `max-age` o `s-maxage` oppure un'intestazione `Expires` al file. Per ulteriori informazioni, consulta Utilizzo delle intestazioni per controllare la durata della cache per i singoli oggetti.

Per ulteriori informazioni su come Minimum TTL (TTL minimo), Default TTL (TTL predefinito) e Maximum TTL (TTL massimo) interagiscono con le direttive `max-age` e `s-maxage` e il campo intestazione `Expires`, consulta the section called "Specifica dell'intervallo di tempo durante il quale CloudFront memorizza nella cache gli oggetti".

Puoi anche controllare per quanto tempo gli errori (ad esempio, `404 Not Found`) rimangono nella cache di CloudFront prima che CloudFront provi di nuovo a richiedere l'oggetto inoltrando un'altra richiesta all'origine. Per ulteriori informazioni, consulta the section called "In che modo CloudFront elabora i codici di stato HTTP 4xx e 5xx dalla tua origine".

Argomenti

- Utilizzo delle intestazioni per controllare la durata della cache per i singoli oggetti
- Fornire contenuti obsoleti (scaduti)
- Specifica dell'intervallo di tempo durante il quale CloudFront memorizza nella cache gli oggetti
- Aggiunta di intestazioni agli oggetti tramite l'utilizzo della console Amazon S3

Utilizzo delle intestazioni per controllare la durata della cache per i singoli oggetti

Puoi utilizzare le intestazioni `Cache-Control` e `Expires` per controllare la durata della permanenza degli oggetti nella cache. Anche le impostazioni per Minimum TTL (TTL minimo), Default TTL (TTL predefinito) e Maximum TTL (TTL massimo) influiscono sulla durata della cache, ma qui di seguito trovi una panoramica su come le intestazioni abbiano un impatto sulla durata della cache:

- La direttiva `Cache-Control max-age` consente di specificare il periodo di tempo (in secondi) durante il quale desideri che un oggetto rimanga nella cache prima che CloudFront ottenga di

nuovo l'oggetto dal server di origine. Il tempo di scadenza minimo supportato da CloudFront è 0 secondi. Il valore massimo è 100 anni. Specifica il valore nel seguente formato:

```
Cache-Control: max-age=secondi
```

Ad esempio, in base alla seguente direttiva, CloudFront manterrà l'oggetto associato nella cache per 3600 secondi (un'ora):

```
Cache-Control: max-age=3600
```

Se desideri che gli oggetti rimangano nelle edge cache di CloudFront per una durata diversa rispetto a quella di permanenza nelle cache dei browser, puoi utilizzare le direttive `Cache-Control max-age` e `Cache-Control s-maxage` insieme. Per ulteriori informazioni, consulta Specifica dell'intervallo di tempo durante il quale CloudFront memorizza nella cache gli oggetti.

- Il campo intestazione `Expires` consente di specificare una data di scadenza e un orario utilizzando il formato specificato in RFC 2616, Hypertext Transfer Protocol - HTTP/1.1 Sezione 3.3.1, Data completa, ad esempio:

  ```
  Sat, 27 Jun 2015 23:59:59 GMT
  ```

Ti consigliamo di utilizzare la direttiva `Cache-Control max-age` invece del campo dell'intestazione `Expires` per controllare la memorizzazione nella cache dell'oggetto. Se specifichi i valori sia per `Cache-Control max-age` sia per `Expires`, CloudFront utilizza solo il valore di `Cache-Control max-age`.

Per ulteriori informazioni, consulta Specifica dell'intervallo di tempo durante il quale CloudFront memorizza nella cache gli oggetti.

Non puoi utilizzare i campi di intestazione `Cache-Control` o `Pragma` HTTP in una richiesta `GET` da un visualizzatore per forzare CloudFront a tornare al server di origine per l'oggetto. CloudFront ignora tali campi di intestazione nelle richieste dei visualizzatori.

Per ulteriori informazioni sui campi delle intestazioni `Cache-Control` e `Expires`, consulta le seguenti sezioni in RFC 2616, Hypertext Transfer Protocol - HTTP/1.1:

- Section 14.9 Controllo della cache
- Section 14.21 Scadenze

Fornire contenuti obsoleti (scaduti)

CloudFront supporta le direttive di controllo della cache `Stale-While-Revalidate` e `Stale-If-Error`. Puoi utilizzare queste direttive per specificare per quanto tempo i contenuti obsoleti rimangono disponibili per i visualizzatori.

Argomenti

`Stale-While-Revalidate`

Questa direttiva consente a CloudFront di fornire contenuti obsoleti dalla cache mentre CloudFront recupera in modo asincrono una versione aggiornata dall'origine. Ciò migliora la latenza poiché i visualizzatori ricevono risposte immediate dalle posizioni edge senza dover attendere il recupero in background. I nuovi contenuti vengono caricati in background per le richieste future.

Example Ad esempio: **`Stale-While-Revalidate`**

CloudFront esegue le seguenti operazioni quando si imposta l'intestazione `Cache-Control` per utilizzare queste direttive.

```
Cache-Control: max-age=3600, stale-while-revalidate=600
```

1. CloudFront memorizzerà nella cache una risposta per un'ora (`max-age=3600`).
2. Se dopo questa durata viene effettuata una richiesta, CloudFront fornisce i contenuti non aggiornati inviando contemporaneamente una richiesta all'origine per riconvalidare e aggiornare i contenuti memorizzati nella cache.
3. Durante la riconvalida dei contenuti, CloudFront fornisce i contenuti obsoleti fino a 10 minuti (`stale-while-revalidate=600`).

> **Note**
>
> CloudFront fornirà il contenuto obsoleto fino al valore della direttiva `stale-while-revalidate` o al valore del TTL massimo di CloudFront, a seconda di quale dei due è

inferiore. Dopo la durata massima del TTL, l'oggetto obsoleto non sarà più disponibile dalla cache edge, indipendentemente dal valore `stale-while-revalidate`.

`Stale-If-Error`

Questa direttiva consente a CloudFront di fornire contenuti obsoleti dalla cache se l'origine non è raggiungibile o restituisce un codice di errore compreso tra 500 e 600. Ciò garantisce che i visualizzatori possano accedere ai contenuti anche durante un'interruzione dell'origine.

Example Ad esempio: **`Stale-If-Error`**

CloudFront esegue le seguenti operazioni quando si imposta l'intestazione `Cache-Control` per utilizzare queste direttive.

```
Cache-Control: max-age=3600, stale-if-error=86400
```

1. CloudFront memorizza nella cache la risposta per un'ora (`max-age=3600`).
2. Se l'origine è inattiva o restituisce un errore dopo questa durata, CloudFront continua a fornire i contenuti obsoleti per un massimo di 24 ore (`stale-if-error=86400`)
3. Se sono state configurate risposte di errore personalizzate, CloudFront tenterà di fornire il contenuto obsoleto se si verifica un errore entro la durata `stale-if-error` specificata. Se i contenuti obsoleti non sono disponibili, CloudFront fornirà le risposte di errore personalizzate configurate per il codice di stato di errore corrispondente. Per ulteriori informazioni, consulta Generazione di risposte di errore personalizzate.

> **Note**
>
> - CloudFront fornirà il contenuto obsoleto fino al valore della direttiva `stale-if-error` o al valore del TTL massimo di CloudFront, a seconda di quale dei due è inferiore. Dopo la durata massima del TTL, l'oggetto obsoleto non sarà più disponibile dalla cache edge, indipendentemente dal valore `stale-if-error`.
> - Se non si configurano risposte `stale-if-error` o risposte di errore personalizzate, CloudFront restituirà l'oggetto obsoleto o inoltrerà la risposta di errore al visualizzatore, a seconda che l'oggetto richiesto sia presente o meno nella cache edge. Per ulteriori

informazioni, consulta Come CloudFront elabora gli errori se non hai configurato pagine di errore personalizzate.

Utilizzo di entrambe le direttive

`stale-while-revalidate` e `stale-if-error` sono entrambe direttive di controllo della cache indipendenti che possono essere utilizzate insieme per ridurre la latenza e aggiungere un buffer affinché l'origine risponda o venga ripristinata.

Example Esempio: utilizzo di entrambe le direttive

CloudFront esegue le seguenti operazioni quando si imposta l'intestazione `Cache-Control` per utilizzare le seguenti direttive.

```
Cache-Control: max-age=3600, stale-while-revalidate=600, stale-if-error=86400
```

1. CloudFront memorizza nella cache la risposta per un'ora (`max-age=3600`).
2. Se si effettuata una richiesta dopo questo durata, CloudFront fornisce i contenuti non aggiornati per un massimo di 10 minuti (`stale-while-revalidate=600`) mentre i contenuti vengono riconvalidati.
3. Se il server di origine restituisce un errore mentre CloudFront tenta di riconvalidare i contenuti, CloudFront continuerà a fornire i contenuti non aggiornati per un massimo di 24 ore (`stale-if-error=86400`).

Il caching è un equilibrio tra prestazioni e dati aggiornati. L'uso di direttive come `stale-while-revalidate` e `stale-if-error` può migliorare le prestazioni e l'esperienza utente, ma è necessario assicurarsi che le configurazioni siano in linea con l'aggiornamento desiderato dei contenuti. Le direttive sui contenuti non aggiornati sono più adatte per i casi d'uso in cui i contenuti devono essere aggiornati ma la disponibilità della versione più recente non è essenziale. Inoltre, se i contenuti non cambiano o cambiano raramente, `stale-while-revalidate` potrebbe aggiungere richieste di rete non necessarie. Prendere invece in considerazione l'impostazione di una lunga durata della cache.

Specifica dell'intervallo di tempo durante il quale CloudFront memorizza nella cache gli oggetti

Per controllare la quantità di tempo in cui CloudFront mantiene un oggetto nella cache prima di inviare un'altra richiesta all'origine, è possibile:

- Impostare i valori TTL minimo, massimo e predefinito nel comportamento della cache di una distribuzione CloudFront. È possibile impostare questi valori in una policy di cache collegata al comportamento della cache (scelta consigliata) o nelle impostazioni della cache legacy.
- Includere l'intestazione `Cache-Control` o `Expires` nelle risposte dall'origine. Queste intestazioni consentono inoltre di determinare per quanto tempo un browser mantiene un oggetto nella cache del browser prima di inviare un'altra richiesta a CloudFront.

Nella tabella seguente viene illustrato come le intestazioni `Cache-Control` e `Expires` inviate dall'origine funzionano insieme alle impostazioni TTL in un comportamento di cache per influire sulla memorizzazione nella cache.

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
L'origine aggiunge una direttiva **`Cache-Control: max-age`** all'oggetto	Caching CloudFront CloudFront memorizza nella cache l'oggetto per il valore minimo della direttiva `Cache-Control: max-age` o per il valore TTL massimo CloudFront. Caching del browser I browser memorizzano nella cache l'oggetto per il valore della direttiva `Cache-Control: max-age` .	Caching CloudFront Il caching di CloudFront dipende dai valori del TTL minimo e TTL massimo CloudFront e dalla direttiva `Cache-Control max-age` : • Se TTL minimo < `max-age` < TTL massimo, CloudFront memorizza nella cache l'oggetto per il valore della direttiva `Cache-Control: max-age` . • Se `max-age` < TTL minimo, allora CloudFron

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
		t memorizza nella cache l'oggetto per il valore del TTL minimo CloudFront. • Se `max-age` > TTL massimo, allora CloudFront memorizza nella cache l'oggetto per il valore del TTL massimo CloudFront. Caching del browser I browser memorizzano nella cache l'oggetto per il valore della direttiva `Cache-Control: max-age` .
L'origine non aggiunge una direttiva **`Cache-Control: max-age`** all'oggetto	Caching CloudFront CloudFront memorizza nella cache l'oggetto per il valore del TTL predefinito CloudFront. Caching del browser Dipende dal browser.	Caching CloudFront CloudFront memorizza nella cache l'oggetto per il valore maggiore del TTL minimo o del TTL predefinito CloudFront. Caching del browser Dipende dal browser.

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
L'origine aggiunge le direttive **`Cache-Control: max-age`** e **`Cache-Control: s-maxage`** all'oggetto	Caching CloudFront CloudFront memorizza nella cache l'oggetto per il valore minimo della direttiva `Cache-Control: s-maxage` o per il valore TTL massimo CloudFront. Caching del browser I browser memorizzano nella cache l'oggetto per il valore della direttiva `Cache-Control max-age` .	Caching CloudFront Il caching di CloudFront dipende dai valori del TTL minimo e TTL massimo CloudFront e dalla direttiva `Cache-Control: s-maxage`: • Se TTL minimo < `s-maxage` < TTL massimo, CloudFront memorizza nella cache l'oggetto per il valore della direttiva `Cache-Control: s-maxage` . • Se `s-maxage` < TTL minimo, allora CloudFront memorizza nella cache l'oggetto per il valore del TTL minimo CloudFront. • Se `s-maxage` > TTL massimo, allora CloudFront memorizza nella cache l'oggetto per il valore del TTL massimo CloudFront. Caching del browser I browser memorizzano nella cache l'oggetto per il valore

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
		della direttiva `Cache-Control: max-age` .

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
L'origine aggiunge un'intestazione **`Expires`** all'oggetto	Caching CloudFront CloudFront memorizza nella cache l'oggetto fino alla data dell'intestazione `Expires` o al valore del TTL massimo di CloudFront, a seconda di quale dei due si verifica prima. Caching del browser I browser memorizzano nella cache l'oggetto fino alla data presente nell'intestazione `Expires`.	Caching CloudFront Il caching di CloudFront dipende dai valori del TTL minimo e TTL massimo CloudFront e dall'intestazione `Expires`: • Se TTL minimo < `Expires` < TTL massimo, CloudFront memorizza nella cache l'oggetto fino alla data e all'ora presente nell'intestazione `Expires`. • Se `Expires` < TTL minimo, allora CloudFront memorizza nella cache l'oggetto per il valore del TTL minimo CloudFront. • Se `Expires` > TTL massimo, allora CloudFront memorizza nella cache l'oggetto per il valore del TTL massimo CloudFront. Caching del browser I browser memorizzano nella cache l'oggetto fino alla data e all'ora presenti nell'intestazione `Expires`.

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
L'origine aggiunge le direttive **`Cache-Control: no-cache`** , **`no-store`** e/o **`private`** all'oggetto	CloudFront e i browser rispettano le intestazioni.	Caching CloudFront CloudFront memorizza nella cache l'oggetto per il valore del TTL minimo CloudFront. Consulta l'avviso sotto questa tabella. Caching del browser I browser rispettano le intestazioni.

Warning

- Se il TTL minimo è maggiore di 0, CloudFront utilizza il TTL minimo della policy della cache, anche se le direttive`no-store`, `private` e/o `Cache-Control: no-cache` sono presenti nelle intestazioni di origine.
  - Se l'origine è raggiungibile, CloudFront ottiene l'oggetto dall'origine e lo restituisce al visualizzatore.
  - Se l'origine non è raggiungibile e il valore TTL minimo o massimo è maggiore di 0, CloudFront servirà l'oggetto ottenuto dall'origine in precedenza.

  Per evitare questo comportamento, includere la direttiva `Cache-Control: stale-if-error=0` con l'oggetto restituito dall'origine. Ciò fa sì che, se l'origine non è raggiungibile, CloudFront restituisca un errore in risposta a richieste future piuttosto che l'oggetto ottenuto dall'origine in precedenza.
- CloudFront non memorizza nella cache il codice di stato HTTP 501 (Non implementato) da un'origine S3 quando le intestazioni dell'origine includono le direttive `Cache-Control: no-cache`, `no-store` e/o `private`. Questo è il comportamento predefinito per un'origine S3, anche se l'impostazione TTL minima è maggiore di 0.

Per informazioni su come modificare le impostazioni per le distribuzioni utilizzando la console CloudFront, consulta Aggiornamento di una distribuzione. Per informazioni su come modificare le impostazioni per le distribuzioni utilizzando le API CloudFront, consulta UpdateDistribution.

Aggiunta di intestazioni agli oggetti tramite l'utilizzo della console Amazon S3

Puoi aggiungere il campo di intestazione `Expires` o `Cache-Control` agli oggetti Amazon S3. Per farlo, è necessario modificare i campi dei metadati dell'oggetto.

Come aggiungere il campo di intestazione **`Expires`** o **`Cache-Control`** agli oggetti Amazon S3

1. Segui la procedura nella sezione Sostituzione dei metadati definiti dal sistema nell'argomento Modifica dei metadati degli oggetti nella console Amazon S3 nella Guida per l'utente di Amazon S3.
2. Per Chiave, scegli il nome dell'intestazione che stai aggiungendo (Cache-Control o Scadenze).
3. In Value (Valore)immetti un valore di intestazione. Ad esempio, per un'intestazione `Cache-Control`, è possibile immettere `max-age=86400`. Per `Expires`, è possibile inserire una data di scadenza e un'ora ad esempio `Wed, 30 Jun 2021 09:28:00 GMT`.
4. Segui il resto della procedura per salvare le modifiche apportate ai metadati.

Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query

Alcune applicazioni Web utilizzano stringhe di query per inviare informazioni al server di origine. Una stringa di query è la parte di una richiesta Web che viene visualizzata dopo un carattere ?; la stringa può contenere uno o più parametri, separati da caratteri &. Nell'esempio che segue, la stringa di query include due parametri, *`colore = rosso`* e *`dimensioni = grandi`*:

`https://d111111abcdef8.cloudfront.net/images/image.jpg?`*`color=red&size=large`*

Per le distribuzioni, puoi scegliere se desideri che CloudFront inoltri le stringhe di query all'origine e se vuoi memorizzare nella cache i contenuti in base a tutti i parametri o ai parametri selezionati. Perché questo potrebbe essere utile? Analizza l'esempio seguente.

Supponiamo che il tuo sito Web sia disponibile in cinque lingue. La struttura delle directory e i nomi dei file per le cinque versioni del sito Web sono identiche. Quando un utente visualizza il sito

web, le richieste inoltrate a CloudFront; includono un parametro della stringa di query relativa alla lingua in base alla lingua che l'utente ha scelto. Puoi configurare CloudFront in modo che inoltri le stringhe di query al server di origine e memorizzi nella cache in base al parametro della lingua. Se configuri il server Web per restituire la versione di una determinata pagina che corrisponda alla lingua selezionata, CloudFront memorizza nella cache ciascuna versione di lingua separatamente, in base al valore del parametro della stringa di query relativo alla lingua.

In questo esempio, se la pagina principale del sito Web è `main.html`, le seguenti cinque richieste comporteranno la memorizzazione nella cache da parte di `main.html` di CloudFront per cinque volte, una volta per ogni valore del parametro della stringa di query relativa alla lingua:

- `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`

Tieni presente quanto segue:

- Alcuni server HTTP non elaborano parametri delle stringhe di query e, di conseguenza, non restituiscono diverse versioni di un oggetto in base ai valori dei parametri. Per queste origini, se configuri CloudFront in modo da inoltrare i parametri delle stringhe di query all'origine, CloudFront continua a memorizzare nella cache in base ai valori dei parametri anche se l'origine restituisce a CloudFront versioni identiche dell'oggetto per ogni valore di parametro.
- Affinché i parametri delle stringhe di query funzionino come descritto nell'esempio precedente con le lingue, devi utilizzare il carattere & come delimitatore tra i parametri delle stringhe di query. Se utilizzi un delimitatore diverso, puoi ottenere risultati imprevisti, a seconda dei parametri che specifichi vengano utilizzati da CloudFront come base per la memorizzazione nella cache, nonché dall'ordine in cui i parametri vengono visualizzati nella stringa di query.

  Negli esempi seguenti viene mostrato cosa accade se utilizzi un delimitatore diverso e configuri CloudFront per la memorizzazione nella cache solo in base al parametro `color`:

  - Nella richiesta che segue, CloudFront memorizza nella cache i contenuti in base al valore del parametro `color`, ma CloudFront interpreta il valore come `red;size=large`:

    ```
    https://d111111abcdef8.cloudfront.net/images/
    image.jpg?color=red;size=large
    ```

- Nella seguente richiesta, CloudFront memorizza nella cache i contenuti, ma basa il caching sui parametri della stringa di query. Questo perché hai configurato CloudFront in modo che memorizzi nella cache in base al parametro `color`, ma CloudFront interpreta la stringa seguente come contenente solo un parametro `size` che ha un valore di *`large;color=red`*:

  ```
  https://d111111abcdef8.cloudfront.net/images/
  image.jpg?size=large;color=red
  ```

È possibile configurare CloudFront in modo che esegua una delle seguenti operazioni:

- Non inoltrare le stringhe di query al server di origine. Se non inoltri le stringhe di query, CloudFront non memorizza nella cache in base ai parametri della stringa di query.
- Inoltra le stringhe di query al server di origine e memorizza nella cache in base a tutti i parametri della stringa di query.
- Inoltra le stringhe di query al server di origine e memorizza nella cache in base a parametri specifici della stringa di query.

Per ulteriori informazioni, consulta the section called “Ottimizzazione del caching”.

Argomenti

- Impostazioni della console e delle API per l’inoltro delle stringhe di query e per la memorizzazione nella cache
- Ottimizzazione del caching
- Parametri della stringa di query e log standard CloudFront (log di accesso)

Impostazioni della console e delle API per l’inoltro delle stringhe di query e per la memorizzazione nella cache

Quando crei una distribuzione nella console CloudFront, CloudFront configura l’inoltro delle stringhe di query e il caching in base al tipo di origine. Facoltativamente, puoi modificare manualmente queste impostazioni. Per ulteriori informazioni, consulta le impostazioni seguenti nella the section called “Tutte le impostazioni distribuzione”:

- the section called “Query String Forwarding and Caching (Inoltro e caching di stringhe di query)”
- the section called “Elenco consentiti stringhe di query”

Per configurare l'inoltro e la memorizzazione nella cache delle stringhe di query con l'API CloudFront, consulta CachePolicy e OriginRequestPolicy nella Documentazione di riferimento delle API di Amazon CloudFront.

Ottimizzazione del caching

Quando si configura CloudFront in modo che memorizzi nella cache in base ai parametri delle stringhe di query, è possibile eseguire la procedura seguente per ridurre il numero di richieste inoltrate all'origine da CloudFront. Quando le edge location CloudFront forniscono gli oggetti, si riduce il carico sul server di origine e si riduce la latenza perché gli oggetti vengono forniti da posizioni più vicine agli utenti.

Cache basata solo su parametri per i quali la tua origine restituisce versioni diverse di un oggetto

Per ogni parametro della stringa di query che la tua applicazione web inoltra a CloudFront, CloudFront inoltra richieste al tuo server di origine per ogni valore di parametro e memorizza nella cache una versione separata dell'oggetto per ogni valore di parametro. Ciò è valido anche se il server di origine restituisce sempre lo stesso oggetto indipendentemente dal valore di parametro. Per più parametri, il numero di richieste e di oggetti si moltiplicano.

Ti consigliamo di configurare CloudFront in modo che memorizzi nella cache solo in base ai parametri della stringa di query per i quali l'origine restituisce versioni differenti e di valutare attentamente i vantaggi del caching in base a ciascun parametro. Supponiamo ad esempio che tu abbia un sito Web di vendita al dettaglio. Disponi delle immagini di una giacca in sei colori diversi e la giacca è disponibile in dieci taglie diverse. Le immagini che hai della giacca mostrano i diversi colori, ma non le differenti taglie. Per ottimizzare la memorizzazione nella cache, dovresti configurare CloudFront in modo che memorizzi nella cache solo in base al parametro colore e non in base al parametro taglia. In questo modo, si aumenta la probabilità che CloudFront possa servire una richiesta dalla cache e di conseguenza si migliorano le prestazioni e si riduce il carico sull'origine.

Elenca sempre i parametri nello stesso ordine

L'ordine dei parametri è importante in materia di stringhe di query. In questo esempio, le stringhe di query sono identiche, anche che i parametri sono in ordine diverso. Per questo motivo CloudFront inoltra due richieste separate per image.jpg all'origine e memorizza nella cache due versioni diverse dell'oggetto:

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red&size=large`

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large&color=red`

  Ti consigliamo sempre di elencare i nomi dei parametri nello stesso ordine, seguendo, ad esempio, l'ordine alfabetico.

Usa sempre lo stesso formato per nomi e valori di parametri

CloudFront considera il formato dei nomi e dei valori dei parametri in caso di caching in base ai parametri della stringa di query. In questo esempio, le stringhe di query sono identiche, eccetto per il formato dei nomi e dei valori dei parametri. Per questo motivo CloudFront inoltra quattro richieste separate per image.jpg all'origine e memorizza nella cache quattro versioni diverse dell'oggetto:

- `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`

Ti consigliamo di usare lo stesso formato, maiuscolo o minuscolo, per i nomi e i valori dei parametri, ad esempio tutte in minuscolo.

Non utilizzare nomi di parametri in conflitto con URL firmati

Se usi URL firmati per limitare l'accesso ai tuoi contenuti (se hai aggiunto firmatari attendibili alla distribuzione), CloudFront rimuove i seguenti parametri della stringa di query prima di inoltrare il resto dell'URL al server di origine:

- `Expires`
- `Key-Pair-Id`
- `Policy`
- `Signature`

Se usi URL firmati e desideri configurare CloudFront per inoltrare le stringhe di query al server di origine, i parametri della stringa di query non possono essere denominati `Expires`, `Key-Pair-Id`, `Policy` o `Signature`.

Parametri della stringa di query e log standard CloudFront (log di accesso)

Se abiliti i log, CloudFront registrerà l'URL completo, inclusi i parametri delle stringhe di query. Questo avviene anche se hai configurato CloudFront in modo che inoltri le stringhe di query al server

di origine. Per ulteriori informazioni sulla registrazione di CloudFront, consulta the section called “Registri di accesso (registri standard)”.

Caching dei contenuti basati su cookie

Per impostazione predefinita, CloudFront non considera i cookie durante l’elaborazione di richieste e risposte o quando memorizza nella cache gli oggetti nelle posizioni edge. Se CloudFront riceve due richieste identiche ad eccezione di ciò che è contenuto nell’intestazione `Cookie`, per impostazione predefinita CloudFront considera le richieste come identiche e restituisce lo stesso oggetto per entrambe.

Puoi configurare CloudFront per inoltrare all’origine alcuni o tutti i cookie nelle richieste dei visualizzatori e per memorizzare nella cache versioni separate degli oggetti in base ai valori dei cookie inoltrati. Quando si esegue questa operazione, CloudFront utilizza alcuni o tutti i cookie presenti nelle richieste del visualizzatore, a prescindere da quelli configurati per l’inoltro, per identificare in modo univoco un oggetto nella cache.

Ad esempio, supponiamo che le richieste per `locations.html` contengano un cookie `country` con un valore di `uk` o `fr`. Quando si configura CloudFront per memorizzare nella cache gli oggetti in base al valore del cookie `country`, CloudFront inoltra le richieste `locations.html` all’origine e include il cookie `country` e il suo valore. Il server di origine restituisce `locations.html` e CloudFront memorizza nella cache l’oggetto una volta per le richieste in cui il valore del cookie `country` è `uk` e una volta per le richieste in cui il valore è `fr`.

> **Important**
>
> Amazon S3 e alcuni server HTTP non elaborano i cookie. Non configurare CloudFront per l’inoltro di cookie a un’origine che non elabora i cookie o che non varia la risposta in base ai cookie. Ciò può causare l’inoltro da parte di CloudFront di più richieste all’origine per lo stesso oggetto, fattore che rallenta le prestazioni e aumenta il carico sull’origine. Se, considerando l’esempio precedente, l’origine non elabora il cookie `country` o restituisce sempre la stessa versione di `locations.html` a CloudFront indipendentemente dal valore del cookie `country`, non configurare CloudFront per l’inoltro di tale cookie.
>
> Al contrario, se l’origine personalizzata dipende da un particolare cookie o invia risposte diverse in base a un cookie, assicurati di configurare CloudFront per inoltrare tale cookie all’origine. In caso contrario, CloudFront rimuove il cookie prima di inoltrare la richiesta all’origine.

Per configurare l'inoltro dei cookie, aggiorna il comportamento della cache della distribuzione. Per ulteriori informazioni sui comportamenti della cache, consulta Cache Behavior Settings (Impostazioni del comportamento della cache), in particolare le sezioni Forward Cookies (Inoltra cookie) e Cookie elenco consentiti.

È possibile configurare ogni comportamento della cache per eseguire una delle operazioni seguenti:

- Inoltro di tutti i cookie all'origine: CloudFront include tutti i cookie inviati dal visualizzatore quando inoltra le richieste all'origine. Quando l'origine restituisce una risposta, CloudFront la memorizza nella cache utilizzando i nomi e i valori dei cookie nella richiesta del visualizzatore. Se la risposta di origine include intestazioni `Set-Cookie`, CloudFront le restituisce al visualizzatore con l'oggetto richiesto. CloudFront memorizza anche nella cache le intestazioni `Set-Cookie` con l'oggetto restituito dall'origine e invia tali intestazioni `Set-Cookie` ai visualizzatori su tutti gli accessi della cache.
- Inoltra un set di cookie specificato dall'utente – CloudFront rimuove tutti i cookie inviati dal visualizzatore che non sono presenti nell'elenco di domini prima di inoltrare una richiesta all'origine. CloudFront memorizza nella cache la risposta utilizzando i nomi dei cookie nell'elenco e i valori nella richiesta del visualizzatore. Se la risposta di origine include intestazioni `Set-Cookie`, CloudFront le restituisce al visualizzatore con l'oggetto richiesto. CloudFront memorizza anche nella cache le intestazioni `Set-Cookie` con l'oggetto restituito dall'origine e invia tali intestazioni `Set-Cookie` ai visualizzatori su tutti gli accessi della cache.

  Per informazioni su come specificare i caratteri jolly nei nomi dei cookie, consulta Cookie elenco consentiti.

  Per conoscere la quota corrente relativa al numero di nomi di cookie che puoi inoltrare per ogni comportamento cache o per richiedere una quota superiore, consulta Quote sulle stringhe di query (impostazioni della cache legacy).
- Nessun inoltro di cookie all'origine: CloudFront non memorizza nella cache gli oggetti in base ai valori dei cookie inviati dal visualizzatore. Inoltre, CloudFront rimuove i cookie prima di inoltrare le richieste all'origine e rimuove le intestazioni `Set-Cookie` dalle risposte prima di restituire le risposte i visualizzatori. Poiché questo non è un modo ottimale per utilizzare le risorse di origine, quando si seleziona questo comportamento della cache, è necessario assicurarsi che l'origine non includa i cookie nelle risposte di origine per impostazione predefinita.

Note importanti su come specificare i cookie che desideri inoltrare:

Log di accesso

Se configuri CloudFront per registrare le richieste e i cookie, CloudFront registra tutti i cookie e i relativi attributi, anche se configuri CloudFront in modo che non inoltri i cookie all'origine oppure se lo configuri in modo che inoltri solo cookie specifici. Per ulteriori informazioni sulla registrazione di CloudFront, consulta Registri di accesso (registri standard).

Distinzione tra lettere maiuscole e minuscole

I nomi e i valori dei cookie fanno entrambi distinzione tra maiuscole e minuscole. Ad esempio, se CloudFront è configurato per inoltrare tutti i cookie e due richieste del visualizzatore per lo stesso oggetto hanno cookie identici ad eccezione delle maiuscole e delle minuscole, CloudFront memorizza l'oggetto nella cache due volte.

CloudFront ordina i cookie

Se CloudFront è configurato per inoltrare i cookie (tutti o un sottoinsieme), CloudFront ordina i cookie nell'ordine naturale in base al nome del cookie prima di inoltrare la richiesta all'origine.

> **Note**
>
> I nomi dei cookie che iniziano con il carattere $ non sono supportati. CloudFront rimuove il cookie prima di inoltrare la richiesta all'origine. Puoi rimuovere il carattere $ o specificare un carattere diverso all'inizio del nome del cookie.

`If-Modified-Since` e `If-None-Match`

Le richieste condizionali `If-Modified-Since` e `If-None-Match` non sono supportate quando CloudFront è configurato per inoltrare i cookie (tutti o un sottoinsieme).

Il formato standard della coppia nome-valore obbligatorio

CloudFront inoltra un'intestazione cookie solo se il valore è conforme al formato standard di coppia nome-valore, ad esempio: `"Cookie: cookie1=value1; cookie2=value2"`

Disabilitazione della memorizzazione nella cache delle intestazioni **`Set-Cookie`**

Se CloudFront è configurato per inoltrare i cookie all'origine (tutti o cookie specifici), memorizza anche nella cache le intestazioni `Set-Cookie` ricevute nella risposta di origine. CloudFront include queste intestazioni `Set-Cookie` nella sua risposta al visualizzatore originale e le include anche nelle risposte successive che vengono servite dalla cache CloudFront.

Se desideri ricevere i cookie all'origine ma non desideri che CloudFront memorizzi nella cache le intestazioni `Set-Cookie` nelle risposte dell'origine, configura l'origine per aggiungere un'intestazione `Cache-Control` con una direttiva `no-cache` che specifica `Set-Cookie` come nome di campo. Ad esempio: `Cache-Control: no-cache="Set-Cookie"`. Per ulteriori informazioni, consulta l'argomento relativo alle direttive di controllo delle risposte della cache nello standard Hypertext Transfer Protocol (HTTP/1.1): Caching.

Lunghezza massima dei nomi dei cookie

Se configuri CloudFront per l'inoltro di cookie specifici all'origine, il numero totale di byte in tutti i nomi dei cookie configurati per l'inoltro da parte di CloudFront non può superare 512 meno il numero di cookie che si stanno inoltrando. Ad esempio, se si configura CloudFront in modo che inoltri 10 cookie al server di origine, la lunghezza complessiva dei nomi dei 10 cookie non può superare 502 byte (512 - 10).

Se configuri CloudFront in modo che inoltri tutti i cookie al server di origine, la lunghezza dei nomi di cookie non è rilevante.

Per ulteriori informazioni sull'utilizzo della console CloudFront per aggiornare una distribuzione in modo che CloudFront inoltri i cookie al server di origine, consulta Aggiornamento di una distribuzione. Per informazioni sull'utilizzo dell'API CloudFront per aggiornare una distribuzione, consulta UpdateDistribution nella Documentazione di riferimento dell'API di Amazon CloudFront.

Caching dei contenuti in base alle intestazioni di richiesta

CloudFront ti consente di scegliere se desideri che CloudFront inoltri le intestazioni al server di origine e memorizzi nella cache le versioni separate di un oggetto specificato in base ai valori dell'intestazione per le richieste dei visualizzatori. In questo modo è possibile distribuire diverse versioni dei tuoi contenuti in base al dispositivo che l'utente utilizza, alla posizione del visualizzatore, al linguaggio utilizzato dal visualizzatore e a un'ampia gamma di altri criteri.

Argomenti

- Configurazione del caching in base alla posizione del visualizzatore
- Configurazione del caching in base al protocollo della richiesta
- Configurazione del caching per i file compressi
- In che modo il caching basato sulle intestazioni influenza le performance
- In che modo il formato delle intestazioni e dei valori delle intestazioni si ripercuotono sul caching
- Intestazioni che CloudFront restituisce al visualizzatore

Intestazioni e distribuzioni – Panoramica

Per impostazione predefinita, CloudFront non considera le intestazioni quando memorizza nella cache gli oggetti nelle edge location. Se il server di origine restituisce due oggetti che differiscono solo in base ai valori delle intestazioni delle richieste, CloudFront memorizza nella cache solo una versione dell'oggetto.

Puoi configurare CloudFront per inoltrare le intestazioni al server di origine e ciò comporta la memorizzazione nella cache da parte di CloudFront di più versioni di un oggetto in base ai valori presenti in una o più intestazioni delle richieste. Per configurare CloudFront allo scopo di memorizzare nella cache gli oggetti in base ai valori di intestazione specifici, devi specificare le impostazioni del comportamento della cache per la tua distribuzione. Per ulteriori informazioni, consulta Cache basata su intestazioni di richiesta selezionate.

Ad esempio, supponiamo che le richieste del visualizzatore per `logo.jpg` contengano un'intestazione personalizzata `Product` con un valore di `Acme` o `Apex`. Quando configuri CloudFront per memorizzare nella cache i tuoi oggetti in base al valore dell'intestazione `Product`, CloudFront inoltra le richieste per `logo.jpg` al server di origine e include l'intestazione `Product` e i relativi valori. CloudFront memorizza nella cache `logo.jpg` una volta per le richieste in cui il valore dell'intestazione `Product` è `Acme` e una volta per le richieste in cui il valore è `Apex`.

Puoi configurare ogni comportamento cache in una distribuzione per eseguire una delle seguenti operazioni:

- Inoltro di tutte le intestazioni al server di origine

> **Note**
>
> Per impostazioni della cache legacy: se configuri CloudFront per inoltrare tutte le intestazioni alla tua origine, il servizio non memorizza nella cache gli oggetti associati al comportamento della cache, ma invia ogni richiesta all'origine.

- Inoltro di un elenco di intestazioni da te specificata. CloudFront memorizza nella cache i tuoi oggetti in base ai valori in tutte le intestazioni specificate. CloudFront inoltra anche le intestazioni inoltrate per impostazione predefinita, ma memorizza i tuoi oggetti nella cache solo in base alle intestazioni che specifichi.
- Inoltra solo le intestazioni predefinite. In questa configurazione, CloudFront non memorizza nella cache gli oggetti in base ai valori riportati nelle intestazioni delle richieste.

Per conoscere la quota corrente relativa al numero di intestazioni che puoi inoltrare per ogni comportamento cache o per richiedere una quota superiore, consulta Quote delle intestazioni.

Per ulteriori informazioni sull'utilizzo della console CloudFront per aggiornare una distribuzione in modo che CloudFront inoltri i cookie al server di origine, consulta Aggiornamento di una distribuzione. Per informazioni sull'utilizzo dell'API CloudFront per aggiornare una distribuzione esistente, consulta Aggiorna distribuzione nella Documentazione di riferimento dell'API di Amazon CloudFront.

Selezione delle intestazioni su cui basare il caching

Le intestazioni che puoi inoltrare al server di origine e su cui CloudFront basa il caching variano a seconda che la tua origine sia un bucket Amazon S3 o un server di origine personalizzato.

- Amazon S3: puoi configurare CloudFront per inoltrare e memorizzare nella cache i tuoi oggetti in base a una serie di intestazioni specifiche (vedi il seguente elenco di eccezioni). Tuttavia, ti consigliamo di evitare intestazioni di inoltro con un server di origine Amazon S3, a meno che non sia necessario implementare la condivisione delle risorse multi-origine (CORS) o si desideri personalizzare il contenuto utilizzando Lambda@Edge negli eventi relativi ai server di origine.
  - Per configurare la condivisione CORS, devi inoltrare intestazioni che consentono a CloudFront di distribuire contenuti per siti Web abilitati per la condivisione di risorse multi-origine (CORS). Per ulteriori informazioni, consulta Configurazione di CloudFront per rispettare le impostazioni CORS.
  - Per personalizzare i contenuti utilizzando le intestazioni che inoltri al tuo server di origine Amazon S3, scrivi e aggiungi le funzioni Lambda@Edge e associale alla tua distribuzione

CloudFront affinché possano essere attivate da un evento relativo a un server di origine. Per ulteriori informazioni sull'utilizzo delle intestazioni per personalizzare contenuti, consulta Esempi di personalizzazione del contenuto in base alle intestazioni del paese o del tipo di dispositivo.

Consigliamo di evitare di inoltrare le intestazioni non utilizzate per personalizzare i contenuti perché inoltrare intestazioni aggiuntive può ridurre il rapporto di occorrenza nella cache. In altre parole, CloudFront non può elaborare tutte le richieste dalle cache edge, come proporzione di tutte le richieste.

- Server di origine personalizzato - Puoi configurare CloudFront per memorizzare nella cache in base al valore di qualsiasi intestazione di richiesta, eccetto nei seguenti casi:
  - `Connection`
  - `Cookie` – Se desideri inoltrare e memorizzare nella cache in base ai cookie, devi utilizzare un'impostazione separate nella tua distribuzione. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.
  - `Host (for Amazon S3 origins)`
  - `Proxy-Authorization`
  - `TE`
  - `Upgrade`

  Puoi configurare CloudFront per memorizzare nella cache gli oggetti in base ai valori riportati nelle intestazioni `Date` e `User-Agent`, ma non lo consigliamo. Queste intestazioni hanno numerosi valori possibili e la memorizzazione nella cache in base ai valori causerebbe l'inoltro da parte di CloudFront di molte più richieste all'origine.

Per un elenco completo di tutte le intestazioni delle richieste HTTP e per informazioni su come CloudFront le elabora, consulta Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3).

Configurazione di CloudFront per rispettare le impostazioni CORS

Se hai abilitato la condivisione di risorse multi-origine (CORS) su un bucket Amazon S3 o un server di origine personalizzato, devi selezionare intestazioni specifiche da inoltrare, in modo che vengano rispettate le impostazioni CORS. Le intestazioni che devi inoltrare variano a seconda del server di origine (Amazon S3 o personalizzato) e della volontà di memorizzare nella cache le risposte `OPTIONS`.

Amazon S3

- Se desideri che le risposte `OPTIONS` vengano memorizzate nella cache, esegui le operazioni descritte di seguito:
  - Scegli le opzioni per le impostazioni predefinite di comportamento della cache che abilitano la memorizzazione nella cache per le risposte `OPTIONS`.
  - Configurare CloudFront per inoltrare le seguenti intestazioni: `Origin`, `Access-Control-Request-Headers` e `Access-Control-Request-Method`.
- Se non desideri che le risposte `OPTIONS` vengano memorizzate nella cache, configura CloudFront affinché inoltri l'intestazione `Origin`, insieme ad altre intestazioni richieste dal server di origine (ad esempio, `Access-Control-Request-Headers`, `Access-Control-Request-Method` o altro).

Server di origine personalizzati – Inoltra l'intestazione `Origin` insieme a qualsiasi altra intestazione richiesta dal server di origine.

Per configurare CloudFront in modo che memorizzi nella cache le risposte basate su CORS, è necessario configurare CloudFront per inoltrare le intestazioni utilizzando una policy della cache. Per ulteriori informazioni, consulta Controllo della chiave della cache con una policy.

Per ulteriori informazioni su CORS e Amazon S3, consulta Utilizzo delle funzionalità Cross-Origin Resource Sharing (CORS) nella Guida per l'utente di Amazon Simple Storage Service.

Configurazione del caching in base al tipo di dispositivo

Se desideri che CloudFront memorizzi nella cache le diverse versioni degli oggetti in base al dispositivo utilizzato dall'utente per visualizzare i contenuti, configura CloudFront in modo che inoltri le intestazioni applicabili al tuo server di origine personalizzato:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

In base al valore dell'intestazione `User-Agent`, CloudFront imposta il valore di queste intestazioni su `true` o `false` prima di inoltrare la richiesta al server di origine. Se il dispositivo ricade in più di una categoria, allora più di un valore potrebbe essere `true`. Ad esempio, per alcuni dispositivi tablet,

CloudFront potrebbe impostare `CloudFront-Is-Mobile-Viewer` e `CloudFront-Is-Tablet-Viewer` su `true`.

Configurazione del caching in base alla lingua del visualizzatore

Se desideri che CloudFront memorizzi nella cache le diverse versioni degli oggetti in base alla lingua specificata nella richiesta, configura CloudFront in modo che inoltri l'intestazione `Accept-Language` all'origine.

Configurazione del caching in base alla posizione del visualizzatore

Se desideri che CloudFront memorizzi nella cache le diverse versioni degli oggetti in base al paese da cui proviene la richiesta, configura CloudFront in modo che inoltri l'intestazione `CloudFront-Viewer-Country` al server di origine. CloudFront converte automaticamente l'indirizzo IP da cui proviene la richiesta in un codice paese a due lettere. Per una elenco dei codici Paese semplice da usare, ordinabile per codice e per nome paese, vedi la voce Wikipedia ISO 3166-1 alfa-2.

Configurazione del caching in base al protocollo della richiesta

Se desideri che CloudFront memorizzi nella cache le diverse versioni degli oggetti in base al protocollo della richiesta, HTTP o HTTPS, configura CloudFront in modo che inoltri l'intestazione `CloudFront-Forwarded-Proto` al server di origine.

Configurazione del caching per i file compressi

Se la tua origine supporta la compressione Brotli, puoi memorizzare nella cache in base all'intestazione `Accept-Encoding`. Configurare il caching solo in base a `Accept-Encoding` se l'origine distribuisce diversi contenuti in base all'intestazione.

In che modo il caching basato sulle intestazioni influenza le performance

Quando configuri CloudFront per la memorizzazione nella cache in base a una o più intestazioni e le intestazioni dispongono di più valori possibili, CloudFront inoltra più richieste al tuo server di origine per lo stesso oggetto. Questo rallenta le prestazioni e aumenta il carico di lavoro del server di origine. Se il server di origine restituisce lo stesso oggetto, indipendentemente dal valore di una determinata intestazione, ti consigliamo di non configurare CloudFront per memorizzare nella cache in base a tale intestazione.

Se configuri CloudFront per inoltrare più di un'intestazione, l'ordine delle intestazioni nelle richieste del visualizzatore non interessa il caching, a condizione che i valori sono gli stessi. Ad esempio,

se una richiesta contiene le intestazioni A:1, B:2 e un'altra richiesta contiene B:2, A:1, CloudFront memorizza nella cache solo una copia dell'oggetto.

In che modo il formato delle intestazioni e dei valori delle intestazioni si ripercuotono sul caching

Quando CloudFront memorizza nella cache in base ai valori dell'intestazione, non considera il caso del nome dell'intestazione, mentre considera il caso del valore dell'intestazione:

- Se le richieste del visualizzatore includono entrambi `Product:Acme` e `product:Acme`, CloudFront memorizza l'oggetto nella cache solo una volta. L'unica differenza tra loro è il caso del nome dell'intestazione, che non interessa la memorizzazione nella cache.
- Se le richieste del visualizzatore includono entrambe `Product:Acme` e `Product:acme`, CloudFront memorizza un oggetto nella cache due volte, poiché il valore è `Acme` in alcune richieste e `acme` in altre.

Intestazioni che CloudFront restituisce al visualizzatore

La configurazione di CloudFront per l'inoltro e la memorizzazione nella cache delle intestazioni non influenza le intestazioni che CloudFront restituisce al visualizzatore. CloudFront restituisce tutte le intestazioni ottenute dal server di origine con poche eccezioni. Per ulteriori informazioni, consulta l'argomento applicabile:

- Origini di Amazon S3 Consulta Intestazioni di risposta HTTP che rimuovono o aggiornano CloudFront.
- Origini personalizzate Consulta Intestazioni di risposta HTTP che CloudFront rimuovono o sostituiscono.

Controllo della chiave della cache con una policy

Con una policy della cache CloudFront, puoi specificare le intestazioni HTTP, i cookie e le stringhe di query incluse da CloudFront nella chiave della cache per gli oggetti che vengono memorizzati nella cache a livello di posizioni edge CloudFront. La chiave della cache è l'identificatore univoco per ogni oggetto nella cache e determina se una richiesta HTTP del visualizzatore genera un riscontro nella cache.

Un riscontro nella cache si verifica quando una richiesta del visualizzatore genera la stessa chiave di cache di una richiesta precedente e l'oggetto per tale chiave di cache si trova nella cache della posizione edge ed è valido. In presenza di un riscontro nella cache, l'oggetto viene servito al visualizzatore da una posizione edge di CloudFront, che presenta i seguenti vantaggi:

- Carico ridotto sul server di origine
- Latenza ridotta per il visualizzatore

L'inclusione di meno valori nella chiave cache aumenta la probabilità di un'occorrenza nella cache. Questo può migliorare le prestazioni del sito web o dell'applicazione grazie a una percentuale di riscontri nella cache più elevata (una percentuale maggiore di richieste visualizzatore che generano un riscontro nella cache). Per ulteriori informazioni, consulta Comprensione della chiave della cache.

Per controllare la chiave della cache, utilizzare una policy della cache CloudFront. Si collega una policy della cache a uno o più comportamenti della cache in una distribuzione CloudFront.

È inoltre possibile utilizzare la policy della cache per specificare le impostazioni durata (TTL) per gli oggetti nella cache CloudFront e consentire a CloudFront di richiedere e memorizzare nella cache gli oggetti compressi.

> **Note**
>
> Le impostazioni della cache non influiscono sulle richieste gRPC perché il traffico gRPC non può essere memorizzato nella cache. Per ulteriori informazioni, consulta Usare gRPC con le distribuzioni CloudFront .

Argomenti

- Informazioni sulle policy della cache

- Creazione di policy della cache
- Utilizzo delle policy della cache gestite
- Comprensione della chiave della cache

Informazioni sulle policy della cache

È possibile utilizzare una policy della cache per migliorare il rapporto di accessi della cache controllando i valori (stringhe di query URL, intestazioni HTTP e cookie) inclusi nella chiave della cache. CloudFront fornisce alcune policy della cache predefinite, note come policy gestite, per casi d'uso comuni. È possibile utilizzare queste policy gestite oppure creare policy della cache personalizzate specifiche per le proprie esigenze. Per ulteriori informazioni sulle policy gestite, consulta Utilizzo delle policy della cache gestite.

Una policy della cache contiene le seguenti impostazioni, suddivise in informazioni sulle policy, impostazioni TTL (Time to Live) e impostazioni della chiave della cache.

Informazioni sulle policy

Nome

Un nome per identificare la policy della cache. Nella console, è possibile utilizzare il nome per collegare la policy della cache a un comportamento della cache.

Descrizione

Un commento per descrivere la policy della cache. Questo è facoltativo, ma può aiutare a identificare lo scopo della policy della cache.

Impostazioni Time to Live (TTL)

Le impostazioni Time to Live (TTL) funzionano insieme alle intestazioni HTTP `Cache-Control` e `Expires` (se si trovano nella risposta di origine) per determinare quanto tempo gli oggetti nella cache CloudFront rimangono validi.

Minimum TTL (TTL minimo)

Il tempo minimo, in secondi, in cui si desidera che gli oggetti rimangano nella cache CloudFront prima che CloudFront verifichi l'origine per stabilire se l'oggetto è stato aggiornato. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

> **Warning**
>
> Se il TTL minimo è maggiore di 0, CloudFront memorizzerà nella cache il contenuto almeno per la durata specificata nel TTL minimo della policy della cache, anche se le direttive `Cache-Control: no-cache`, `no-store` o `private` sono presenti nelle intestazioni di origine.

Maximum TTL (TTL massimo)

Il tempo massimo, in secondi, in cui si desidera che gli oggetti rimangano nella cache CloudFront prima che CloudFront verifichi l'origine per stabilire se l'oggetto è stato aggiornato. CloudFront utilizza questa impostazione solo quando l'origine invia le intestazioni `Cache-Control` o `Expires` con l'oggetto. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Default TTL (TTL di default)

Il tempo predefinito, in secondi, in cui si desidera che gli oggetti rimangano nella cache CloudFront prima che CloudFront verifichi l'origine per stabilire se l'oggetto è stato aggiornato. CloudFront utilizza il valore di questa impostazione come TTL dell'oggetto solo quando l'origine non invia intestazioni `Cache-Control` o `Expires` con l'oggetto. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

> **Note**
>
> Se le impostazioni TTL minimo, TTL massimo e TTL predefinito sono tutte impostate su 0, ciò disabilita il caching di CloudFront.

Impostazioni chiave cache

Le impostazioni della chiave della cache specificano i valori nelle richieste del visualizzatore che CloudFront include nella chiave della cache. I valori possono includere stringhe di query URL, intestazioni HTTP e cookie. I valori inclusi nella chiave cache vengono automaticamente inclusi nelle richieste che CloudFront invia all'origine, note come richieste di origine. Per informazioni sul controllo delle richieste di origine senza influire sulla chiave della cache, consulta Controllo delle richieste di origine con una policy.

Le impostazioni della chiave della cache includono:

- Headers
- Cookie
- Stringhe di query
- Supporto della compressione

Headers

Le intestazioni HTTP nelle richieste del visualizzatore che CloudFront include nella chiave cache e nelle richieste di origine. Per le intestazioni puoi scegliere una delle seguenti impostazioni:

- None (Nessuna) - Le intestazioni HTTP nelle richieste del visualizzatore non sono incluse nella chiave della cache e non vengono incluse automaticamente nelle richieste di origine.
- Includere le seguenti intestazioni - Si specifica quali intestazioni HTTP nelle richieste del visualizzatore sono incluse nella chiave della cache e incluse automaticamente nelle richieste di origine.

Quando si utilizza l'impostazione Includere le seguenti intestazioni, si specificano le intestazioni HTTP in base al loro nome e non al loro valore. Considera, ad esempio, la seguente intestazione HTTP:

```
Accept-Language: en-US,en;q=0.5
```

In questo caso, si specifica l'intestazione come `Accept-Language`, non come `Accept-Language: en-US,en;q=0.5`. Tuttavia, CloudFront include l'intestazione completa, compreso il suo valore, nella chiave cache e nelle richieste di origine.

È inoltre possibile includere alcune intestazioni generate da CloudFront nella chiave cache. Per ulteriori informazioni, consulta the section called “Aggiunta di intestazioni della richiesta CloudFront”.

Cookie

I cookie nelle richieste del visualizzatore che CloudFront include nella chiave cache e nelle richieste di origine. Per i cookie puoi scegliere una delle seguenti impostazioni:

- None (Nessuno) - I cookie nelle richieste del visualizzatore non sono inclusi nella chiave cache e non vengono automaticamente inclusi nelle richieste di origine.

- All (Tutti) - I cookie nelle richieste del visualizzatore sono inclusi nella chiave cache e vengono automaticamente inclusi nelle richieste di origine.
- Includere cookie specifici - Si specifica quali cookie nelle richieste del visualizzatore sono inclusi nella chiave cache e automaticamente inclusi nelle richieste di origine.
- Includere tutti i cookie tranne - Si specifica quali cookie nelle richieste del visualizzatore non sono inclusi nella chiave cache e non vengono automaticamente inclusi nelle richieste di origine. Tutti gli altri cookie, eccetto quelli specificati, sono inclusi nella chiave cache e automaticamente inclusi nelle richieste di origine.

Quando si utilizza l'impostazione Includere i cookie specificati o Includere tutti i cookie tranne, si specificano i cookie in base al loro nome e non al loro valore. Considera, ad esempio, l'intestazione `Cookie` seguente.

```
Cookie: session_ID=abcd1234
```

In questo caso, si specifica il cookie come `session_ID`, non come `session_ID=abcd1234`. Tuttavia, CloudFront include il cookie completo, compreso il suo valore, nella chiave cache e nelle richieste di origine.

Stringhe di query

Le stringhe di query URL nelle richieste di visualizzatore che CloudFront include nella chiave cache e nelle richieste di origine. Per le stringhe di query, è possibile scegliere una delle seguenti impostazioni:

- None (Nessuna) - Le stringhe di query nelle richieste del visualizzatore non sono incluse nella chiave cache e non vengono automaticamente incluse nelle richieste di origine.
- All (Tutte) - Le stringhe di query nelle richieste del visualizzatore sono incluse nella chiave della cache e vengono incluse automaticamente nelle richieste di origine.
- Includere stringhe di query specifiche - Si specifica quali stringhe di query nelle richieste del visualizzatore devono essere incluse nella chiave cache e incluse automaticamente nelle richieste di origine.
- Includere tutte le stringhe di query tranne - Si specifica quali stringhe di query nelle richieste del visualizzatore non sono incluse nella chiave cache e non vengono automaticamente incluse nelle richieste di origine. Tutte le altre stringhe di query, eccetto quelle specificate, sono incluse nella chiave cache e incluse automaticamente nelle richieste di origine.

Quando si utilizza l'impostazione Includere le stringhe di query specificate o Includere tutte le stringhe di query, si specificano le stringhe di query in base al loro nome e non al loro valore. Considera, ad esempio, il seguente percorso URL:

```
/content/stories/example-story.html?split-pages=false
```

In questo caso, si specifica la stringa di query come `split-pages`, non come `split-pages=false`. Tuttavia, CloudFront include la stringa di query completa, incluso il suo valore, nella chiave cache e nelle richieste di origine.

> **Note**
>
> Per le impostazioni della chiave della cache, CloudFront tratta il carattere asterisco (`*`) per le intestazioni, le stringhe di query e i cookie come una stringa letterale, non come un carattere jolly.

Supporto della compressione

Queste impostazioni consentono a CloudFront di richiedere e memorizzare nella cache oggetti compressi nei formati di compressione Gzip o Brotli, quando il visualizzatore li supporta. Queste impostazioni consentono anche il funzionamento della compressione CloudFront. I visualizzatori indicano il loro supporto per questi formati di compressione con l'intestazione `Accept-Encoding` HTTP.

> **Note**
>
> I browser web Chrome e Firefox supportano la compressione Brotli solo quando la richiesta viene inviata utilizzando HTTPS. Questi browser non supportano Brotli con richieste HTTP.

Attivare queste impostazioni quando si verifica una delle seguenti condizioni:

- La tua origine restituisce oggetti compressi Gzip quando i visualizzatori li supportano (le richieste contengono l'intestazione `Accept-Encoding` HTTP con `gzip` come valore). In questo caso, utilizza l'impostazione Abilitato per Gzip (imposta `EnableAcceptEncodingGzip` su `true` nell'API CloudFront, negli SDK AWS, in AWS CLI o CloudFormation).

- L'origine restituisce oggetti compressi Brotli quando i visualizzatori li supportano (le richieste contengono l'intestazione `Accept-Encoding` HTTP con `br` come valore). In questo caso, utilizza l'impostazione Abilitato per Brotli (imposta `EnableAcceptEncodingBrotli` su `true` nell'API CloudFront, negli SDK AWS, in AWS CLI o CloudFormation).
- Il comportamento della cache a cui è collegata questa policy della cache è configurato con la Compressione CloudFront. In questo caso, è possibile abilitare la memorizzazione nella cache per Gzip o Brotli, o entrambi. Quando la compressione CloudFront è abilitata, abilitare la memorizzazione nella cache per entrambi i formati può contribuire a ridurre i costi per il trasferimento dei dati su Internet.

> **Note**
>
> Se si abilita la memorizzazione nella cache per uno o entrambi questi formati di compressione, non includere l'intestazione `Accept-Encoding` in una policy di richiesta di origine associata allo stesso comportamento della cache. CloudFront include sempre questa intestazione nelle richieste di origine quando la memorizzazione nella cache è abilitata per uno di questi formati, pertanto l'inclusione `Accept-Encoding` in una policy di richiesta di origine non ha alcun effetto.

Se il server di origine non restituisce oggetti compressi Gzip o Brotli o il comportamento della cache non è configurato con la compressione CloudFront, non abilitare la memorizzazione nella cache per gli oggetti compressi. Se lo fai, potrebbe causare una diminuzione del tuo rapporto di hit della cache.

Di seguito viene illustrato come queste impostazioni influiscono su una distribuzione CloudFront. Tutti gli scenari seguenti presuppongono che la richiesta del visualizzatore includa l'intestazione `Accept-Encoding`. Quando la richiesta del visualizzatore non include l'intestazione `Accept-Encoding`, CloudFront non include questa intestazione nella chiave della cache e non la include nella richiesta di origine corrispondente.

Quando la memorizzazione nella cache degli oggetti compressi è attivata per entrambi i formati di compressione

Se il visualizzatore supporta sia Gzip che Brotli, cioè se i valori `gzip` e `br` sono entrambi nell'intestazione `Accept-Encoding` nella richiesta del visualizzatore, CloudFront procede come segue:

- Normalizza l'intestazione `Accept-Encoding: br,gzip` e include l'intestazione normalizzata nella chiave della cache. La chiave della cache non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.
- Se la posizione del bordo contiene un oggetto compresso Brotli o Gzip nella cache che corrisponde alla richiesta e non è scaduto, la posizione del bordo restituisce l'oggetto al visualizzatore.
- Se la posizione edge non ha un oggetto compresso Brotli o Gzip nella cache che corrisponde alla richiesta e non è scaduto, CloudFront include l'intestazione normalizzata (`Accept-Encoding: br,gzip`) nella richiesta di origine corrispondente. La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Se il visualizzatore supporta un formato di compressione ma non l'altro, ad esempio, se `gzip` è un valore nell'intestazione `Accept-Encoding` nella richiesta del visualizzatore ma `br` non lo è, CloudFront esegue le seguenti operazioni:

- Normalizza l'intestazione `Accept-Encoding: gzip` e include l'intestazione normalizzata nella chiave della cache. La chiave della cache non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.
- Se la posizione edge contiene un oggetto compresso Gzip nella cache che corrisponde alla richiesta e non è scaduto, la posizione edge restituisce l'oggetto al visualizzatore.
- Se la posizione edge non ha un oggetto Gzip compresso nella cache che corrisponde alla richiesta e non è scaduto, CloudFront include l'intestazione normalizzata (`Accept-Encoding: gzip`) nella richiesta di origine corrispondente. La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Per capire cosa fa CloudFront se il visualizzatore supporta Brotli ma non Gzip, sostituire i due formati di compressione l'uno con l'altro nell'esempio precedente.

Se il visualizzatore non supporta Brotli o GZip, cioè se l'intestazione `Accept-Encoding` nella richiesta del visualizzatore non contiene `br` o `gzip` come valori, CloudFront:

- Non include l'intestazione `Accept-Encoding` nella chiave della cache.
- Include `Accept-Encoding: identity` nella richiesta di origine corrispondente. La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Quando la memorizzazione nella cache degli oggetti compressi è abilitata per un formato di compressione, ma non per l'altro

Se il visualizzatore supporta il formato per il quale è abilitata la memorizzazione nella cache, ad esempio, se la memorizzazione nella cache degli oggetti compressi è abilitata per Gzip e il visualizzatore supporta Gzip (`gzip` è uno dei valori nell'intestazione `Accept-Encoding` nella richiesta del visualizzatore), CloudFront procede come segue:

- Normalizza l'intestazione `Accept-Encoding: gzip` e include l'intestazione normalizzata nella chiave della cache.
- Se la posizione edge contiene un oggetto compresso Gzip nella cache che corrisponde alla richiesta e non è scaduto, la posizione edge restituisce l'oggetto al visualizzatore.
- Se la posizione edge non ha un oggetto Gzip compresso nella cache che corrisponde alla richiesta e non è scaduto, CloudFront include l'intestazione normalizzata (`Accept-Encoding: gzip`) nella richiesta di origine corrispondente. La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Questo comportamento è lo stesso quando il visualizzatore supporta sia Gzip che Brotli (l'intestazione `Accept-Encoding` nella richiesta del visualizzatore include entrambi `gzip` e `br` come valori), perché in questo scenario, la memorizzazione nella cache degli oggetti compressi per Brotli non è abilitata.

Per capire cosa fa CloudFront se la memorizzazione nella cache degli oggetti compressi è abilitata per Brotli ma non per Gzip, sostituire i due formati di compressione l'uno con l'altro nell'esempio precedente.

Se il visualizzatore non supporta il formato di compressione per il quale è abilitata la memorizzazione nella cache (l'intestazione `Accept-Encoding` nella richiesta del visualizzatore non contiene il valore per quel formato), CloudFront:

- Non include l'intestazione `Accept-Encoding` nella chiave della cache.
- Include `Accept-Encoding: identity` nella richiesta di origine corrispondente. La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Quando la memorizzazione nella cache degli oggetti compressi è disabilitata per entrambi i formati

Quando la memorizzazione nella cache degli oggetti compressi è disabilitata per entrambi i formati di compressione, CloudFront tratta l'intestazione `Accept-Encoding` allo stesso

modo di qualsiasi altra intestazione HTTP nella richiesta del visualizzatore. Per impostazione predefinita, non è inclusa nella chiave della cache e non è inclusa nelle richieste di origine. È possibile includerla nell'elenco delle intestazioni in una policy della cache o in una policy di richiesta di origine come qualsiasi altra intestazione HTTP.

Creazione di policy della cache

È possibile utilizzare una policy della cache per migliorare il rapporto di accessi della cache controllando i valori (stringhe di query URL, intestazioni HTTP e cookie) inclusi nella chiave della cache. È possibile creare una policy della cache nella console di CloudFront, con l'AWS Command Line Interface (AWS CLI) o con l'API CloudFront.

Dopo aver creato una policy della cache, è possibile collegarla a uno o più comportamenti della cache in una distribuzione CloudFront.

Console

Per creare una policy della cache (console)

1. Accedi alla Console di gestione AWS e apri la pagina Policy nella console CloudFront all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home?#/policies .
2. Scegliere Crea policy cache.
3. Scegliere l'impostazione desiderata per questa policy della cache. Per ulteriori informazioni, consulta Informazioni sulle policy della cache.
4. Al termine, scegli Create (Crea).

Dopo aver creato una policy della cache, è possibile collegarla a un comportamento della cache.

Per allegare una policy della cache a una distribuzione esistente (console)

1. Apri la pagina Distribuzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Scegli la distribuzione da aggiornare, quindi scegli la scheda Comportamenti.
3. Scegliere il comportamento della cache da aggiornare, quindi scegliere Modifica.

   In alternativa, per creare un nuovo comportamento della cache, scegliere Crea comportamento.

4. Per la Chiave di cache e richiesta di origine, assicurarsi che sia scelto Policy di cache e policy di richiesta origine.
5. Per Policy cache, scegliere la policy della cache da collegare a questo comportamento della cache.
6. Scegli Save changes (Salva modifiche) nella parte inferiore della pagina.

Per allegare una policy della cache a una nuova distribuzione (console)

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere Create Distribution (Crea distribuzione).
3. Per la Chiave di cache e richiesta di origine, assicurarsi che sia scelto Policy di cache e policy di richiesta origine.
4. Per Cache policy (Policy della cache), scegliere la policy della cache da associare al comportamento predefinito della cache di questa distribuzione.
5. Scegliere le impostazioni desiderate per l'origine, il comportamento predefinito della cache e altre impostazioni di distribuzione. Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.
6. Al termine, scegliere Crea distribuzione.

CLI

Per creare una policy della cache con AWS Command Line Interface (AWS CLI), utilizzare il comando aws cloudfront create-cache-policy. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare una policy della cache (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `cache-policy.yaml` che contiene tutti i parametri di input per il comando create-cache-policy.

```
aws cloudfront create-cache-policy --generate-cli-skeleton yaml-input > cache-policy.yaml
```

2. Aprire il file `cache-policy.yaml` appena creato. Modificare il file per specificare le impostazioni delle policy della cache desiderate, quindi salvare il file. È possibile rimuovere i campi facoltativi dal file, ma non rimuovere i campi obbligatori.

   Per ulteriori informazioni sulle impostazioni delle policy della cache, consulta Informazioni sulle policy della cache.

3. Utilizzare il comando seguente per creare la policy della cache utilizzando i parametri di input dal file `cache-policy.yaml`.

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

   Prendere nota del valore `Id` nell'output del comando. Questo è l'ID della policy della cache ed è necessario per collegare la policy della cache al comportamento della cache di una distribuzione CloudFront.

Per collegare una policy della cache a una distribuzione esistente (CLI con file di input)

1. Utilizzare il comando seguente per salvare la configurazione di distribuzione per la distribuzione CloudFront che si desidera aggiornare. Sostituire *`distribution_ID`* con l'ID della distribuzione.

   ```
   aws cloudfront get-distribution-config --id distribution_ID --output yaml >
    dist-config.yaml
   ```

2. Aprire il file `dist-config.yaml` appena creato. Modificare il file, apportando le seguenti modifiche a ogni comportamento della cache che si sta aggiornando per utilizzare una policy della cache.

   - Nel comportamento della cache, aggiungere un campo denominato `CachePolicyId`. Per il valore del campo, utilizzare l'ID della policy della cache annotato dopo la creazione della policy.
   - Rimuovere i campi `MinTTL`, `MaxTTL`, `DefaultTTL` e `ForwardedValues` dal comportamento della cache. Queste impostazioni sono specificate nella policy della cache, pertanto non è possibile includere questi campi e una policy della cache nello stesso comportamento della cache.

- Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare la policy della cache. Sostituire *`distribution_ID`* con l'ID della distribuzione.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Per allegare una policy della cache a una nuova distribuzione (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `distribution.yaml` che contiene tutti i parametri di input per il comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Aprire il file `distribution.yaml` appena creato. Nel comportamento predefinito della cache immettere nel campo `CachePolicyId` l'ID della policy della cache annotato dopo la creazione della policy. Continuare a modificare il file per specificare le impostazioni di distribuzione desiderate, quindi salvare il file al termine.

   Per ulteriori informazioni sulle impostazioni di distribuzione, consulta Riferimento a tutte le impostazioni di distribuzione.
3. Utilizzare il comando seguente per creare la distribuzione utilizzando i parametri di input dal file `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Per creare una policy della cache con l'API CloudFront, utilizzare CreateCachePolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta Informazioni sulle policy della cache e la documentazione di riferimento delle API per l'SDK AWS o altro client API.

Dopo aver creato una policy della cache, è possibile collegarla a un comportamento della cache, utilizzando una delle seguenti chiamate API:

- Per collegarlo a un comportamento della cache in una distribuzione esistente, utilizzare UpdateDistribution.
- Per collegarlo a un comportamento della cache in una nuova distribuzione, utilizzare CreateDistribution.

Per entrambe le chiamate API, fornire l'ID della policy della cache nel campo `CachePolicyId`, all'interno di un comportamento della cache. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione e la documentazione di riferimento delle API per l'SDK AWS o un altro client API.

Utilizzo delle policy della cache gestite

CloudFront fornisce un set di policy della cache gestite che è possibile collegare a qualsiasi comportamento della cache della distribuzione. Con una policy della cache gestita, non è necessario scrivere o gestire policy della cache personalizzate. Le policy gestite utilizzano impostazioni ottimizzate per casi d'uso specifici.

Per utilizzare una policy della cache gestita, è necessario collegarla a un comportamento della cache nella distribuzione. Il processo è lo stesso di quando si crea una policy della cache, ma invece di crearne una nuova, è sufficiente collegare una delle policy della cache gestite. Si allega la policy per nome (con la console) o per ID (con AWS CLI o SDK). I nomi e gli ID sono elencati nella sezione seguente.

Per ulteriori informazioni, consulta Creazione di policy della cache.

Negli argomenti seguenti vengono descritte le policy della cache gestite che è possibile utilizzare.

Argomenti

- Amplify
- CachingDisabled
- CachingOptimized
- CachingOptimizedForUncompressedObjects
- Elemental-MediaPackage

- UseOriginCacheControlHeaders
- UseOriginCacheControlHeaders-QueryStrings

Amplify

Visualizzare questa policy nella console di CloudFront

Questa policy è progettata per l'utilizzo con un'origine che è una Web App AWS Amplify.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`2e54312d-136d-493c-8eb9-b001f22f67d2`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 2 secondi
- TTL massimo = 600 secondi (10 minuti)
- TTL di default = 2 secondi
- Intestazioni incluse nella chiave cache:
  - `Authorization`
  - `CloudFront-Viewer-Country`
  - `Host`

  Viene inclusa anche l'intestazione `Accept-Encoding` normalizzata perché l'impostazione degli oggetti compressi della cache è abilitata. Per ulteriori informazioni, consulta Supporto della compressione.
- Cookie inclusi nella chiave cache: tutti i cookie sono inclusi.
- Stringhe di query incluse nella chiave cache: tutte le stringhe di query sono incluse.
- Impostazione cache oggetti compressi: Abilitata. Per ulteriori informazioni, consulta Supporto della compressione.

> **Warning**
>
> Poiché questa policy dispone di un TTL minimo maggiore di 0, CloudFront memorizzerà nella cache il contenuto almeno per la durata specificata nel TTL minimo della policy della cache,

anche se le direttive `Cache-Control: no-cache`, `no-store` o `private` sono presenti nelle intestazioni di origine.

Policy di cache di Hosting AWS Amplify

Amplify utilizza le seguenti policy della cache gestite per ottimizzare la configurazione della cache predefinita per le applicazioni dei clienti:

- Amplify-Default
- Amplify-DefaultNoCookies
- Amplify-ImageOptimization
- Amplify-StaticContent

> **Note**
>
> Queste policy sono utilizzate solo da Amplify. Si sconsiglia di utilizzare queste policy per le distribuzioni.

Per ulteriori informazioni sulla gestione della configurazione della cache per l'applicazione ospitata su Amplify, consulta Gestione della configurazione della cache nella Guida per l'utente di Amplify Hosting.

CachingDisabled

Visualizzare questa policy nella console di CloudFront

Questa policy disabilita la memorizzazione nella cache. Questa policy è utile per il contenuto dinamico e per le richieste che non sono memorizzabili nella cache.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`4135ea2d-6df8-44a3-9df3-4b5a84be39ad`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 0 secondi

- TTL massimo = 0 secondi
- TTL di default = 0 secondi
- Intestazioni incluse nella chiave cache: nessuna
- Cookie inclusi nella chiave cache: nessuno
- Stringhe di query incluse nella chiave della cache: nessuna
- Impostazione cache degli oggetti compressi: disabilitata

CachingOptimized

Visualizzare questa policy nella console di CloudFront

Questa policy è progettata per ottimizzare l'efficienza della cache riducendo al minimo i valori inclusi da CloudFront nella chiave cache. CloudFront non include alcuna stringa di query o cookie nella chiave della cache e include solo l'intestazione `Accept-Encoding` normalizzata. Ciò consente a CloudFront di memorizzare separatamente nella cache gli oggetti nei formati di compressione Gzip e Brotli quando l'origine li restituisce o quando la Compressione edge CloudFront è abilitata.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`658327ea-f89d-4fab-a63d-7e88639e58f6`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 1 secondo
- TTL massimo = 31.536.000 secondi (365 giorni).
- TTL di default = 86.400 secondi (24 ore).
- Intestazioni incluse nella chiave della cache: nessuna è esplicitamente inclusa. L'intestazione `Accept-Encoding` normalizzata viene inclusa perché l'impostazione degli oggetti compressi della cache è abilitata. Per ulteriori informazioni, consulta Supporto della compressione.
- Cookie inclusi nella chiave cache: nessuno.
- Stringhe di query incluse nella chiave della cache: nessuna.
- Impostazione cache oggetti compressi: Abilitata. Per ulteriori informazioni, consulta Supporto della compressione.

> **Warning**
>
> Poiché questa policy dispone di un TTL minimo maggiore di 0, CloudFront memorizzerà nella cache il contenuto almeno per la durata specificata nel TTL minimo della policy della cache, anche se le direttive `Cache-Control: no-cache`, `no-store` o `private` sono presenti nelle intestazioni di origine.

CachingOptimizedForUncompressedObjects

Visualizzare questa policy nella console di CloudFront

Questa policy è progettata per ottimizzare l'efficienza della cache riducendo al minimo i valori inclusi nella chiave cache. Non sono incluse stringhe di query, intestazioni o cookie. Questa policy è identica a quella precedente, ma disabilita l'impostazione degli oggetti compressi nella cache.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`b2884449-e4de-46a7-ac36-70bc7f1ddd6d`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 1 secondo
- TTL massimo = 31.536.000 secondi (365 giorni)
- TTL di default = 86.400 secondi (24 ore)
- Intestazioni incluse nella chiave cache: nessuna
- Cookie inclusi nella chiave cache: nessuno
- Stringhe di query incluse nella chiave della cache: nessuna
- Impostazione cache degli oggetti compressi: disabilitata

> **Warning**
>
> Poiché questa policy dispone di un TTL minimo maggiore di 0, CloudFront memorizzerà nella cache il contenuto almeno per la durata specificata nel TTL minimo della policy della cache, anche se le direttive `Cache-Control: no-cache`, `no-store` o `private` sono presenti nelle intestazioni di origine.

Elemental-MediaPackage

Visualizzare questa policy nella console di CloudFront

Questo criterio è progettato per l'utilizzo con un'origine che è un endpoint AWS Elemental MediaPackage.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`08627262-05a9-4f76-9ded-b50ca2e3a84f`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 0 secondi
- TTL massimo = 31.536.000 secondi (365 giorni)
- TTL di default = 86.400 secondi (24 ore)
- Intestazioni incluse nella chiave cache:
  - `Origin`

  Viene inclusa anche l'intestazione `Accept-Encoding` normalizzata perché l'impostazione degli oggetti compressi della cache è abilitata per Gzip. Per ulteriori informazioni, consulta Supporto della compressione.
- Cookie inclusi nella chiave cache: nessuno
- Stringhe di query incluse nella chiave della cache:
  - `aws.manifestfilter`
  - `start`
  - `end`
  - `m`
- Impostazione cache oggetti compressi: abilitata per Gzip. Per ulteriori informazioni, consulta Supporto della compressione.

UseOriginCacheControlHeaders

Visualizzare questa policy nella console di CloudFront

Questa policy è progettata per essere utilizzata con un'origine che restituisce intestazioni di risposta HTTP `Cache-Control` e non fornisce contenuti diversi in base ai valori presenti nella stringa di

query. Se l'origine fornisce diversi contenuti in base ai valori presenti nella stringa di query, valuta la possibilità di utilizzare UseOriginCacheControlHeaders-QueryStrings.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`83da9c7e-98b4-4e11-a168-04f0df8e2c65`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 0 secondi
- TTL massimo = 31.536.000 secondi (365 giorni)
- TTL di default = 0 secondi
- Intestazioni incluse nella chiave cache:
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  Viene inclusa anche l'intestazione `Accept-Encoding` normalizzata perché l'impostazione degli oggetti compressi della cache è abilitata. Per ulteriori informazioni, consulta Supporto della compressione.
- Cookie inclusi nella chiave della cache: tutti i cookie sono inclusi.
- Stringhe di query incluse nella chiave della cache: nessuna.
- Impostazione cache oggetti compressi: Abilitata. Per ulteriori informazioni, consulta Supporto della compressione.

UseOriginCacheControlHeaders-QueryStrings

Visualizzare questa policy nella console di CloudFront

Questa policy è progettata per essere utilizzata con un'origine che restituisce intestazioni di risposta HTTP `Cache-Control` e fornisce contenuti diversi in base ai valori presenti nella stringa di query. Se l'origine non fornisce contenuti diversi in base ai valori presenti nella stringa di query, valuta la possibilità di utilizzare UseOriginCacheControlHeaders.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`4cc15a8a-d715-48a4-82b8-cc0b614638fe`

Questa policy ha le seguenti impostazioni:

- TTL minimo = 0 secondi
- TTL massimo = 31.536.000 secondi (365 giorni)
- TTL di default = 0 secondi
- Intestazioni incluse nella chiave cache:
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  Viene inclusa anche l'intestazione `Accept-Encoding` normalizzata perché l'impostazione degli oggetti compressi della cache è abilitata. Per ulteriori informazioni, consulta Supporto della compressione.
- Cookie inclusi nella chiave della cache: tutti i cookie sono inclusi.
- Stringhe di query incluse nella chiave della cache: tutte le stringhe di query sono incluse.
- Impostazione cache oggetti compressi: Abilitata. Per ulteriori informazioni, consulta Supporto della compressione.

Comprensione della chiave della cache

La chiave cache determina se una richiesta del visualizzatore a una edge location CloudFront genera una occorrenza della cache. La chiave cache è l'identificatore univoco per un oggetto nella cache. Ogni oggetto nella cache ha una chiave cache univoca.

Un hit della cache si verifica quando una richiesta diel visualizzatore genera la stessa chiave di cache di una richiesta precedente e l'oggetto per tale chiave di cache si trova nella cache della posizione edge ed è valido. In presenza di un'occorrenza nella cache, l'oggetto richiesto viene servito al visualizzatore da una edge location CloudFront, che presenta i seguenti vantaggi:

- Carico ridotto sul server di origine
- Latenza ridotta per il visualizzatore

È possibile ottenere prestazioni migliori dal sito Web o dall'applicazione quando si dispone di un rapporto di hit della cache più elevato (una percentuale maggiore di richieste di visualizzatori che si traducono in un hit della cache). Un modo per migliorare il rapporto di accesso alla cache consiste nell'includere solo i valori minimi necessari nella chiave della cache. Per ulteriori informazioni, consultare le sezioni indicate di seguito.

È possibile modificare i valori (stringhe di query URL, intestazioni HTTP e cookie) nella chiave della cache utilizzando una policy della cache. Puoi anche modificare la chiave della cache utilizzando una funzione Lambda@Edge o una funzione CloudFront su una richiesta visualizzatore. Prima di modificare la chiave della cache, è importante capire come è stata progettata l'applicazione e quando e come potrebbe servire risposte diverse in base alle caratteristiche della richiesta del visualizzatore. Quando un valore nella richiesta del visualizzatore determina la risposta restituita dall'origine, è necessario includere tale valore nella chiave della cache. Ma se includi un valore nella chiave della cache che non influisce sulla risposta restituita dall'origine, potresti finire per memorizzare nella cache oggetti duplicati.

Chiave della cache predefinita

Per impostazione predefinita, la chiave della cache per una distribuzione CloudFront include le seguenti informazioni:

- Il nome di dominio della distribuzione CloudFront (ad esempio, d1111abcdef8.cloudfront.net)
- Il percorso URL dell'oggetto richiesto (ad esempio, `/content/stories/example-story.html`)

> **Note**
>
> Il metodo `OPTIONS` è incluso nella chiave cache per le richieste `OPTIONS`. Ciò significa che le risposte alle richieste `OPTIONS` vengono memorizzate nella cache separatamente dalle risposte alle richieste `GET` e `HEAD`.

Altri valori della richiesta del visualizzatore non sono inclusi nella chiave cache, per impostazione predefinita. Si consideri la seguente richiesta HTTP da un browser 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/
```

Quando una richiesta del visualizzatore come questa arriva in una posizione edge di CloudFront, CloudFront utilizza la chiave cache per determinare se esiste un'occorrenza nella cache. Per impostazione predefinita, solo i seguenti componenti della richiesta sono inclusi nella chiave cache: `/content/stories/example-story.html` e `d111111abcdef8.cloudfront.net`. Se l'oggetto richiesto non è nella cache (una mancata cache), CloudFront invia una richiesta all'origine per ottenere l'oggetto. Dopo aver ottenuto l'oggetto, CloudFront lo restituisce al visualizzatore e lo memorizza nella cache della edge location.

Quando CloudFront riceve un'altra richiesta per lo stesso oggetto, come determinato dalla chiave cache, CloudFront serve immediatamente l'oggetto memorizzato nella cache al visualizzatore, senza inviare una richiesta all'origine. Ad esempio, si consideri la seguente richiesta HTTP che viene dopo la richiesta precedente.

```
            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/
```

Questa richiesta è per lo stesso oggetto della richiesta precedente, ma è diversa dalla richiesta precedente. Ha una stringa di query URL diversa, diverse intestazioni `User-Agent` e `Referer` e un cookie `session_id` diverso. Tuttavia, nessuno di questi valori fa parte della chiave cache per impostazione predefinita, quindi questa seconda richiesta genera un hit della cache.

Personalizzazione della chiave della cache

In alcuni casi, è possibile includere ulteriori informazioni nella chiave della cache, anche se ciò potrebbe comportare un minor numero di accessi della cache. È possibile specificare cosa includere nella chiave della cache utilizzando una policy della cache.

Ad esempio, se il server di origine utilizza l'intestazione `Accept-Language` HTTP nelle richieste del visualizzatore per restituire contenuti diversi in base alla lingua del visualizzatore, è possibile includere questa intestazione nella chiave cache. Quando si esegue questa operazione, CloudFront utilizza questa intestazione per determinare le occorrenze nella cache e include l'intestazione nelle richieste di origine (richieste che CloudFront invia all'origine quando c'è una mancanza di cache).

Una potenziale conseguenza dell'inclusione di valori aggiuntivi nella chiave cache è che CloudFront potrebbe finire per memorizzare nella cache oggetti duplicati a causa della variazione che può verificarsi nelle richieste del visualizzatore. Ad esempio, i visualizzatori potrebbero inviare uno dei seguenti valori per l'intestazione `Accept-Language`:

- `en-US,en`
- `en,en-US`
- `en-US, en`
- `en-US`

Tutti questi valori diversi indicano che la lingua del visualizzatore è l'inglese, ma la variazione può costringere CloudFront a creare la cache dello stesso oggetto più volte. Ciò può ridurre gli accessi della cache e aumentare il numero di richieste di origine. È possibile evitare questa duplicazione non includendo l'intestazione `Accept-Language` nella chiave cache e configurando invece il sito Web o l'applicazione per utilizzare URL diversi per il contenuto in lingue diverse (ad esempio `/en-US/content/stories/example-story.html`).

Per qualsiasi valore specificato che si intende includere nella chiave cache, è necessario assicurarsi di comprendere quante diverse varianti di tale valore potrebbero apparire nelle richieste del visualizzatore. Per alcuni valori di richiesta, raramente ha senso includerli nella chiave della cache. Ad esempio, l'intestazione `User-Agent` può avere migliaia di varianti univoche, quindi in genere non è un buon candidato per l'inclusione nella chiave della cache. I cookie che hanno valori specifici dell'utente o specifici della sessione e sono univoci per migliaia (o addirittura milioni) di richieste non sono buoni candidati per l'inclusione della chiave della cache. Se si includono questi valori nella chiave cache, ogni variazione univoca genera un'altra copia dell'oggetto nella cache. Se queste copie

dell'oggetto non sono univoche o se si finisce con un numero così elevato di oggetti leggermente diversi che ogni oggetto ottiene solo un piccolo numero di hit della cache, è possibile considerare un approccio diverso. È possibile escludere questi valori altamente variabili dalla chiave della cache oppure è possibile contrassegnare gli oggetti come non memorizzabili nella cache.

Prestare attenzione quando si personalizza la chiave della cache. A volte è auspicabile, ma può avere conseguenze indesiderate come la memorizzazione nella cache di oggetti duplicati, l'abbassamento del rapporto di accesso alla cache e l'aumento del numero di richieste di origine. Se il sito Web o l'applicazione di origine deve ricevere determinati valori dalle richieste dei visualizzatori per analisi, telemetria o altri usi, ma questi valori non modificano l'oggetto restituito dall'origine, utilizzare una policy di richiesta origine per includere questi valori nelle richieste di origine ma non includerli nella chiave della cache.

Controllo delle richieste di origine con una policy

Quando una richiesta del visualizzatore a CloudFront genera una mancata cache (l'oggetto richiesto non viene memorizzato nella cache nella edge location), CloudFront invia una richiesta all'origine per recuperare l'oggetto. Questo è chiamata una richiesta di origine. La richiesta di origine include sempre le seguenti informazioni dalla richiesta del visualizzatore:

- Il percorso URL (solo il percorso, senza stringhe di query URL o il nome di dominio)
- Il corpo della richiesta (se ce n'è uno)
- Le intestazioni HTTP che vengono incluse automaticamente da CloudFront in ogni richiesta origine, incluse `Host`, `User-Agent` e `X-Amz-Cf-Id`.

Altre informazioni dalla richiesta del visualizzatore, ad esempio stringhe di query URL, intestazioni HTTP e cookie, non sono incluse nella richiesta di origine per impostazione predefinita. (Eccezione: con le impostazioni della cache legacy, CloudFront inoltra le intestazioni all'origine per impostazione predefinita.) Tuttavia, potresti voler ricevere alcune di queste altre informazioni all'origine, ad esempio per raccogliere dati per analisi o telemetria. È possibile utilizzare una policy di richiesta origine per controllare le informazioni incluse in una richiesta di origine.

Le policy di richiesta origine sono separate dalle policy della cache, che controllano la chiave della cache. In questo modo, è possibile ricevere informazioni aggiuntive all'origine e di mantenere anche una buona percentuale di riscontri nella cache (la percentuale di richieste visualizzatore che si traducono in un riscontro nella cache). È possibile eseguire questa operazione controllando separatamente quali informazioni sono incluse nelle richieste di origine (utilizzando la policy di richiesta origine) e quali sono incluse nella chiave cache (utilizzando la policy della cache).

Sebbene i due tipi di policy siano separati, sono correlati. Tutte le stringhe di query URL, le intestazioni HTTP e i cookie inclusi nella chiave della cache (utilizzando una policy della cache) vengono automaticamente inclusi nelle richieste di origine. Utilizzare la policy di richiesta origine per specificare le informazioni che si desidera includere nelle richieste di origine, ma non includere nella chiave cache. Proprio come una policy della cache, si collega una policy di richiesta di origine a uno o più comportamenti della cache in una distribuzione CloudFront.

Inoltre, è possibile utilizzare una policy di richiesta origine per aggiungere ulteriori intestazioni HTTP a una richiesta di origine che non sono state incluse nella richiesta del visualizzatore. Queste intestazioni aggiuntive vengono aggiunte da CloudFront prima di inviare la richiesta di origine, con i valori di intestazione che vengono determinati automaticamente in base alla richiesta del

visualizzatore. Per ulteriori informazioni, consulta the section called “Aggiunta di intestazioni della richiesta CloudFront”.

Argomenti

Comprendere le policy relative alle richieste di origine

CloudFront fornisce alcune policy di richiesta di origine predefinite, note come policy gestite, per i casi di utilizzo comuni. È possibile utilizzare queste policy gestite oppure creare policy di richiesta di origine specifiche per le proprie esigenze. Per ulteriori informazioni sulle policy gestite, consulta Utilizzo delle policy di richiesta origine gestite.

Una policy di richiesta origine contiene le seguenti impostazioni, che sono categorizzate in informazioni sulle policy e impostazioni della richiesta di origine.

Informazioni sulle policy

Nome

Un nome per identificare la policy della richiesta di origine. Nella console, è possibile utilizzare il nome per collegare la policy di richiesta origine a un comportamento della cache.

Descrizione

Un commento per descrivere la policy della richiesta di origine. Si tratta di un'opzione facoltativa.

Impostazioni richiesta origine

Le impostazioni della richiesta origine specificano i valori nelle richieste del visualizzatore incluse nelle richieste che CloudFront invia all'origine (note come richieste di origine). I valori possono includere stringhe di query URL, intestazioni HTTP e cookie. I valori specificati sono inclusi nelle richieste di origine, ma non sono inclusi nella chiave cache. Per informazioni sul controllo della chiave cache, consulta Controllo della chiave della cache con una policy.

Headers

Le intestazioni HTTP nelle richieste di visualizzatore che CloudFront include nelle richieste di origine. Per le intestazioni puoi scegliere una delle seguenti impostazioni:

- None (Nessuna) - Le intestazioni HTTP nelle richieste del visualizzatore non sono incluse nelle richieste di origine.
- All viewer headers (Tutte le intestazioni del visualizzatore) - Tutte le intestazioni HTTP nelle richieste del visualizzatore sono incluse nelle richieste di origine.
- Tutte le intestazioni dei visualizzatori e le seguenti intestazioni CloudFront - Tutte le intestazioni HTTP nelle richieste dei visualizzatori sono incluse nelle richieste di origine. Inoltre, è possibile specificare quale delle intestazioni CloudFront si desidera aggiungere alle richieste di origine. Per ulteriori informazioni sulle intestazioni CloudFront, consulta the section called “Aggiunta di intestazioni della richiesta CloudFront”.
- Includere le intestazioni seguenti - Specificare quali intestazioni HTTP sono incluse nelle richieste di origine.

> **Note**
>
> Non specificare un'intestazione già inclusa nelle impostazioni Intestazioni personalizzate origine. Per ulteriori informazioni, consulta Configurazione di CloudFront per aggiungere intestazioni personalizzate alle richieste origine.

- Tutte le intestazioni visualizzatore eccetto – Vengono specificate quali intestazioni HTTP non sono incluse nelle richieste origine. Tutte le altre intestazioni HTTP nelle richieste visualizzatore, tranne quelle specificate, sono incluse.

Quando si utilizza l'impostazione Tutte le intestazioni del visualizzatore e le intestazioni CloudFront seguenti, Includere le seguenti intestazioni o Tutte le intestazioni del visualizzatore tranne, le intestazioni HTTP vengono specificate in base al nome e non al valore. CloudFront include l'intestazione completa, compreso il suo valore, nelle richieste origine.

> **Note**
>
> Quando si utilizza l’impostazione Tutte le intestazioni del visualizzatore eccetto per rimuovere l'intestazione `Host` del visualizzatore, CloudFront aggiunge una nuova intestazione `Host` con il nome di dominio dell'origine alla richiesta origine.

Cookie

I cookie nelle richieste del visualizzatore che CloudFront include nelle richieste di origine. Per i cookie puoi scegliere una delle seguenti impostazioni:

- None (Nessuno) - I cookie nelle richieste del visualizzatore non sono inclusi nelle richieste di origine.
- All (Tutti) - I cookie nelle richieste del visualizzatore sono inclusi nelle richieste di origine.
- Includere i seguenti cookie – Vengono specificati i cookie nelle richieste visualizzatore che vengono inclusi nelle richieste origine.
- Tutti i cookie tranne – Vengono specificati i cookie nelle richieste visualizzatore che non vengono inclusi nelle richieste origine. Tutti gli altri cookie nelle richieste visualizzatore vengono inclusi.

Quando si utilizza l'impostazione Includere i cookie seguenti o Tutti i cookie tranne, i cookie vengono specificati solo in base al loro nome. CloudFront include il cookie completo, compreso il suo valore, nelle richieste origine.

Stringhe di query

Le stringhe di query URL nelle richieste di visualizzatore che CloudFront include nelle richieste di origine. Per le stringhe di query, è possibile scegliere una delle seguenti impostazioni:

- None (Nessuna) - Le stringhe di query nelle richieste del visualizzatore non sono incluse nelle richieste di origine.
- All (Tutte) - Tutte le stringhe di query nelle richieste del visualizzatore sono incluse nelle richieste di origine.
- Includere le seguenti stringhe di query – Vengono specificate le stringhe di query nelle richieste visualizzatore che vengono incluse nelle richieste origine.
- Tutte le stringhe di query eccetto – Vengono specificate le stringhe di query nelle richieste visualizzatore che non vengono incluse nelle richieste origine. Tutte le altre stringhe di query vengono incluse.

Quando si utilizza l'impostazione Includere le seguenti stringhe di query o Tutte le stringhe di query eccetto, le stringhe di query vengono specificate solo in base al loro nome. CloudFront include la stringa di query completa, compreso il suo valore, nelle richieste origine.

Creazione di policy di richiesta origine

È possibile utilizzare una policy di richiesta di origine per controllare i valori (stringhe di query URL, intestazioni HTTP e cookie) inclusi nelle richieste CloudFront inviate all'origine. È possibile creare una policy di richiesta di origine nella console di CloudFront, con l'AWS Command Line Interface (AWS CLI), o con l'API CloudFront.

Dopo aver creato una policy di richiesta di origine, è possibile collegarla a uno o più comportamenti della cache in una distribuzione CloudFront.

Le policy di richiesta origine non sono obbligatorie. Quando a un comportamento della cache non è associata una policy di richiesta origine, la richiesta di origine include tutti i valori specificati nella policy della cache, ma nulla di più.

> **Note**
>
> Per utilizzare una policy di richiesta origine, il comportamento della cache deve utilizzare anche una policy della cache. Non è possibile utilizzare una policy di richiesta origine in un comportamento della cache senza una policy della cache.

Console

Per creare una policy di richiesta origine (console)

1. Accedi alla Console di gestione AWS e apri la pagina Policy nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Scegliere Richiesta origine, quindi scegliere Crea policy richiesta origine.
3. Scegliere l'impostazione desiderata per questa policy di richiesta origine. Per ulteriori informazioni, consulta Comprendere le policy relative alle richieste di origine.
4. Al termine, scegli Create (Crea).

Dopo aver creato una policy di richiesta origine, è possibile collegarla a un comportamento della cache.

Allegare una policy di richiesta origine a una distribuzione esistente (console)

1. Apri la pagina Distribuzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Scegli la distribuzione da aggiornare, quindi scegli la scheda Comportamenti.
3. Scegliere il comportamento della cache da aggiornare, quindi scegliere Modifica.

   In alternativa, per creare un nuovo comportamento della cache, scegliere Crea comportamento.
4. Per la Chiave di cache e richiesta di origine, assicurarsi che sia scelto Policy di cache e policy di richiesta origine.
5. Per Policy richiesta origine, scegliere la policy di richiesta origine da associare a questo comportamento della cache.
6. Scegli Save changes (Salva modifiche) nella parte inferiore della pagina.

Allegare una policy di richiesta origine a una nuova distribuzione (console)

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere Create Distribution (Crea distribuzione).
3. Per la Chiave di cache e richiesta di origine, assicurarsi che sia scelto Policy di cache e policy di richiesta origine.
4. Per Origin request policy (Policy di richiesta di origine), scegliere la policy di richiesta di origine da associare al comportamento predefinito della cache di questa distribuzione.
5. Scegliere le impostazioni desiderate per l'origine, il comportamento predefinito della cache e altre impostazioni di distribuzione. Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.
6. Al termine, scegliere Crea distribuzione.

CLI

Per creare una policy di richiesta di origine con l'interfaccia a riga di comando di AWS Command Line Interface (AWS CLI), utilizza il comando aws cloudfront create-origin-request-policy. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare una policy di richiesta origine (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `origin-request-policy.yaml` che contiene tutti i parametri di input per il comando create-origin-request-policy.

```
aws cloudfront create-origin-request-policy --generate-cli-skeleton yaml-input >
 origin-request-policy.yaml
```

2. Aprire il file `origin-request-policy.yaml` appena creato. Modificare il file per specificare le impostazioni delle policy di richiesta origine desiderate, quindi salvare il file. È possibile rimuovere i campi facoltativi dal file, ma non rimuovere i campi obbligatori.

   Per ulteriori informazioni sulle impostazioni delle policy di richiesta di origine, consulta Comprendere le policy relative alle richieste di origine.

3. Utilizzare il comando seguente per creare la policy di richiesta origine utilizzando i parametri di input dal file `origin-request-policy.yaml`.

```
aws cloudfront create-origin-request-policy --cli-input-yaml file://origin-
request-policy.yaml
```

   Prendere nota del valore `Id` nell'output del comando. Questo è l'ID della policy di richiesta di origine ed è necessario per collegare la policy di richiesta di origine al comportamento della cache di una distribuzione CloudFront.

Per allegare una policy di richiesta origine a una distribuzione esistente (CLI con file di input)

1. Utilizzare il comando seguente per salvare la configurazione di distribuzione per la distribuzione CloudFront che si desidera aggiornare. Sostituire *`distribution_ID`* con l'ID della distribuzione.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Aprire il file `dist-config.yaml` appena creato. Modificare il file, apportando le seguenti modifiche a ogni comportamento della cache che si sta aggiornando per utilizzare una policy di richiesta origine.

   - Nel comportamento della cache, aggiungere un campo denominato `OriginRequestPolicyId`. Per il valore del campo, utilizzare l'ID della policy di richiesta di origine annotato dopo aver creato la policy.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare la policy di richiesta origine. Sostituire *`distribution_ID`* con l'ID della distribuzione.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Per allegare una policy di richiesta origine a una nuova distribuzione (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `distribution.yaml` che contiene tutti i parametri di input per il comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Aprire il file `distribution.yaml` appena creato. Nel comportamento predefinito della cache, nel campo `OriginRequestPolicyId`, immettere l'ID della policy della richiesta origine annotato dopo la creazione della policy. Continuare a modificare il file per specificare le impostazioni di distribuzione desiderate, quindi salvare il file al termine.

   Per ulteriori informazioni sulle impostazioni di distribuzione, consulta Riferimento a tutte le impostazioni di distribuzione.

3. Utilizzare il comando seguente per creare la distribuzione utilizzando i parametri di input dal file `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Per creare una policy di richiesta di origine con l'API CloudFront, utilizzare CreateOriginRequestPolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta Comprendere le policy relative alle richieste di origine e la documentazione di riferimento delle API per l'SDK AWS o altro client API.

Dopo aver creato una policy di richiesta origine, è possibile collegarla a un comportamento della cache, utilizzando una delle seguenti chiamate API:

- Per collegarlo a un comportamento della cache in una distribuzione esistente, utilizzare UpdateDistribution.
- Per collegarlo a un comportamento della cache in una nuova distribuzione, utilizzare CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID della policy di richiesta di origine nel campo `OriginRequestPolicyId`, all'interno di un comportamento della cache. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione e la documentazione di riferimento delle API per l'SDK AWS o un altro client API.

Utilizzo delle policy di richiesta origine gestite

CloudFront fornisce un set di policy di richiesta di origine gestite che è possibile collegare a qualsiasi comportamento della cache della distribuzione. Con una policy di richiesta di origine gestita, non è necessario scrivere o gestire le proprie policy di richiesta origine. Le policy gestite utilizzano impostazioni ottimizzate per casi d'uso specifici.

Per utilizzare una policy di richiesta origine gestita, è necessario collegarla a un comportamento della cache nella distribuzione. Il processo è lo stesso di quando si crea una policy di richiesta origine, ma invece di crearne una nuova, è sufficiente allegare una delle policy di richiesta origine gestite. Si allega la policy per nome (con la console) o per ID (con AWS CLI o SDK). I nomi e gli ID sono elencati nella sezione seguente.

Per ulteriori informazioni, consulta Creazione di policy di richiesta origine.

Negli argomenti seguenti vengono descritte le policy di richiesta di origine gestite che è possibile utilizzare.

Argomenti

AllViewer

Visualizzare questa policy nella console di CloudFront

Questa policy include tutti i valori (stringhe di query, intestazioni e cookie) della richiesta visualizzatore.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`216adef6-5c7f-47e4-b989-5492eafa07d3`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine: tutte le intestazioni nella richiesta del visualizzatore
- Cookie inclusi nelle richieste di origine: Tutti
- Stringhe di query incluse nelle richieste di origine: Tutte

AllViewerAndCloudFrontHeaders-2022-06

Visualizzare questa policy nella console di CloudFront

Questa policy include tutti i valori (intestazioni, cookie e stringhe di query) della richiesta visualizzatore e tutte le intestazioni di CloudFront rilasciate fino a giugno 2022 (le intestazioni di CloudFront rilasciate dopo giugno 2022 non sono incluse).

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`33f36d7e-f396-46d9-90e0-52428a34d9dc`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine: tutte le intestazioni nella richiesta del visualizzatore e le seguenti intestazioni di 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`
- Cookie inclusi nelle richieste di origine: Tutti
- Stringhe di query incluse nelle richieste di origine: Tutte

AllViewerExceptHostHeader

Visualizzare questa policy nella console di CloudFront

Questa policy non include l'intestazione `Host` della richiesta visualizzatore, ma include tutti gli altri valori (intestazioni, cookie e stringhe di query) della richiesta visualizzatore.

Questa policy include anche intestazioni di richiesta CloudFront aggiuntive per il protocollo HTTP, la versione HTTP, la versione TLS e tutte le intestazioni relative al tipo di dispositivo e alla posizione del visualizzatore.

Questa policy è pensata per l'utilizzo con Gateway Amazon API e le origini della funzione URL AWS Lambda. Queste origini prevedono che l'intestazione `Host` contenga il nome di dominio di origine, non il nome di dominio della distribuzione CloudFront. L'inoltro dell'intestazione `Host` dalla richiesta visualizzatore a queste origini può impedirne il funzionamento.

> **Note**
>
> Quando utilizzi questa policy di richiesta origine gestita per rimuovere l'intestazione `Host` del visualizzatore, CloudFront aggiunge una nuova intestazione `Host` con il nome di dominio dell'origine alla richiesta origine.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`b689b0a8-53d0-40ab-baf2-68738e2966ac`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste origine: tutte le intestazioni nella richiesta visualizzatore ad eccezione dell'intestazione `Host`
- Cookie inclusi nelle richieste di origine: Tutti
- Stringhe di query incluse nelle richieste di origine: Tutte

CORS-CustomOrigin

Visualizzare questa policy nella console di CloudFront

Questa policy include l'intestazione che abilita le richieste CORS (Cross-Origin Resource Sharing) quando l'origine è un'origine personalizzata.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`59781a5b-3903-41f3-afcb-af62929ccde1`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine:
  - `Origin`
- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Nessuna

CORS-S3Origin

Visualizzare questa policy nella console di CloudFront

Questa policy include le intestazioni che abilitano le richieste CORS (Cross-Origin Resource Sharing) quando l'origine è un bucket Amazon S3.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`88a5eaf4-2fd4-4709-b370-b4c650ea3fcf`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine:
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Nessuna

Elemental-MediaTailor-PersonalizedManifests

Visualizzare questa policy nella console di CloudFront

Questa policy è stata concepita per essere utilizzata con un'origine che è un endpoint AWS Elemental MediaTailor.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`775133bc-15f2-49f9-abea-afb2e0bf67d2`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine:
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
  - `User-Agent`
  - `X-Forwarded-For`
- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Tutte

HostHeaderOnly

Visualizzare questa policy nella console di CloudFront

Questa policy include solo l'intestazione `Host` della richiesta origine. Non include stringhe di query o cookie.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`bf0718e1-ba1e-49d1-88b1-f726733018ae`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste origine: host
- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Nessuna

UserAgentRefererHeaders

Visualizzare questa policy nella console di CloudFront

Questa policy include solo le intestazioni `User-Agent` e `Referer`. Non include stringhe di query o cookie.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`acba4595-bd28-49b8-b9fe-13317c0390fa`

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine:
  - `User-Agent`
  - `Referer`
- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Nessuna

Aggiunta di intestazioni della richiesta CloudFront

È possibile configurare CloudFront per aggiungere intestazioni HTTP specifiche alle richieste ricevute da CloudFront dai visualizzatori e gli inoltri all'origine o alla funzione edge. I valori di queste intestazioni HTTP sono basati sulle caratteristiche del visualizzatore o della richiesta del visualizzatore. Le intestazioni forniscono informazioni relative al tipo di dispositivo, indirizzo IP, posizione geografica, protocollo di richiesta (HTTP o HTTPS), versione HTTP, dettagli della connessione TLS, impronta JA3 e impronta JA4 del visualizzatore. Puoi anche configurare il comportamento della cache della distribuzione per inoltrare intestazioni WebSocket. Per ulteriori informazioni, consulta Utilizzare WebSockets con le distribuzioni CloudFront.

Con queste intestazioni, l'origine o la funzione edge può ricevere informazioni sul visualizzatore senza la necessità da parte dell'utente di scrivere il proprio codice per determinare tali informazioni. Se l'origine restituisce risposte diverse in base alle informazioni contenute in queste intestazioni, è possibile includerle nella chiave cache in modo che le risposte vengano memorizzate nella cache di CloudFront separatamente. Ad esempio, l'origine potrebbe rispondere con contenuti in una lingua specifica in base al paese in cui si trova il visualizzatore o con contenuti personalizzati per un tipo di dispositivo specifico. L'origine potrebbe anche scrivere queste intestazioni nei file di registro, che è possibile utilizzare per determinare le informazioni su dove si trovano i visualizzatori, quali tipi di dispositivi utilizzano e altro ancora.

Se si desidera includere intestazioni nella chiave della cache, utilizzare una policy della cache. Per ulteriori informazioni, consulta Controllo della chiave della cache con una policy e the section called “Comprensione della chiave della cache”.

Per ricevere queste intestazioni alla tua origine, ma non includerle nella chiave cache, utilizzare una policy di richiesta di origine. Per ulteriori informazioni, consulta Controllo delle richieste di origine con una policy.

Argomenti

Intestazioni del tipo di dispositivo

È possibile aggiungere le seguenti intestazioni per determinare il tipo di dispositivo del visualizzatore. In base al valore dell'intestazione `User-Agent`, CloudFront imposta il valore di queste intestazioni su `true` o `false`. Se il dispositivo ricade in più di una categoria, allora più di un valore potrebbe essere `true`. Ad esempio, per alcuni dispositivi tablet, CloudFront imposta `CloudFront-Is-Mobile-Viewer` e `CloudFront-Is-Tablet-Viewer` su `true`.

- `CloudFront-Is-Android-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è un dispositivo con il sistema operativo Android.
- `CloudFront-Is-Desktop-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è un dispositivo desktop.
- `CloudFront-Is-IOS-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è un dispositivo con un sistema operativo mobile Apple, come iPhone, iPod touch e alcuni dispositivi iPad.
- `CloudFront-Is-Mobile-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è un dispositivo mobile.
- `CloudFront-Is-SmartTV-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è una smart TV.
- `CloudFront-Is-Tablet-Viewer` - Impostare su `true` quando CloudFront stabilisce che il visualizzatore è un tablet.

Intestazioni di posizione del visualizzatore

È possibile aggiungere le seguenti intestazioni per stabilire la posizione del visualizzatore. CloudFront determina i valori per queste intestazioni in base all'indirizzo IP del visualizzatore. Per i caratteri non ASCII nei valori delle intestazioni, CloudFront codifica in percentuale i caratteri in base alla sezione 1.2 della RFC 3986.

- `CloudFront-Viewer-Address` - Contiene l'indirizzo IP del visualizzatore e la porta di origine della richiesta. Ad esempio, un valore di intestazione di `198.51.100.10:46532` significa che l'indirizzo IP del visualizzatore è 198.51.100.10 e la porta di origine della richiesta è 46532.
- `CloudFront-Viewer-ASN` - Contiene il numero di sistema autonomo (ASN) del visualizzatore.

> **Note**
>
> È possibile aggiungere `CloudFront-Viewer-Address` e `CloudFront-Viewer-ASN` in una policy di richiesta di origine, ma non in una policy della cache.

- `CloudFront-Viewer-Country` - Contiene il codice paese di due lettere per il Paese del visualizzatore. Per un elenco dei codici paese, vedere ISO 3166-1 alpha-2.
- `CloudFront-Viewer-City` - Contiene il nome della città del visualizzatore.

Quando aggiungi le seguenti intestazioni, CloudFront le applica a tutte le richieste, eccetto quelle che hanno origine dal network AWS:

- `CloudFront-Viewer-Country-Name` - Contiene il nome del Paese del visualizzatore.
- `CloudFront-Viewer-Country-Region` - Contiene un codice (fino a tre caratteri) che rappresenta la regione del visualizzatore. La regione è la suddivisione di primo livello (la più ampia o meno specifica) del codice ISO 3166-2.
- `CloudFront-Viewer-Country-Region-Name` - Contiene il nome della regione del visualizzatore. La regione è la suddivisione di primo livello (la più ampia o meno specifica) del codice ISO 3166-2.
- `CloudFront-Viewer-Latitude` - Contiene la latitudine approssimativa del visualizzatore.
- `CloudFront-Viewer-Longitude` - Contiene la longitudine approssimativa del visualizzatore.
- `CloudFront-Viewer-Metro-Code` - Contiene il codice metro del visualizzatore. Questo è presente solo quando il visualizzatore è negli Stati Uniti.
- `CloudFront-Viewer-Postal-Code` - Contiene il codice postale del visualizzatore.

- `CloudFront-Viewer-Time-Zone` Contiene il fuso orario del visualizzatore, in formato database del fuso orario IANA (ad esempio, `America/Los_Angeles`).

> **Note**
>
> `CloudFront-Viewer-City`, `CloudFront-Viewer-Metro-Code` e `CloudFront-Viewer-Postal-Code` potrebbero non essere disponibili per ogni indirizzo IP. Alcuni indirizzi IP non possono essere geolocalizzati con sufficiente precisione per ottenere tali informazioni.

Intestazioni per determinare la struttura dell'intestazione del visualizzatore

È possibile aggiungere le seguenti intestazioni per identificare il visualizzatore in base alle intestazioni che invia. Ad esempio, browser diversi possono inviare le intestazioni HTTP in un determinato ordine. Se il browser specificato nell'intestazione `User-Agent` non corrisponde all'ordine di intestazione previsto per quel browser, è possibile rifiutare la richiesta. Inoltre, se il valore `CloudFront-Viewer-Header-Count` non corrisponde al numero di intestazioni in `CloudFront-Viewer-Header-Order`, è possibile rifiutare la richiesta.

- `CloudFront-Viewer-Header-Order`: contiene i nomi delle intestazioni del visualizzatore nell'ordine richiesto, separati dai due punti. Ad esempio: `CloudFront-Viewer-Header-Order: Host:User-Agent:Accept:Accept-Encoding`. Le intestazioni oltre il limite di 7.680 caratteri vengono troncate.
- `CloudFront-Viewer-Header-Count`: contiene il numero totale delle intestazioni del visualizzatore.

Intestazioni relative a TLS

Puoi aggiungere le seguenti intestazioni per determinare l'impronta JA3, l'impronta JA4 e i dettagli della connessione TLS del visualizzatore:

- `CloudFront-Viewer-JA3-Fingerprint`: contiene l'impronta JA3 del visualizzatore. L'impronta JA3 può aiutare a determinare se la richiesta proviene da un client noto, se si tratta di malware o bot dannoso o di un'applicazione prevista (presente nell'elenco di quelle consentite).

- `CloudFront-Viewer-JA4-Fingerprint`: contiene l'impronta JA4 del visualizzatore. Analogamente all'impronta JA3, l'impronta JA4 può aiutare a determinare se la richiesta proviene da un client noto, se si tratta di malware o bot dannoso o di un'applicazione prevista (presente nell'elenco di quelle consentite). Puoi utilizzare l'impronta per creare un database di utenti buoni o malintenzionati noti da utilizzare durante l'ispezione delle richieste HTTP. Puoi quindi controllare il valore dell'intestazione sui server web delle applicazioni o in Lambda@Edge e Funzioni CloudFront per confrontare il valore dell'intestazione con un elenco di impronte di malware conosciute per bloccare i client dannosi.
- `CloudFront-Viewer-TLS` – Contiene la versione SSL/TLS, il cifrario e le informazioni sull'handshake SSL/TLS utilizzato per la connessione tra il visualizzatore e CloudFront. Il valore dell'intestazione è nel seguente formato:

  ```
  SSL/TLS_version:cipher:handshake_information
  ```

  Per *`handshake_information`*, l'intestazione può contenere uno dei seguenti valori:

  - `fullHandshake` — È stato eseguito un handshake completo per la sessione SSL/TLS.
  - `sessionResumed` — Una precedente sessione SSL/TLS è stata ripresa.
  - `connectionReused` — Una precedente connessione SSL/TLS è stata riutilizzata.

  Di seguito sono riportati alcuni valori di esempio per questa intestazione:

  ```
  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
  ```

  Per l'elenco completo delle possibili versioni e cifrature SSL/TLS che possono essere presenti in questo valore di intestazione, consulta the section called "Protocolli e cifrari supportati tra visualizzatori e CloudFront".

> **Note**
>
> - Le impronte digitali JA3 e JA4 derivano dal pacchetto `Client Hello` SSL/TLS. Sono presenti solo per le richieste HTTPS.
> - Per queste intestazioni correlate a TLS, puoi aggiungerle a una policy di richiesta di origine, ma non a una policy della cache.

Altre intestazioni CloudFront

Puoi aggiungere le seguenti intestazioni per determinare l'URI della richiesta originale del visualizzatore, i parametri e i valori della stringa di query della richiesta originale, il protocollo e la versione:

- `CloudFront-Error-Uri`: contiene l'URI della richiesta originale ricevuto dal visualizzatore.
- `CloudFront-Error-Args`: contiene i parametri e i valori della stringa di query della richiesta originale.
- `CloudFront-Forwarded-Proto` - Contiene il protocollo della richiesta del visualizzatore (HTTP o HTTPS).
- `CloudFront-Viewer-Http-Version` - Contiene la versione HTTP della richiesta del visualizzatore.

Comprendere come interagiscono le policy di richiesta origine e le policy della cache

Puoi utilizzare una policy di richiesta origine CloudFront per controllare le richieste inviate da CloudFront all'origine, chiamate richieste origine. Per utilizzare una policy di richiesta origine, devi collegare una policy della cache allo stesso comportamento della cache. Non è possibile utilizzare una policy di richiesta origine in un comportamento della cache senza una policy della cache. Per ulteriori informazioni, consulta Controllo delle richieste di origine con una policy.

Le policy di richiesta origine e le policy della cache interagiscono per determinare i valori che vengono inclusi da CloudFront nelle richieste origine. Tutte le stringhe di query URL, le intestazioni HTTP e i cookie specificati nella chiave della cache (utilizzando una policy della cache) vengono automaticamente inclusi nelle richieste origine. Anche tutte le stringhe di query, le intestazioni e i

cookie aggiuntivi specificati in una policy di richiesta origine vengono inclusi nelle richieste origine (ma non nella chiave di cache).

Le policy di richiesta origine e le policy della cache dispongono di impostazioni che potrebbero sembrare in conflitto tra loro. Ad esempio, una policy potrebbe consentire determinati valori mentre un'altra policy li blocca. Nella tabella seguente viene descritto quali valori vengono inclusi da CloudFront nelle richieste origine quando si utilizzano insieme le impostazioni di una policy di richiesta origine e una policy della cache. Queste impostazioni si applicano in genere a tutti i tipi di valori (stringhe di query, intestazioni e cookie), con la differenza che non è possibile specificare tutte le intestazioni o utilizzare un elenco di blocchi di intestazioni in una policy della cache.

	Policy di richiesta origine			
	Nessuno	Tutti	Elenco di indirizzi consentiti	Elenco di indirizzi bloccati
Policy della cache				
Nessuno	Nessun valore della richiesta visualizzatore viene incluso nella richiesta origine, ad eccezione dei valori predefiniti inclusi in ogni richiesta origine. Per ulteriori informazioni, consulta Controllo delle richieste di origine con una policy.	Tutti i valori della richiesta visualizzatore sono inclusi nella richiesta origine.	Solo i valori specificati nella policy di richiesta origine sono inclusi nella richiesta origine.	Tutti i valori della richiesta visualizzatore ad eccezione di quelli specificati nella policy di richiesta origine sono inclusi nella richiesta origine.

	Policy di richiesta origine			
	Nessuno	Tutti	Elenco di indirizzi consentiti	Elenco di indirizzi bloccati
Tutti Nota: non è possibile specificare tutte le intestazioni in una policy della cache.	Tutte le stringhe di query e i cookie della richiesta visualizzatore vengono inclusi nella richiesta origine.	Tutti i valori della richiesta visualizzatore sono inclusi nella richiesta origine.	Tutte le stringhe di query e i cookie della richiesta visualizzatore, e le eventuali intestazioni specificate nella policy di richiesta origine, sono inclusi nella richiesta origine.	Tutte le stringhe di query e i cookie della richiesta visualizzatore sono inclusi nella richiesta origine, anche quelli specificati nell'elenco di indirizzi bloccati della policy di richiesta origine. L'impostazione della policy della cache sostituisce l'elenco di indirizzi bloccati della policy di richiesta origine.

	Policy di richiesta origine			
	Nessuno	Tutti	Elenco di indirizzi consentiti	Elenco di indirizzi bloccati
Elenco di indirizzi consentiti	Solo i valori specificati della richiesta visualizzatore vengono inclusi nella richiesta origine.	Tutti i valori della richiesta visualizzatore sono inclusi nella richiesta origine.	Tutti i valori specificati nella policy della cache o nella policy della richiesta origine sono inclusi nella richiesta origine.	I valori specificati nella policy della cache sono inclusi nella richiesta origine, anche se gli stessi valori sono specificati nell'elenco di indirizzi bloccati della policy di richiesta origine. L’elenco di indirizzi consentiti della policy della cache sostituisce l'elenco di indirizzi bloccati della policy di richiesta origine.

	Policy di richiesta origine			
	Nessuno	Tutti	Elenco di indirizzi consentiti	Elenco di indirizzi bloccati
Elenco di indirizzi bloccati Nota: non è possibile specificare intestazioni in un elenco di indirizzi bloccati della policy della cache.	Tutte le stringhe di query e i cookie della richiesta visualizzatore, ad eccezione di quelli specificati, vengono inclusi nella richiesta origine.	Tutti i valori della richiesta visualizzatore sono inclusi nella richiesta origine.	I valori specificati nella policy di richiesta origine sono inclusi nella richiesta origine, anche se gli stessi valori sono specificati nell'elenco di indirizzi bloccati della policy della cache. L’elenco di indirizzi consentiti della policy di richiesta origine sostituisce l'elenco di indirizzi bloccati della policy della cache.	Tutti i valori della richiesta visualizzatore, ad eccezione di quelli specificati nella policy della cache o nella policy di richiesta origine, sono inclusi nella richiesta origine.

Aggiunta o rimozione di intestazioni HTTP in risposte CloudFront con una policy

Puoi configurare CloudFront per modificare le intestazioni HTTP nelle risposte inviate ai visualizzatori (browser web e altri client). CloudFront può rimuovere le intestazioni ricevute dall'origine o aggiungere intestazioni alla risposta, prima di inviare la risposta ai visualizzatori. L'esecuzione di queste modifiche non richiede la scrittura di codice o la modifica dell'origine.

Ad esempio, è possibile rimuovere intestazioni come `X-Powered-By` e `Vary` in modo che CloudFront non le includa nelle risposte che invia ai visualizzatori. In alternativa, puoi aggiungere intestazioni HTTP come le seguenti:

- Un'intestazione `Cache-Control` per controllare il caching del browser.
- Un'intestazione `Access-Control-Allow-Origin` per consentire la condivisione di risorse multiorigine (CORS). È anche possibile aggiungere altre intestazioni CORS.
- Un set di intestazioni di sicurezza comuni, ad esempio `Strict-Transport-Security`, `Content-Security-Policy` e `X-Frame-Options`.
- Un'intestazione `Server-Timing` per visualizzare le informazioni relative alle prestazioni e al routing della richiesta e della risposta tramite CloudFront.

Per specificare le intestazioni che CloudFront aggiunge o rimuove alle risposte HTTP, è necessario utilizzare una policy delle intestazioni di risposta. Collegare una policy delle intestazioni di risposta a uno o più comportamenti della cache. CloudFront modifica le intestazioni nelle risposte HTTP che invia per le richieste corrispondenti a un comportamento della cache. CloudFront modifica le intestazioni alle risposte che CloudFront serve dalla cache e quelle che CloudFront inoltra dall'origine. Se la risposta di origine include una o più intestazioni presenti in una policy delle intestazioni di risposta, la policy può specificare se CloudFront utilizza l'intestazione ricevuta dall'origine o la sovrascrive con quella della policy delle intestazioni di risposta.

> **Note**
>
> Se aggiungi intestazioni che controllano il caching del browser alle policy delle intestazioni di risposta, ad esempio `Cache-Control`, CloudFront aggiunge queste intestazioni solo alla risposta visualizzatore. Queste intestazioni non influiscono sul modo in cui CloudFront memorizza nella cache l'oggetto richiesto.

CloudFront fornisce policy delle intestazioni di risposta predefinite, note come policy gestite, per casi d'uso comuni. È possibile utilizzare queste policy gestite oppure creare policy specifiche per le proprie esigenze. Puoi collegare una singola policy delle intestazioni di risposta a più comportamenti della cache in più distribuzioni nella tua Account AWS.

Per ulteriori informazioni, consulta gli argomenti seguenti:

Argomenti

Comprendere le policy delle intestazioni di risposta

È possibile utilizzare una policy delle intestazioni di risposta per specificare le intestazioni HTTP che Amazon CloudFront rimuove o aggiunge alle risposte inviate ai visualizzatori. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perchè utilizzarle, consulta Aggiunta o rimozione di intestazioni delle risposte con una policy.

Nei seguenti argomenti vengono illustrate le impostazioni di una policy delle intestazioni di risposta. Le impostazioni sono raggruppate in categorie, che sono rappresentate nei seguenti argomenti.

Argomenti

Dettagli della policy (metadati)

Le impostazioni dei dettagli della policy contengono metadati relativi a una policy delle intestazioni di risposta.

- Nome – Un nome per identificare la policy delle intestazioni di risposta. Nella console, è possibile utilizzare il nome per collegare la policy a un comportamento della cache.
- Descrizione (facoltativo) – Un commento per descrivere la policy delle intestazioni di risposta. Questo è facoltativo, ma può aiutare a identificare lo scopo della policy.

Intestazioni CORS

Le impostazioni CORS (Cross-Origin Resource Sharing) consentono di aggiungere e configurare le intestazioni CORS in una policy delle intestazioni di risposta.

Questo elenco si concentra su come specificare le impostazioni e i valori validi in una policy delle intestazioni di risposta. Per ulteriori informazioni su ciascuna di queste intestazioni e su come vengono utilizzate per richieste e risposte CORS reali, vedere condivisione di risorse multiorigine nei documenti Web MDN e nelle Specifiche del protocollo CORS.

Access-Control-Allow-Credentials

Questa è un'impostazione booleana (`true` o `false`) che determina se CloudFront aggiunge o meno l'intestazione `Access-Control-Allow-Credentials` nelle risposte alle richieste CORS. Quando questa impostazione è `true`, CloudFront aggiunge l'intestazione `Access-Control-Allow-Credentials: true` nelle risposte alle richieste CORS. Altrimenti CloudFront non aggiunge questa intestazione alle risposte.

Access-Control-Allow-Headers

Specifica i nomi di intestazione utilizzati da CloudFront come valori per l'intestazione `Access-Control-Allow-Headers` nelle risposte alle richieste di verifica preliminare CORS. I valori validi per questa impostazione includono i nomi delle intestazioni HTTP o il carattere jolly (*), che indica che sono consentite tutte le intestazioni.

> **Note**
>
> L'intestazione `Authorization` non può utilizzare un carattere jolly e deve essere elencata in modo esplicito.

Esempi di uso valido del carattere jolly

Esempio	Corrisponderà	Non corrisponderà
`x-amz-*`	`x-amz-test` `x-amz-`	`x-amz`
`x-*-amz`	`x-test-amz` `x--amz`	
`*`	Tutte le intestazioni tranne `Authorization`	`Authorization`

Access-Control-Allow-Methods

Specifica i metodi HTTP utilizzati da CloudFront come valori per l'intestazione `Access-Control-Allow-Methods` nelle risposte alle richieste di verifica preliminare CORS. I valori validi includono `GET`, `DELETE`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT` oppure `ALL`. `ALL` è un valore speciale che include tutti i metodi HTTP elencati.

Access-Control-Allow-Origin

Specifica i valori che CloudFront può utilizzare nell'intestazione di risposta `Access-Control-Allow-Origin`. I valori validi per questa impostazione includono un'origine specifica (ad esempio `http://www.example.com`) o il carattere jolly (`*`) che indica che sono consentite tutte le origini.

> **Note**
>
> - Il carattere jolly (`*`) è consentito come sottodominio più a sinistra (`*.example.org`).
> - Il carattere jolly (`*`) non è consentito nelle seguenti posizioni:
>   - Domini di primo livello (`example.*`)
>   - A destra dei sottodomini (`test.*.example.org`) o all'interno di qualsiasi sottodominio (`*test.example.org`)
>   - All'interno dei termini (`exa*mple.org`))

Per alcuni esempi di utilizzo del carattere jolly, consulta la tabella seguente.

Esempio	Corrisponderà	Non corrisponderà

`http://*.example.org`	`http://www.example.org`
	
	`http://test.example.org`
		`https``://test.example.org`
		
		`https``://test.example.org:123`
		
		`http://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`	

`http://example.org:1*3`	`http://example.org:123`	

Esempio	Corrisponderà	Non corrisponderà

	`http://example.org:1893`
	
	`http://example.org:13`	

`*.example.org:1*`	`test.example.org:123`	

Access-Control-Expose-Headers

Specifica i nomi di intestazione utilizzati da CloudFront come valori per l'intestazione `Access-Control-Expose-Headers` nelle risposte alle richieste CORS. I valori validi per questa impostazione includono i nomi delle intestazioni HTTP o il carattere jolly (`*`).

Access-Control-Max-Age

Un certo numero di secondi, che CloudFront utilizza come valore per l'intestazione `Access-Control-Max-Age` nelle risposte alle richieste di verifica preliminare CORS.

Sostituzione dell'origine

Un'impostazione booleana che determina il comportamento di CloudFront quando la risposta dall'origine contiene una delle intestazioni CORS presenti anche nella policy.

- Quando è impostata su `true` e la risposta origine contiene un'intestazione CORS che si trova anche nella policy, CloudFront aggiunge l'intestazione CORS nella policy alla risposta. CloudFront invia quindi la risposta al visualizzatore. CloudFront ignora l'intestazione ricevuta dall'origine.
- Quando è impostata su `false` e la risposta origine contiene un'intestazione CORS (a prescindere che l'intestazione CORS sia presente nella policy), CloudFront include nella risposta l'intestazione CORS ricevuta dall'origine. CloudFront non aggiunge alcuna intestazione CORS nella policy alla risposta inviata al visualizzatore.

Intestazioni di sicurezza

Le impostazioni delle intestazioni di sicurezza consentono di aggiungere e configurare diverse intestazioni di risposta HTTP correlate alla sicurezza in una policy delle intestazioni di risposta.

Questo elenco si concentra su come specificare l'impostazione e i valori validi in una policy delle intestazioni di risposta. Per ulteriori informazioni su ciascuna di queste intestazioni e su come vengono utilizzate nelle risposte HTTP reali, vedere i collegamenti ai documenti Web MDN.

Content-Security-Policy

Specifica le direttive della policy di sicurezza dei contenuti che CloudFront utilizza come valori per l'intestazione della risposta `Content-Security-Policy`.

Per ulteriori informazioni su questa intestazione e sulle direttive di policy valide, consulta Content-Security-Policy nei documenti Web MDN.

> **Note**
>
> Il valore dell'intestazione `Content-Security-Policy` è limitato a 1783 caratteri.

Referrer-Policy

Specifica la direttiva della policy sui criteri di riferimento che CloudFront utilizza come valore per l'intestazione della risposta `Referrer-Policy`. I valori validi per questa impostazione sono: `no-referrer`, `no-referrer-when-downgrade`, `origin`, `origin-when-cross-origin`, `same-origin`, `strict-origin`, `strict-origin-when-cross-origin` oppure `unsafe-url`.

Per ulteriori informazioni su questa intestazione e su queste direttive, consulta Referrer-Policy nei documenti Web MDN.

Strict-Transport-Security

Specifica le direttive e le impostazioni utilizzate da CloudFront come valore per l'intestazione della risposta `Strict-Transport-Security`. Per questa impostazione, è necessario specificare separatamente:

- Un certo numero di secondi, che CloudFront utilizza come valore per questa direttiva di intestazione `max-age`
- Un'impostazione booleana (`true` o `false`) per `preload`, che determina se CloudFront include la direttiva `preload` nel valore di questa intestazione
- Un'impostazione booleana (`true` o `false`) per `includeSubDomains`, che determina se CloudFront include la direttiva `includeSubDomains` nel valore di questa intestazione

Per ulteriori informazioni su questa intestazione e su queste direttive, consulta Strict-Transport-Security nei documenti Web MDN.

X-Content-Type-Options

Questa è un'impostazione booleana (`true` o `false`) che determina se CloudFront aggiunge o meno l'intestazione `X-Content-Type-Options` alle risposte. Quando questa impostazione è `true`, CloudFront aggiunge l'intestazione `X-Content-Type-Options: nosniff` alle risposte. In caso contrario, CloudFront non aggiunge questa intestazione.

Per ulteriori informazioni su questa intestazione, consulta X-Content-Type-Options nei documenti Web MDN.

X-Frame-Options

Specifica la direttiva che CloudFront utilizza come valore per l'intestazione della risposta `X-Frame-Options`. I valori validi per questa impostazione sono `DENY` o `SAMEORIGIN`.

Per ulteriori informazioni su questa intestazione e su queste direttive, consulta X-Frame-Options nei documenti Web MDN.

X-XSS-Protection

Specifica le direttive e le impostazioni utilizzate da CloudFront come valore per l'intestazione della risposta `X-XSS-Protection`. Per questa impostazione, è necessario specificare separatamente:

- Un'impostazione `X-XSS-Protection` di `0` (disabilita il filtro XSS) o `1`(abilita il filtro XSS)
- Un'impostazione booleana (`true` o `false`) per `block`, che determina se CloudFront include la direttiva `mode=block` nel valore di questa intestazione
- Un URI di reporting, che determina se CloudFront include la direttiva `report=`*`reporting URI`* nel valore di questa intestazione

Puoi specificare `true` per `block` oppure puoi specificare un URI di reporting, ma non entrambi insieme. Per ulteriori informazioni su questa intestazione e su queste direttive, consulta X-XSS-Protection nei documenti Web MDN.

Sostituzione dell'origine

Ognuna di queste impostazioni delle intestazioni di sicurezza contiene un'impostazione booleana (`true` o `false`) che determina il comportamento di CloudFront quando la risposta dall'origine contiene quell'intestazione.

Quando questa impostazione è `true` e la risposta di origine contiene l'intestazione, CloudFront include l'intestazione ricevuta dall'origine nella risposta inviata al visualizzatore. Ignora l'intestazione ricevuta dall'origine.

Quando questa impostazione è `false` e la risposta di origine contiene l'intestazione, CloudFront include l'intestazione ricevuta dall'origine nella risposta inviata al visualizzatore.

Quando la risposta di origine non contiene l'intestazione, CloudFront aggiunge l'intestazione nella policy alla risposta che invia al visualizzatore. CloudFront lo fa quando questa impostazione è impostata su `true` o `false`.

Intestazioni personalizzate

Le impostazioni delle intestazioni personalizzate consentono di aggiungere e configurare intestazioni HTTP personalizzate in una policy delle intestazioni di risposta. CloudFront aggiunge queste intestazioni a ogni risposta che restituisce ai visualizzatori. Per ogni intestazione personalizzata, si specifica anche il valore per l'intestazione, sebbene l'impostazione di un valore sia facoltativa. Questo perché CloudFront può aggiungere un'intestazione di risposta senza valore.

Ogni intestazione personalizzata ha anche la sua impostazione Sostituzione origine:

- Quando questa impostazione è `true` e la risposta di origine contiene l'intestazione personalizzata presente nella policy, CloudFront aggiunge l'intestazione personalizzata nella policy alla risposta che invia al visualizzatore. Ignora l'intestazione ricevuta dall'origine.
- Quando questa impostazione è `false` e la risposta di origine contiene l'intestazione personalizzata presente nella policy, CloudFront include l'intestazione personalizzata ricevuta dall'origine nella risposta inviata al visualizzatore.
- Quando la risposta di origine non contiene l'intestazione personalizzata presente nella policy, CloudFront aggiunge l'intestazione personalizzata nella policy alla risposta inviata al visualizzatore. CloudFront lo fa quando questa impostazione è impostata su `true` o `false`.

Rimozione delle intestazioni

Puoi specificare le intestazioni che desideri che CloudFront rimuova dalle risposte che riceve dall'origine in modo che le intestazioni non vengano incluse nelle risposte che CloudFront invia ai visualizzatori. CloudFront rimuove le intestazioni da ogni risposta che invia ai visualizzatori, indipendentemente dal fatto che gli oggetti vengano serviti dalla cache di CloudFront o dall'origine.

Ad esempio, puoi rimuovere le intestazioni che non sono utili per i browser, ad esempio `X-Powered-By` o `Vary`, in modo che CloudFront rimuova queste intestazioni dalle risposte che invia ai visualizzatori.

Quando si specificano le intestazioni da rimuovere utilizzando una policy delle intestazioni di risposta, CloudFront rimuove prima le intestazioni e poi aggiunge le intestazioni specificate in altre sezioni della policy delle intestazioni di risposta (intestazioni CORS, intestazioni di sicurezza, intestazioni personalizzate e così via). Se specifichi un'intestazione da rimuovere ma aggiungi anche la stessa intestazione in un'altra sezione della policy, CloudFront include l'intestazione nelle risposte che invia ai visualizzatori.

> **Note**
>
> Puoi utilizzare una policy delle intestazioni di risposta per rimuovere le intestazioni `Server` e `Date` che CloudFront ha ricevuto dall'origine, in modo che queste intestazioni (come ricevute dall'origine) non siano incluse nelle risposte che CloudFront invia ai visualizzatori. Tuttavia, se effettui questa operazione, CloudFront aggiunge una propria versione di queste intestazioni alle risposte che invia ai visualizzatori. Per l'intestazione `Server` aggiunta da CloudFront, il valore dell'intestazione è `CloudFront`.

Intestazioni che non puoi rimuovere

Non è possibile rimuovere le seguenti intestazioni utilizzando una policy delle intestazioni di risposta. Se specifichi queste intestazioni nella sezione Rimuovi intestazioni di una policy sulle intestazioni di risposta (`ResponseHeadersPolicyRemoveHeadersConfig` nell'API), ricevi un errore.

- `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`

Intestazione di temporizzazione server

Utilizzo dell'impostazione `Server-Timing` dell'intestazione per abilitare l'intestazione `Server-Timing` nelle risposte HTTP inviate da CloudFront. È possibile utilizzare questa intestazione per

visualizzare i parametri che possono aiutarti a ottenere informazioni dettagliate sul comportamento e le prestazioni di CloudFront e l'origine. Ad esempio, è possibile vedere quale livello di cache ha servito un hit nella cache. In alternativa, puoi vedere la prima latenza di byte dall'origine in caso di mancata cache. I parametri nell'intestazione `Server-Timing` possono aiutarti a risolvere i problemi o a testare l'efficienza della tua configurazione o origine CloudFront.

Per ulteriori informazioni sui parametri CloudFront nell'intestazione `Server-Timing`, consulta gli argomenti seguenti.

Per abilitare l'intestazione `Server-Timing`, creare (o modificare) una policy per le intestazioni di risposta.

Argomenti

Frequenza di campionamento e intestazione richiesta Pragma

Quando si abilita l'intestazione `Server-Timing` in un criterio delle intestazioni di risposta, si specifica anche la frequenza di campionamento. La frequenza di campionamento è un numero 0-100 (incluso) che specifica la percentuale di risposte a cui si desidera che CloudFront aggiunga l'intestazione `Server-Timing`. Quando imposti la frequenza di campionamento su 100, CloudFront aggiunge l'intestazione `Server-Timing` alla risposta HTTP per ogni richiesta che corrisponde al comportamento della cache a cui è collegato il criterio delle intestazioni di risposta. Quando lo si imposta su 50, CloudFront aggiunge l'intestazione al 50% delle risposte per le richieste che corrispondono al comportamento della cache. È possibile impostare la frequenza di campionamento su qualsiasi numero 0-100 con un massimo di quattro cifre decimali.

Quando la frequenza di campionamento è impostata su un numero inferiore a 100, non è possibile controllare a quali risposte CloudFront aggiunge l'intestazione `Server-Timing`, solo la percentuale. Tuttavia, è possibile aggiungere l'intestazione `Pragma` con un valore impostato su `server-timing`in una richiesta HTTP per ricevere l'intestazione `Server-Timing` nella risposta a tale richiesta. Funziona a prescindere dalla frequenza di campionamento impostata. Anche quando la frequenza di campionamento è impostata su zero (0), CloudFront aggiunge l'intestazione `Server-Timing` alla risposta se la richiesta contiene l'intestazione `Pragma: server-timing`.

Intestazione Server-Timing dell'origine

In caso di mancata esecuzione della cache e CloudFront inoltra la richiesta al server di origine, l'origine potrebbe includere l'intestazione `Server-Timing` nella sua risposta a CloudFront. In questo caso, CloudFront aggiunge i suoi parametri all'intestazione `Server-Timing` ricevuta dall'origine. La risposta che CloudFront invia al visualizzatore contiene un'intestazione `Server-Timing` che include il valore che proviene dall'origine e i parametri aggiunti da CloudFront. Il valore dell'intestazione dall'origine potrebbe essere alla fine o tra due set di parametri che CloudFront aggiunge all'intestazione.

Quando si verifica un hit nella cache, la risposta che CloudFront invia al visualizzatore contiene una singola intestazione `Server-Timing`, che include solo i parametri di CloudFront nel valore dell'intestazione (il valore dall'origine non è incluso).

Metriche dell'intestazione del server-timing

Quando CloudFront aggiunge l'intestazione `Server-Timing` a una risposta HTTP, il valore dell'intestazione contiene uno o più parametri che ti possono aiutare a ottenere informazioni sul comportamento e le prestazioni di CloudFront e della tua origine. L'elenco seguente contiene tutti i parametri e i relativi valori potenziali. Un'intestazione `Server-Timing` contiene solo alcuni di questi parametri, a seconda della natura della richiesta e della risposta tramite CloudFront.

Alcuni di questi parametri sono inclusi nell'intestazione `Server-Timing` con solo il nome (nessun valore). Altri hanno un nome e un valore. Quando un parametro ha un valore, il nome e il valore sono separati da un punto e virgola (`;`). Quando l'intestazione contiene più di un parametro, i parametri sono separati da una virgola (`,`).

cdn-cache-hit

: CloudFront ha fornito una risposta dalla cache senza effettuare una richiesta all'origine.

cdn-cache-refresh

: CloudFront ha fornito una risposta dalla cache dopo aver inviato una richiesta all'origine per verificare che l'oggetto memorizzato nella cache sia ancora valido. In questo caso, CloudFront non ha recuperato l'oggetto completo dall'origine.

cdn-cache-miss

: CloudFront non ha fornito la risposta dalla cache. In questo caso, CloudFront ha richiesto l'oggetto completo dall'origine prima di restituire la risposta.

cdn-pop

Contiene un valore che descrive quale punto di presenza (POP) di CloudFront ha gestito la richiesta.

cdn-rid

Contiene un valore con l'identificatore univoco CloudFront per la richiesta. È possibile utilizzare questo identificatore di richiesta (RID) per la risoluzione dei problemi con Supporto

cdn-hit-layer

Questa metrica è presente quando CloudFront fornisce una risposta dalla cache senza effettuare una richiesta all'origine. Contiene uno dei seguenti valori:

- EDGE - CloudFront ha fornito la risposta memorizzata nella cache da una posizione POP.
- REC- CloudFront ha fornito la risposta memorizzata nella cache da una posizione edge cache regionale (REC).
- Origin Shield - CloudFront ha fornito la risposta memorizzata nella cache del REC che funge da Origin Shield.

cdn-upstream layer

Quando CloudFront richiede l'oggetto completo dall'origine, questa metrica è presente e contiene uno dei seguenti valori:

- EDGE - Una posizione POP ha inviato la richiesta direttamente all'origine.
- REC- Una posizione REC ha inviato la richiesta direttamente all'origine.
- Origin Shield - Il REC che agisce come Origin Shield ha inviato la richiesta direttamente all'origine.

cdn-upstream-dns

Contiene un valore con il numero di millisecondi utilizzati per recuperare il record DNS per l'origine. Un valore pari a zero (0) indica che CloudFront ha utilizzato un risultato DNS memorizzato nella cache o ha riutilizzato una connessione esistente.

cdn-upstream-connect

Contiene un valore con il numero di millisecondi tra il completamento della richiesta DNS di origine e una connessione TCP (e TLS, se applicabile) all'origine completata. Un valore pari a zero (0) indica che CloudFront ha riutilizzato una connessione esistente.

cdn-upstream-fbl

Contiene un valore con il numero di millisecondi tra il completamento della richiesta HTTP di origine e la ricezione del primo byte nella risposta dall'origine (latenza primo byte).

cdn-downstream-fbl

Contiene un valore con il numero di millisecondi tra il momento in cui la posizione edge ha finito di ricevere la richiesta e il numero di millisecondi in cui ha inviato il primo byte della risposta al visualizzatore.

Esempi di intestazione Sever-Timing

Di seguito sono illustrati alcuni esempi di una intestazione `Server-Timing` che un visualizzatore potrebbe ricevere da CloudFront quando l'impostazione dell'intestazione `Server-Timing` è abilitata.

Example — cache miss

Il seguente esempio mostra un'intestazione `Server-Timing` che un visualizzatore potrebbe ricevere quando l'oggetto richiesto non si trova nella cache di CloudFront.

```
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
```

Questa intestazione `Server-Timing` del parametro indica quanto segue:

- La richiesta di origine è stata inviata da un punto di presenza (POP) di CloudFront (`cdn-upstream-layer;desc="EDGE"`).
- CloudFront ha utilizzato un risultato DNS memorizzato nella cache per l'origine (`cdn-upstream-dns;dur=0`).
- A CloudFront sono stati necessari 114 millisecondi per completare la connessione TCP (e TLS, se applicabile) all'origine (`cdn-upstream-connect;dur=114`).
- Ci sono voluti 177 millisecondi perché CloudFront ricevesse il primo byte della risposta dall'origine, dopo aver completato la richiesta (`cdn-upstream-fbl;dur=177`).
- L'oggetto richiesto non era nella cache di CloudFront (`cdn-cache-miss`).
- La richiesta è stata ricevuta nella posizione edge identificata dal codice `PHX50-C2` (`cdn-pop;desc="PHX50-C2"`).

- L'ID univoco di CloudFront per questa richiesta era `yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==` (`cdn-rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg=="`).
- CloudFront ha impiegato 436 millisecondi per inviare il primo byte della risposta al visualizzatore, dopo aver ricevuto la richiesta del visualizzatore (`cdn-downstream-fbl;dur=436`).

Example - hit della cache

Il seguente esempio mostra un'intestazione `Server-Timing` che un visualizzatore potrebbe ricevere quando l'oggetto richiesto si trova nella cache di CloudFront.

```
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
```

Questa intestazione `Server-Timing` del parametro indica quanto segue:

- L'oggetto richiesto è nella cache (). (`cdn-cache-hit`).
- La richiesta è stata ricevuta nella posizione edge identificata dal codice `SEA19-C1` (`cdn-pop;desc="SEA19-C1"`).
- L'ID univoco di CloudFront per questa richiesta era `nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==` (`cdn-rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g=="`).
- L'oggetto richiesto è stato memorizzato nella cache in una posizione REC (Regional Edge Cache) (`cdn-hit-layer;desc="REC"`).
- CloudFront ha impiegato 137 millisecondi per inviare il primo byte della risposta al visualizzatore, dopo aver ricevuto la richiesta del visualizzatore (`cdn-downstream-fbl;dur=137`).

Creazione di policy delle intestazioni di risposta

È possibile utilizzare una policy delle intestazioni di risposta per specificare le intestazioni HTTP che Amazon CloudFront aggiunge o rimuove dalle risposte HTTP. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perché utilizzarle, consulta Aggiunta o rimozione di intestazioni delle risposte con una policy.

È possibile creare una policy delle intestazioni di risposta nella console CloudFront. Oppure, è possibile crearne una utilizzando AWS CloudFormation, AWS Command Line Interface (AWS CLI)

o l'API CloudFront. Dopo aver creato una policy delle intestazioni di risposta, è possibile collegarla a uno o più comportamenti della cache in una distribuzione CloudFront.

Prima di creare una policy personalizzata delle intestazioni di risposta, dovresti vedere se una delle policy delle intestazioni di risposta gestita si adatta al caso d'uso. In tal caso, puoi collegarla al comportamento della cache. In questo modo, non è necessario creare o gestire la policy delle intestazioni di risposta personalizzate.

Console

Per creare una policy delle intestazioni di risposta (console)

1. Eseguire l'accesso alla Console di gestione AWS, poi vai alla scheda Intestazioni di risposta sulla pagina Policy nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/policies/responseHeaders.
2. Scegliere Creazione delle policy delle intestazioni di risposta.
3. Nella Creazione delle policy delle intestazioni di risposta, eseguire le seguenti operazioni:

   a. Nel pannello Dettagli, inserisci un Nome per la policy delle intestazioni di risposta e (facoltativamente) una Descrizione che spieghi a cosa serve la policy.

   b. Nel pannello Condivisione di risorse multiorigine (CORS), scegli il toggle Configurazione CORS e configura le intestazioni CORS che vuoi aggiungere alla policy. Se si desidera che le intestazioni configurate sostituiscano le intestazioni ricevute da CloudFront dall'origine, selezionare la casella di controllo Sostituzione origine.

      Per ulteriori informazioni sulle impostazioni delle intestazioni CORS, consulta the section called “Intestazioni CORS”.

   c. Nel pannello Intestazioni di sicurezza, scegliere l'interruttore e configurare ciascuna delle intestazioni di sicurezza che si desidera aggiungere alla policy.

      Per ulteriori informazioni sulle impostazioni delle intestazioni di sicurezza, consulta the section called “Intestazioni di sicurezza”.

   d. Nel pannello Intestazioni personalizzate, aggiungi le intestazioni personalizzate che vuoi includere nella policy.

      Per ulteriori informazioni sulle impostazioni delle intestazioni personalizzate, consulta the section called “Intestazioni personalizzate”.

e. Nel pannello Remove headers (Rimuovi intestazioni), aggiungere i nomi di tutte le intestazioni che si desidera che CloudFront rimuova dalla risposta dell'origine e che non includa nella risposta che invia ai visualizzatori.

   Per ulteriori informazioni sulle impostazioni di rimozione delle intestazioni, consulta the section called “Rimozione delle intestazioni”.

f. Nel pannello Server-Timing header (Intestazione Server-Timing), scegliere il selettore Enable (Abilita) e inserire una frequenza di campionamento (un numero compreso tra 0 e 100, entrambi inclusi).

   Per ulteriori informazioni sull'intestazione `Server-Timing`, consulta the section called “Intestazione di temporizzazione server”.

4. Scegliere Crea per creare la policy.

Dopo aver creato una policy delle intestazioni di risposta, è possibile collegarla a un comportamento della cache in una distribuzione CloudFront.

Per allegare una policy delle intestazioni di risposta a una distribuzione esistente (console)

1. Apri la pagina Distribuzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Scegli la distribuzione da aggiornare, quindi scegli la scheda Comportamenti.
3. Selezionare il comportamento della cache da aggiornare, quindi scegliere Modifica.

   In alternativa, per creare un nuovo comportamento della cache, scegliere Crea comportamento.
4. Per Policy delle intestazioni di risposta, scegliere la policy da aggiungere al comportamento della cache.
5. Scegli Salva modifiche per aggiornare il comportamento della cache. Se stai creando un nuovo comportamento della cache, scegli Crea comportamento.

Per allegare una policy delle intestazioni di risposta a una nuova distribuzione (console)

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere Create Distribution (Crea distribuzione).

3. Per Policy delle intestazioni di risposta, scegliere la policy da aggiungere al comportamento della cache.
4. Scegliere le altre impostazioni per la distribuzione. Per ulteriori informazioni, consulta the section called “Tutte le impostazioni distribuzione”.
5. Scegliere Crea una distribuzione per creare la distribuzione.

CloudFormation

Per creare una policy delle intestazioni di risposta con CloudFormation, usa il Tipo di risorsa `AWS::CloudFront::ResponseHeadersPolicy`. L'esempio seguente mostra la sintassi del modello CloudFormation, in formato YAML, per la creazione di una policy delle intestazioni di risposta.

```
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
```

Per ulteriori informazioni, consulta AWS::CloudFront::ResponseHeadersPolicy nella Guida per l'utente AWS CloudFormation.

CLI

Per creare una policy delle intestazioni di risposta con AWS Command Line Interface (AWS CLI), utilizzare il comando aws cloudfront create-response-headers-policy. È possibile utilizzare un file

di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare una policy delle intestazioni di risposta (CLI con file di input)

1. Per creare un file denominato , utilizza il comando seguente `response-headers-policy.yaml`. Tale file contiene tutti i parametri di input per il comando create-response-headers-policy.

```
aws cloudfront create-response-headers-policy --generate-cli-skeleton yaml-input
 > response-headers-policy.yaml
```

2. Aprire il file `response-headers-policy.yaml` appena creato. Modificare il file per specificare un nome di policy e la configurazione della policy di intestazione di risposta desiderata, quindi salvare il file.

   Per ulteriori informazioni sulle impostazioni delle policy delle intestazioni di risposta, consulta the section called “Comprendere le policy delle intestazioni di risposta”.

3. Per creare una policy delle intestazioni di risposta, utilizzare il comando seguente. Il criterio creato utilizza i parametri di input del file `response-headers-policy.yaml`.

```
aws cloudfront create-response-headers-policy --cli-input-yaml file://response-
headers-policy.yaml
```

   Prendere nota del valore `Id` nell'output del comando. Questo è l'ID della policy delle intestazioni di risposta. È necessario per collegare la policy al comportamento della cache di una distribuzione CloudFront.

Per allegare una policy delle intestazioni di risposta a una distribuzione esistente (CLI con file di input)

1. Utilizzare il comando seguente per salvare la configurazione di distribuzione per la distribuzione CloudFront che si desidera aggiornare. Sostituire *`distribution_ID`* con l'ID della distribuzione.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Aprire il file denominato `dist-config.yaml` appena creato. Modificare il file, apportando le seguenti modifiche al comportamento della cache per utilizzare la policy delle intestazioni di risposta.

   - Nel comportamento della cache, aggiungere un campo denominato `ResponseHeadersPolicyId`. Per il valore del campo, utilizzare l'ID della policy di intestazione di risposta annotato dopo la creazione della policy.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare la policy delle intestazioni di risposta. Sostituire *distribution_ID* con l'ID della distribuzione.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Per allegare una policy delle intestazioni di risposta a una nuova distribuzione (CLI con file di input)

1. Per creare un file denominato , utilizza i comandi seguenti `distribution.yaml`. Tale file contiene tutti i parametri di input per il comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Aprire il file `distribution.yaml` appena creato. Nel comportamento predefinito della cache immettere nel campo `ResponseHeadersPolicyId` l'ID della policy delle intestazioni di risposta annotato dopo la creazione della policy. Continuare a modificare il file per specificare le impostazioni di distribuzione desiderate, quindi salvare il file al termine.

   Per ulteriori informazioni sulle impostazioni di distribuzione, consulta Riferimento a tutte le impostazioni di distribuzione.

3. Utilizzare il comando seguente per creare la distribuzione utilizzando i parametri di input dal file `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Per creare una policy delle intestazioni di risposta con l'API CloudFront, utilizzare CreateResponseHeadersPolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta the section called “Comprendere le policy delle intestazioni di risposta” e la documentazione di riferimento delle API per l'SDK AWS o altro client API.

Dopo aver creato una policy delle intestazioni di risposta, è possibile collegarla a un comportamento della cache, utilizzando una delle seguenti chiamate API:

- Per collegarlo a un comportamento della cache in una distribuzione esistente, utilizzare UpdateDistribution.
- Per collegarlo a un comportamento della cache in una nuova distribuzione, utilizzare CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID della policy delle intestazioni di risposta nel campo `ResponseHeadersPolicyId`, all'interno di un comportamento della cache. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione e la documentazione di riferimento delle API per l'SDK AWS o un altro client API.

Utilizzo di policy di intestazioni di risposta gestite

Con una policy delle intestazioni di risposta CloudFront, puoi specificare le intestazioni HTTP che Amazon CloudFront rimuove aggiunge alle risposte inviate ai visualizzatori. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perché utilizzarle, consulta Aggiunta o rimozione di intestazioni delle risposte con una policy.

CloudFront fornisce policy per le intestazioni di risposta gestite che è possibile collegare ai comportamenti della cache nelle distribuzioni CloudFront. Con una policy delle intestazioni di risposta

gestita, non è necessario scrivere o gestire policy personalizzate. Le policy gestite da contengono set di intestazioni di risposta HTTP per casi d'uso comuni.

Per utilizzare una policy di intestazioni di risposta gestita, è necessario collegarla a un comportamento della cache nella distribuzione. Il processo è lo stesso di quando si crea una policy di intestazioni di risposta personalizzata. Tuttavia, invece di creare una nuova policy, si allega una delle policy gestite. Si allega la policy per nome (con la console) o per ID (con CloudFormation, AWS CLI o SDK AWS). I nomi e gli ID sono elencati nella sezione seguente.

Per ulteriori informazioni, consulta the section called “Creazione di policy delle intestazioni di risposta”.

Negli argomenti seguenti vengono descritte le policy delle intestazioni di risposta gestite che è possibile utilizzare.

Argomenti

CORS-and-SecurityHeadersPolicy

Visualizzare questa policy nella console di CloudFront

Usa questa policy gestita per consentire semplici richieste CORS da qualsiasi origine. Utilizza questa policy gestita per aggiungere un set di intestazioni di sicurezza a tutte le risposte inviate da CloudFront ai visualizzatori. Questa policy combina le policy the section called “SimpleCORS” e the section called “SecurityHeadersPolicy” in uno.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

```
e61eb60c-9c35-4d20-a928-2b84e02af89c
```

Impostazioni delle policy

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
Intestazioni CORS:	`Access-Control-Allow-Origin`	`*`	No
Intestazioni di sicurezza:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sì
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

CORS-With-Preflight

Visualizzare questa policy nella console di CloudFront

Utilizzare questa policy gestita per consentire richieste CORS da qualsiasi origine, incluse le richieste di verifica preliminare. Per richieste di verifica preliminare (utilizzando il metodo HTTP `OPTIONS`), CloudFront aggiunge tutte e tre le seguenti intestazioni alla risposta. Per semplici richieste CORS, CloudFront aggiunge solo l'intestazione `Access-Control-Allow-Origin`.

Se la risposta che CloudFront riceve dall'origine include una di queste intestazioni, CloudFront utilizza l'intestazione ricevuta (e il suo valore) nella risposta al visualizzatore. CloudFront non utilizza l'intestazione in questa policy.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`5cc3b908-e619-4b99-88e5-2cf7f45965bd`

Impostazioni delle policy

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
Intestazioni CORS:	`Access-Control-Allow-Methods`	`DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`	No
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	

CORS-with-preflight-and-SecurityHeadersPolicy

Visualizzare questa policy nella console di CloudFront

Usa questa policy gestita per consentire richieste CORS da qualsiasi origine. Sono incluse le richieste di verifica preliminare. Utilizza questa policy gestita per aggiungere un set di intestazioni di sicurezza a tutte le risposte inviate da CloudFront ai visualizzatori. Questa policy combina le policy the section called “CORS-With-Preflight” e the section called “SecurityHeadersPolicy” in uno.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`eaab4381-ed33-4a86-88ca-d9558dc6cd63`

Impostazioni delle policy

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
Intestazioni CORS:	`Access-Control-Allow-Methods`	`DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`	No
	`Access-Control-Allow-Origin`	`*`	

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
	`Access-Control-Expose-Headers`	`*`	
Intestazioni di sicurezza:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sì
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

SecurityHeadersPolicy

Visualizzare questa policy nella console di CloudFront

Utilizza questa policy gestita per aggiungere un set di intestazioni di sicurezza a tutte le risposte inviate da CloudFront ai visualizzatori. Per ulteriori informazioni su queste intestazioni di sicurezza, consulta Mozilla's web security guidelines (Linee guida sulla sicurezza Web di Mozilla).

Con questa policy delle intestazioni di risposta, CloudFront aggiunge `X-Content-Type-Options: nosniff` a tutte le risposte. Questo è il caso in cui la risposta ricevuta da CloudFront dall'origine includeva questa intestazione e quando no. Per tutte le altre intestazioni di questa policy, se la risposta che CloudFront riceve dall'origine include tale intestazione, CloudFront utilizza l'intestazione ricevuta (e il suo valore) nella risposta al visualizzatore. Non utilizza l'intestazione in questa policy.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`67f7725c-6f97-4210-82d7-5512b31e9d03`

Impostazioni delle policy

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
Intestazioni di sicurezza:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sì
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

SimpleCORS

Visualizzare questa policy nella console di CloudFront

Usa questa policy gestita per consentire semplici richieste CORS da qualsiasi origine. Con questa policy, CloudFront aggiunge l'intestazione `Access-Control-Allow-Origin: *` a tutte le risposte per semplici richieste CORS.

Se la risposta che CloudFront riceve dall'origine include l'intestazione `Access-Control-Allow-Origin`, CloudFront utilizza quell'intestazione (e il suo valore) nella risposta al visualizzatore. CloudFront non utilizza l'intestazione in questa policy.

Quando si utilizza CloudFormation, l'AWS CLI o l'API di CloudFront, l'ID di questa policy è:

`60669652-455b-4ae9-85a4-c4c02393f86c`

Impostazioni delle policy

	Nome intestazione	Valore intestazione	Sostituzione dell'origine?
Intestazioni CORS:	`Access-Control-Allow-Origin`	*	No

Comportamento di richieste e risposte

I seguenti argomenti descrivono come CloudFront gestisce le richieste e le risposte.

Puoi scoprire come CloudFront interagisce con Amazon S3 o le origini personalizzate, gestisce vari metodi e intestazioni HTTP, elabora i codici di stato e gestisce la memorizzazione nella cache e le risposte agli errori.

Argomenti

Come CloudFront elabora le richieste HTTP e HTTPS

Per le origini di Amazon S3, CloudFront accetta per impostazione predefinita le richieste nei protocolli HTTP e HTTPS per gli oggetti in una CloudFront distribuzione. CloudFront quindi inoltra le richieste al tuo bucket Amazon S3 utilizzando lo stesso protocollo in cui sono state effettuate le richieste.

Per i server di origine personalizzati, al momento della creazione della distribuzione, puoi specificare il modo in cui CloudFront accede ai server di origine: solo tramite HTTP oppure con il protocollo utilizzato dal visualizzatore. Per ulteriori informazioni su come CloudFront gestisce le richieste HTTP e HTTPS per le origini personalizzate, consulta. Protocolli

Per informazioni su come limitare la distribuzione, in modo che gli utenti finali possano accedere agli oggetti solo tramite HTTPS, consulta Usa HTTPS con CloudFront.

> **Note**
>
> L'addebito per le richieste HTTPS è superiore al costo delle richieste HTTP. Per ulteriori informazioni sulle tariffe di fatturazione, consulta la pagina CloudFront dei prezzi.

Comportamento di richieste e risposte per origini Amazon S3

Per capire come CloudFront elabora le richieste e le risposte quando usi Amazon S3 come origine, consulta le seguenti sezioni:

Argomenti

- In che modo CloudFront elabora e inoltra le richieste alla tua origine Amazon S3
- In che modo CloudFront elabora le risposte dalla tua origine Amazon S3

In che modo CloudFront elabora e inoltra le richieste alla tua origine Amazon S3

Scopri come CloudFront elabora le richieste dei visualizzatori e le inoltra alla tua origine Amazon S3.

Indice

- Timeout di risposta dell'origine
- Richieste simultanee per lo stesso oggetto (compressione richieste)

Durata del caching e TTL minimo

Per controllare per quanto tempo gli oggetti rimangono in una CloudFront cache prima di CloudFront inoltrare un'altra richiesta all'origine, puoi:

- Configurare la tua origine per aggiungere un'intestazione `Cache-Control` o un campo di intestazione `Expires` a ogni oggetto.
- Specificate un valore per Minimum TTL nei comportamenti CloudFront della cache.
- Utilizzare il valore di default di 24 ore.

Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Indirizzi IP client

Se un visualizzatore invia una richiesta a CloudFront e non include un'intestazione di `X-Forwarded-For` richiesta, CloudFront ottiene l'indirizzo IP del visualizzatore dalla connessione TCP, aggiunge un'`X-Forwarded-For`intestazione che include l'indirizzo IP e inoltra la richiesta all'origine. Ad esempio, se CloudFront ottiene l'indirizzo IP `192.0.2.2` dalla connessione TCP, inoltra la seguente intestazione all'origine:

```
X-Forwarded-For: 192.0.2.2
```

Se un visualizzatore invia una richiesta CloudFront e include un'intestazione di `X-Forwarded-For` richiesta, CloudFront ottiene l'indirizzo IP del visualizzatore dalla connessione TCP, lo aggiunge alla fine dell'`X-Forwarded-For`intestazione e inoltra la richiesta all'origine. Ad esempio, se la richiesta del visualizzatore include `X-Forwarded-For: 192.0.2.4,192.0.2.3` e CloudFront ottiene l'indirizzo IP `192.0.2.2` dalla connessione TCP, inoltra l'intestazione seguente all'origine:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

> **Note**
>
> L'`X-Forwarded-For`intestazione contiene IPv4 indirizzi (come 192.0.2.44) e IPv6 indirizzi (come 2001:0 db 8:85 a3: :8a2e: 0370:7334).

Richieste GET condizionali

Quando CloudFront riceve una richiesta per un oggetto scaduto da una cache edge, inoltra la richiesta all'origine Amazon S3 per ottenere la versione più recente dell'oggetto o per ottenere la conferma da Amazon S3 che la cache edge ha già CloudFront la versione più recente. Quando Amazon S3 ha originariamente inviato l'oggetto a CloudFront, includeva un `ETag` valore e un `LastModified` valore nella risposta. Nella nuova richiesta CloudFront inoltrata ad Amazon S3 CloudFront , aggiunge una o entrambe le seguenti intestazioni:

- Un'intestazione `If-Match` o `If-None-Match` che contiene il valore `ETag` per la versione scaduta dell'oggetto.
- Un'intestazione `If-Modified-Since` che contiene il valore `LastModified` per la versione scaduta dell'oggetto.

Amazon S3 utilizza queste informazioni per determinare se l'oggetto è stato aggiornato e, quindi, se restituire l'intero oggetto CloudFront o restituire solo un codice di stato HTTP 304 (non modificato).

Cookie

Amazon S3 non elabora i cookie. Se configuri un comportamento di cache per inoltrare i cookie a un'origine Amazon S3, CloudFront inoltra i cookie, ma Amazon S3 li ignora. Tutte le richieste future per lo stesso oggetto, indipendentemente dalla variazione o meno del cookie, vengono servite dall'oggetto esistente nella cache.

Cross-Origin Resource Sharing (CORS)

Se desideri rispettare CloudFront le impostazioni di condivisione delle risorse tra origini diverse di Amazon S3, configura l'inoltro delle intestazioni selezionate CloudFront ad Amazon S3. Per ulteriori informazioni, consulta Caching dei contenuti in base alle intestazioni di richiesta.

Richieste GET che includono un corpo

Se una `GET` richiesta del visualizzatore include un corpo, CloudFront restituisce un codice di stato HTTP 403 (Forbidden) al visualizzatore.

Metodi HTTP

Se configuri CloudFront per elaborare tutti i metodi HTTP supportati, CloudFront accetta le seguenti richieste dai visualizzatori e le inoltra alla tua origine Amazon S3:

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

CloudFront memorizza sempre nella cache le risposte e le richieste. `GET` `HEAD` È inoltre possibile configurare CloudFront la memorizzazione nella cache delle risposte alle `OPTIONS` richieste. CloudFront non memorizza nella cache le risposte alle richieste che utilizzano gli altri metodi.

Se desideri utilizzare caricamenti in più parti per aggiungere oggetti a un bucket Amazon S3, devi aggiungere CloudFront un controllo di accesso all'origine (OAC) alla tua distribuzione e fornire all'OAC le autorizzazioni necessarie. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

> **Important**
>
> Se configuri CloudFront per accettare e inoltrare ad Amazon S3 tutti i metodi HTTP CloudFront supportati, devi creare un CloudFront OAC per limitare l'accesso ai tuoi contenuti Amazon S3 e concedere all'OAC le autorizzazioni richieste. Ad esempio, se configuri per accettare e CloudFront inoltrare questi metodi perché desideri utilizzare il `PUT` metodo, devi configurare le policy dei bucket di Amazon S3 per gestire le `DELETE` richieste in modo appropriato in modo che gli utenti non possano eliminare le risorse che non desideri. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

Per informazioni sulle operazioni supportate da Amazon S3 consulta la documentazione di Amazon S3.

Intestazioni di richiesta HTTP che rimuovono o aggiornano CloudFront

CloudFront rimuove o aggiorna alcune intestazioni prima di inoltrare le richieste alla tua origine Amazon S3. Per la maggior parte delle intestazioni questo comportamento corrisponde a quello

delle origini personalizzate. Per un elenco completo delle intestazioni delle richieste HTTP e di come CloudFront le elabora, consulta. Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

Lunghezza massima di una richiesta e lunghezza massima di un URL

La lunghezza massima di una richiesta, inclusi il percorso, l'eventuale stringa di query e le intestazioni, è di 20.480 byte.

CloudFront costruisce un URL a partire dalla richiesta. La lunghezza massima di questo URL è di 8192 byte.

Se una richiesta o un URL supera la lunghezza massima, CloudFront restituisce il codice di stato HTTP 413 (Request Entity Too Large) al visualizzatore, quindi interrompe la connessione TCP con il visualizzatore.

Stapling OCSP

Quando un visualizzatore invia una richiesta HTTPS per un oggetto CloudFront o deve confermare con l'autorità di certificazione (CA) che il certificato SSL per il dominio non è stato revocato. OCSP stapling velocizza la convalida dei certificati consentendo di CloudFront convalidare il certificato e di memorizzare nella cache la risposta della CA, in modo che il client non debba convalidare il certificato direttamente con la CA.

Il miglioramento delle prestazioni dello stapling OCSP è più pronunciato quando si CloudFront ricevono molte richieste HTTPS per oggetti nello stesso dominio. Ogni server in una edge location di CloudFront deve inviare una richiesta di convalida distinta. Quando CloudFront riceve molte richieste HTTPS per lo stesso dominio, ogni server nell'edge location riceve subito una risposta dalla CA che può inserire in un pacchetto nell'handshake SSL. Quando il visualizzatore ritiene che il certificato sia valido, CloudFront può servire l'oggetto richiesto. Se la tua distribuzione non riceve molto traffico in una edge location di CloudFront , è più probabile che le nuove richieste siano indirizzate a un server che non ha ancora convalidato il certificato presso la CA. In tal caso, il visualizzatore esegue separatamente la fase di convalida e il CloudFront server serve l'oggetto. Tale CloudFront server invia inoltre una richiesta di convalida alla CA, quindi la prossima volta che riceve una richiesta che include lo stesso nome di dominio, riceve una risposta di convalida dalla CA.

Protocolli

CloudFront inoltra le richieste HTTP o HTTPS al server di origine in base al protocollo della richiesta del visualizzatore, HTTP o HTTPS.

> **Important**
>
> Se il tuo bucket Amazon S3 è configurato come endpoint di un sito Web, non puoi configurare l'utilizzo di HTTPS CloudFront per comunicare con la tua origine perché Amazon S3 non supporta le connessioni HTTPS in quella configurazione.

Stringhe di query

Puoi configurare se CloudFront inoltrare i parametri della stringa di query alla tua origine Amazon S3. Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

Timeout connessione origine e tentativi

Il timeout della connessione Origin è il numero di secondi che CloudFront attendono quando si tenta di stabilire una connessione all'origine.

I tentativi di connessione all'origine sono il numero di volte in cui si CloudFront tenta di connettersi all'origine.

Insieme, queste impostazioni determinano la durata dei CloudFront tentativi di connessione all'origine prima di passare all'origine secondaria (nel caso di un gruppo di origine) o restituire una risposta di errore al visualizzatore. Per impostazione predefinita, CloudFront attende fino a 30 secondi (3 tentativi da 10 secondi ciascuno) prima di tentare di connettersi all'origine secondaria o restituire una risposta di errore. Puoi ridurre questo tempo specificando un timeout di connessione più breve, un numero inferiore di tentativi o entrambi.

Per ulteriori informazioni, consulta Controllo dei timeout e dei tentativi di origine.

Timeout di risposta dell'origine

Il timeout di risposta origine, noto anche come timeout di lettura origine o timeout di richiesta origine, si applica a entrambi i valori seguenti:

- La quantità di tempo, in secondi, che CloudFront attende una risposta dopo l'inoltro di una richiesta all'origine.
- La quantità di tempo, in secondi, che CloudFront attende dopo aver ricevuto un pacchetto di risposta dall'origine e prima di ricevere il pacchetto successivo.

CloudFront il comportamento dipende dal metodo HTTP della richiesta del visualizzatore:

- `GET`e `HEAD` richieste: se l'origine non risponde entro 30 secondi o smette di rispondere per 30 secondi, CloudFront interrompe la connessione. Se il numero specificato di tentativi di connessione all'origine è superiore a 1, CloudFront riprova per ottenere una risposta completa. CloudFront prova fino a 3 volte, in base al valore dell'impostazione dei tentativi di connessione di origine. Se l'origine non risponde durante il terzo tentativo, CloudFront non riprova fino a che non riceve un'altra richiesta per il contenuto sulla stessa origine.
- `DELETE`,`OPTIONS`, `PATCH`PUT, e `POST` richieste: se l'origine non risponde entro 30 secondi, CloudFront interrompe la connessione e non riprova a contattare l'origine. Il client può inoltrare nuovamente la richiesta, se necessario.

Non è possibile modificare il timeout di risposta per un'origine Amazon S3 (un bucket S3 che non è configurato con l'hosting di siti Web statici).

Richieste simultanee per lo stesso oggetto (compressione richieste)

Quando una CloudFront edge location riceve una richiesta per un oggetto e l'oggetto non è presente nella cache o l'oggetto memorizzato nella cache è scaduto, invia CloudFront immediatamente la richiesta all'origine. Tuttavia, se ci sono richieste simultanee per lo stesso oggetto, ovvero se richieste aggiuntive per lo stesso oggetto (con la stessa chiave di cache) arrivano all'edge location prima di CloudFront ricevere la risposta alla prima richiesta, si CloudFront interrompe prima di inoltrare le richieste aggiuntive all'origine. Questa breve pausa aiuta a ridurre il carico sull'origine. CloudFront invia la risposta dalla richiesta originale a tutte le richieste ricevute mentre era in pausa. Questa operazione è chiamata compressione richieste. Nei CloudFront log, la prima richiesta viene identificata come una `Miss` nel `x-edge-result-type` campo e le richieste compresse vengono identificate come a. `Hit` Per ulteriori informazioni sui CloudFront log, vedere. the section called “CloudFront e registrazione delle funzioni edge”

CloudFront comprime solo le richieste che condividono una chiave di cache. Se le richieste aggiuntive non condividono la stessa chiave di cache perché, ad esempio, hai configurato la cache in base CloudFront alle intestazioni delle richieste o ai cookie o alle stringhe di query, CloudFront inoltra tutte le richieste con una chiave di cache univoca all'origine.

Se desideri impedire la compressione di tutte le richieste, puoi utilizzare la policy della cache gestita `CachingDisabled`, che impedisce anche il caching. Per ulteriori informazioni, consulta Utilizzo delle policy della cache gestite.

Se desideri evitare la compressione delle richieste per oggetti specifici, puoi impostare il TTL minimo per il comportamento cache su 0 e configurare l'origine in modo che invii `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` o `Cache-Control: s-maxage=0`. Queste configurazioni aumenteranno il carico sull'origine e introdurranno una latenza aggiuntiva per le richieste simultanee che vengono messe in pausa durante l' CloudFront attesa della risposta alla prima richiesta.

> **Important**
>
> Attualmente, CloudFront non supporta la compressione della richiesta se si abilita l'inoltro dei cookie nella politica della cache, nella politica di richiesta di origine o nelle impostazioni della cache legacy.

In che modo CloudFront elabora le risposte dalla tua origine Amazon S3

Scopri come CloudFront elabora le risposte dalla tua origine Amazon S3.

Indice

Richieste annullate

Se un oggetto non si trova nella cache edge e se un visualizzatore termina una sessione (ad esempio, chiude un browser) dopo averlo CloudFront recuperato dall'origine ma prima che possa consegnare l'oggetto richiesto, CloudFront non lo memorizza nella cache nell'edge location.

Intestazioni di risposta HTTP che rimuovono o aggiornano CloudFront

CloudFront rimuove o aggiorna i seguenti campi di intestazione prima di inoltrare la risposta dall'origine Amazon S3 al visualizzatore:

- `X-Amz-Id-2`
- `X-Amz-Request-Id`

- `Set-Cookie`— Se configuri CloudFront per inoltrare i cookie, inoltrerà il campo di `Set-Cookie` intestazione ai client. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.
- `Trailer`
- `Transfer-Encoding`— Se la tua origine Amazon S3 restituisce questo campo di intestazione, CloudFront imposta il valore su `chunked` prima di restituire la risposta al visualizzatore.
- `Upgrade`
- `Via`— CloudFront imposta il valore seguente nella risposta al visualizzatore:

  `Via: http-version alphanumeric-string.cloudfront.net (CloudFront)`

  Ad esempio, il valore è simile al seguente:

  `Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)`

Dimensione massima del file memorizzabile nella cache

La dimensione massima di un corpo di risposta che viene CloudFront salvato nella cache è di 50 GB. Questa dimensione include risposte di trasferimento in blocchi che non specificano il valore di intestazione `Content-Length`.

È possibile utilizzare CloudFront per memorizzare nella cache un oggetto di dimensioni maggiori di tali dimensioni utilizzando le richieste di intervallo per richiedere gli oggetti in parti di dimensioni pari o inferiori a 50 GB ciascuna. CloudFrontmemorizza nella cache queste parti perché ognuna di esse pesa 50 GB o meno. Dopo che il visualizzatore ha recuperato tutte le parti dell'oggetto, può ricostruire l'oggetto originale più grande. Per ulteriori informazioni, consulta Utilizzare richieste di intervallo per memorizzare nella cache oggetti di grandi dimensioni.

Reindirizzamenti

Puoi configurare un bucket Amazon S3 per reindirizzare tutte le richieste a un altro nome host, ovvero un altro bucket Amazon S3 o un server HTTP. Se configuri un bucket per reindirizzare tutte le richieste e se il bucket è l'origine di una CloudFront distribuzione, ti consigliamo di configurare il bucket per reindirizzare tutte le richieste a una CloudFront distribuzione utilizzando il nome di dominio per la distribuzione (ad esempio, d111111abcdef8.cloudfront.net) o un nome di dominio alternativo (un CNAME) associato a una distribuzione (ad esempio, example.com). In caso contrario, le richieste del visualizzatore vengono CloudFront ignorate e gli oggetti vengono serviti direttamente dalla nuova origine.

> **Note**
>
> Se reindirizzi le richieste a un nome di dominio alternativo, devi anche aggiornare il servizio DNS per il tuo dominio aggiungendo un record CNAME. Per ulteriori informazioni, consulta Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs.

Di seguito viene descritto ciò che accade quando configuri un bucket per reindirizzare tutte le richieste:

1. Un visualizzatore (ad esempio un browser) richiede un oggetto da CloudFront.
2. CloudFront inoltra la richiesta al bucket Amazon S3 che è l'origine della tua distribuzione.
3. Amazon S3 restituisce un codice di stato HTTP 301 (Spostato in modo permanente) e la nuova posizione.
4. CloudFront memorizza nella cache il codice di stato del reindirizzamento e la nuova posizione e restituisce i valori al visualizzatore. CloudFront non segue il reindirizzamento per recuperare l'oggetto dalla nuova posizione.
5. Il visualizzatore invia un'altra richiesta per l'oggetto, ma questa volta specifica la nuova posizione da cui è stato ottenuto: CloudFront

   - Se il bucket Amazon S3 reindirizza tutte le richieste a una CloudFront distribuzione, utilizzando il nome di dominio per la distribuzione o un nome di dominio alternativo, CloudFront richiede l'oggetto dal bucket Amazon S3 o dal server HTTP nella nuova posizione. Quando la nuova posizione restituisce l'oggetto, lo restituisce al visualizzatore e lo CloudFront memorizza nella cache in una posizione periferica.
   - Se il bucket Amazon S3 reindirizza le richieste verso un'altra posizione, la seconda richiesta viene ignorata. CloudFront Il bucket Amazon S3 o il server HTTP nella nuova posizione restituiscono l'oggetto direttamente al visualizzatore, in modo che l'oggetto non venga mai memorizzato nella cache edge. CloudFront

Comportamento di richieste e risposte per origini personalizzate

Per comprendere come CloudFront elabora le richieste e le risposte quando utilizzi origini personalizzate, consulta le seguenti sezioni:

Argomenti

In che modo CloudFront elabora e inoltra le richieste all'origine personalizzata

Scopri come CloudFront elabora le richieste degli utenti e le inoltra alla tua origine personalizzata.

Indice

- Richieste simultanee per lo stesso oggetto (compressione richieste)
- User-Agent Intestazione

Autenticazione

Per inoltrare l'intestazione `Authorization` all'origine, puoi configurare il server di origine per richiedere l'autenticazione client per i seguenti tipi di richieste:

- `DELETE`
- `GET`
- `HEAD`
- `PATCH`
- `PUT`
- `POST`

Per `OPTIONS` le richieste, l'autenticazione del client può essere configurata solo se utilizzi le seguenti CloudFront impostazioni:

- CloudFront è configurato per inoltrare l'`Authorization`intestazione all'origine
- CloudFront è configurato per non memorizzare nella cache la risposta alle richieste `OPTIONS`

Per ulteriori informazioni, consulta Configurazione di CloudFront per inoltrare l'intestazione `Authorization`.

Puoi utilizzare HTTP o HTTPS per inoltrare le richieste al server di origine. Per ulteriori informazioni, consulta Usa HTTPS con CloudFront.

Durata del caching e TTL minimo

Per controllare per quanto tempo i tuoi oggetti rimangono in una CloudFront cache prima di CloudFront inoltrare un'altra richiesta all'origine, puoi:

- Configurare la tua origine per aggiungere un'intestazione `Cache-Control` o un campo di intestazione `Expires` a ogni oggetto.
- Specificate un valore per Minimum TTL nei comportamenti CloudFront della cache.
- Utilizzare il valore di default di 24 ore.

Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Indirizzi IP client

Se un visualizzatore invia una richiesta a CloudFront e non include un'intestazione di `X-Forwarded-For` richiesta, CloudFront ottiene l'indirizzo IP del visualizzatore dalla connessione TCP, aggiunge un'`X-Forwarded-For`intestazione che include l'indirizzo IP e inoltra la richiesta all'origine. Ad esempio, se CloudFront ottiene l'indirizzo IP `192.0.2.2` dalla connessione TCP, inoltra la seguente intestazione all'origine:

```
X-Forwarded-For: 192.0.2.2
```

Se un visualizzatore invia una richiesta CloudFront e include un'intestazione di `X-Forwarded-For` richiesta, CloudFront ottiene l'indirizzo IP del visualizzatore dalla connessione TCP, lo aggiunge alla fine dell'`X-Forwarded-For`intestazione e inoltra la richiesta all'origine. Ad esempio, se la richiesta del visualizzatore include `X-Forwarded-For: 192.0.2.4,192.0.2.3` e CloudFront ottiene l'indirizzo IP `192.0.2.2` dalla connessione TCP, inoltra l'intestazione seguente all'origine:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Alcune applicazioni, come i sistemi di bilanciamento del carico (incluso Elastic Load Balancing), i firewall per applicazioni Web, i reverse proxy, i sistemi di prevenzione delle intrusioni e l'API Gateway, aggiungono l'indirizzo IP del server perimetrale che ha inoltrato la richiesta alla fine CloudFront dell'intestazione. `X-Forwarded-For` Ad esempio, se CloudFront include `X-Forwarded-For: 192.0.2.2` una richiesta che inoltra a ELB e se l'indirizzo IP del server CloudFront perimetrale è 192.0.2.199, la richiesta ricevuta dall' EC2 istanza contiene l'intestazione seguente:

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> L'`X-Forwarded-For`intestazione contiene IPv4 indirizzi (come 192.0.2.44) e indirizzi (come 2001:0 db 8:85 a3: :8a2e: IPv6 0370:7334).
> Nota inoltre che l'intestazione può essere modificata da ogni nodo sul percorso del server corrente (). `X-Forwarded-For` CloudFront Per ulteriori informazioni, consulta la sezione 8.1 di RFC 7239. È inoltre possibile modificare l'intestazione utilizzando le funzioni di CloudFront edge computing.

Autenticazione SSL lato client

CloudFront supporta l'autenticazione TLS reciproca (mTLS) in cui sia il client che il server si autenticano a vicenda tramite certificati. Con MTL configurato, è CloudFront possibile convalidare i certificati client durante l'handshake TLS e, facoltativamente, eseguire Funzioni per implementare una logica di convalida personalizzata. CloudFront

Per le origini che richiedono certificati lato client quando MTLS non è configurato, elimina la richiesta. CloudFront

Per ulteriori informazioni sulla configurazione degli MTL, consulta. ???

CloudFront non supporta l'autenticazione client con certificati SSL lato client. Se un'origine richiede un certificato lato client, elimina la richiesta. CloudFront

Compression

Per ulteriori informazioni, consulta Distribuzione di file compressi.

Richieste condizionali

Quando CloudFront riceve una richiesta per un oggetto scaduto da una cache edge, inoltra la richiesta all'origine per ottenere la versione più recente dell'oggetto o per ottenere la conferma dall'origine che la cache CloudFront edge ha già la versione più recente. In genere, quando l'origine ha inviato l'oggetto per l'ultima volta CloudFront, nella risposta `ETag` includeva un `LastModified` valore, un valore o entrambi i valori. Nella nuova richiesta che CloudFront inoltra all'origine, CloudFront aggiunge uno o entrambi i seguenti elementi:

- Un'intestazione `If-Match` o `If-None-Match` che contiene il valore `ETag` per la versione scaduta dell'oggetto.
- Un'intestazione `If-Modified-Since` che contiene il valore `LastModified` per la versione scaduta dell'oggetto.

L'origine utilizza queste informazioni per determinare se l'oggetto è stato aggiornato e, quindi, se restituire l'intero oggetto CloudFront o restituire solo un codice di stato HTTP 304 (non modificato).

> **Note**
>
> `If-Modified-Sincee` le richieste `If-None-Match` condizionali non sono supportate quando CloudFront è configurato per inoltrare i cookie (tutti o un sottoinsieme).

Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.

Cookie

È possibile configurare CloudFront l'inoltro dei cookie all'origine. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.

Cross-Origin Resource Sharing (CORS)

Se desideri CloudFront rispettare le impostazioni di condivisione delle risorse tra origini diverse, configura CloudFront l'inoltro dell'`Origin`intestazione all'origine. Per ulteriori informazioni, consulta Caching dei contenuti in base alle intestazioni di richiesta.

Encryption (Crittografia)

Puoi richiedere ai visualizzatori di utilizzare HTTPS per inviare richieste CloudFront e richiedere di CloudFront inoltrare le richieste all'origine personalizzata utilizzando il protocollo utilizzato dal visualizzatore. Per ulteriori informazioni, vedi le seguenti impostazioni di distribuzione:

- Viewer Protocol Policy (Policy protocollo visualizzatore)
- Protocollo (solo origini personalizzate)

CloudFront inoltra le richieste HTTPS al server di origine utilizzando i protocolli SSLv3, TLSv1 .0, TLSv1 .1, TLSv1 .2 e .3. TLSv1 Per le origini personalizzate, puoi scegliere i protocolli SSL che desideri utilizzare CloudFront per comunicare con la tua origine:

- Se utilizzi la CloudFront console, scegli i protocolli utilizzando le caselle di controllo Origin SSL Protocols. Per ulteriori informazioni, consulta Creazione di una distribuzione.
- Se utilizzi l' CloudFront API, specifica i protocolli utilizzando l'`OriginSslProtocols`elemento. Per ulteriori informazioni, consulta OriginSslProtocolse DistributionConfignell'Amazon CloudFront API Reference.

Se l'origine è un bucket Amazon S3, CloudFront il valore predefinito è .3. TLSv1

> **Important**
>
> Le altre versioni di SSL e TLS non sono supportate.

Per ulteriori informazioni sull'utilizzo di HTTPS con CloudFront, consulta. Usa HTTPS con CloudFront Per un elenco dei cifrari che CloudFront supportano la comunicazione HTTPS tra i visualizzatori e tra l'origine e l'utente CloudFront, CloudFront consulta. Protocolli e cifrari supportati tra visualizzatori e CloudFront

Richieste GET che includono un corpo

Se una `GET` richiesta del visualizzatore include un corpo, CloudFront restituisce al visualizzatore un codice di stato HTTP 403 (Proibito).

Metodi HTTP

Se configuri CloudFront per elaborare tutti i metodi HTTP che supporta, CloudFront accetta le seguenti richieste dai visualizzatori e le inoltra alla tua origine personalizzata:

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

CloudFront memorizza sempre nella cache le risposte e le richieste. `GET` `HEAD` È inoltre possibile configurare CloudFront la memorizzazione nella cache delle risposte alle `OPTIONS` richieste. CloudFront non memorizza nella cache le risposte alle richieste che utilizzano gli altri metodi.

Per ulteriori informazioni sulla configurazione relativa all'elaborazione di questi metodi mediante la tua origine personalizzata, consulta la documentazione relativa alla tua origine.

> **Important**
>
> Se configuri CloudFront per accettare e inoltrare all'origine tutti i metodi HTTP CloudFront supportati, configura il server di origine per gestire tutti i metodi. Ad esempio, se configuri per accettare e CloudFront inoltrare questi metodi perché desideri utilizzarli`POST`, devi configurare il server di origine in modo che gestisca `DELETE` le richieste in modo appropriato,

in modo che gli utenti non possano eliminare le risorse che non desideri. Per ulteriori informazioni, consulta la documentazione relativa al tuo server HTTP.

Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

La tabella che segue elenca le intestazioni di richieste HTTP che è possibile inoltrare alle origini personalizzate e Amazon S3 (con le eccezioni indicate). Per ciascuna intestazione, sono incluse le informazioni seguenti:

- CloudFront comportamento se non configuri l'intestazione CloudFront per inoltrare l'intestazione all'origine, il che comporta la memorizzazione nella cache degli oggetti in base CloudFront ai valori dell'intestazione.
- Se è possibile configurare la memorizzazione nella cache degli oggetti in base CloudFront ai valori di intestazione per quell'intestazione.

  Puoi CloudFront configurare la memorizzazione nella cache degli oggetti in base ai valori nelle `User-Agent` intestazioni `Date` and, ma non è consigliabile. Queste intestazioni hanno molti valori possibili e la memorizzazione nella cache in base ai loro valori CloudFront comporterebbe l'inoltro di un numero significativamente maggiore di richieste all'origine.

Per ulteriori informazioni sul caching in base ai valori di intestazione, consulta Caching dei contenuti in base alle intestazioni di richiesta.

Header	Comportamento se non configuri la memorizza zione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
Intestazioni definite da terzi	Impostazioni della cache legacy: CloudFront inoltra le intestazioni all'origine.	Sì
`Accept`	CloudFront rimuove l'intestazione.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`Accept-Charset`	CloudFront rimuove l'intestazione.	Sì
`Accept-Encoding`	Se il valore contiene `gzip` `obr`, CloudFront inoltra un'`Accept-Encoding` intestazione normalizzata all'origine. Per ulteriori informazioni, consultare Supporto della compressione e Distribuzione di file compressi.	Sì
`Accept-Language`	CloudFront rimuove l'intestazione.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`Authorization`	• `GET`e `HEAD` richieste: CloudFront rimuove il campo di `Authorization` intestazione prima di inoltrare la richiesta all'origine. • `OPTIONS`richieste: CloudFront rimuove il campo di `Authorization` intestazione prima di inoltrare la richiesta all'origine se CloudFront configuri la configurazione per memorizzare nella cache le risposte alle richieste. `OPTIONS` CloudFront inoltra il campo di `Authorization` intestazione all'origine se non si configura per memorizzare nella cache le risposte CloudFront alle richieste OPTIONS. • `DELETE`, `PATCH``POST`, e `PUT` richieste: CloudFront non rimuove il campo di intestazione prima di inoltrare la richiesta all'origine.	Sì
`Cache-Control`	CloudFront inoltra l'intestazione alla tua origine.	No
`CloudFront-Forwarded-Proto`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine. Per ulteriori informazioni, consulta Configurazione del caching in base al protocollo della richiesta.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`CloudFront-Is-Desktop-Viewer`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine. Per ulteriori informazioni, consulta Configurazione del caching in base al tipo di dispositivo.	Sì
`CloudFront-Is-Mobile-Viewer`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine. Per ulteriori informazioni, consulta Configurazione del caching in base al tipo di dispositivo.	Sì
`CloudFront-Is-Tablet-Viewer`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine. Per ulteriori informazioni, consulta Configurazione del caching in base al tipo di dispositivo.	Sì
`CloudFront-Viewer-Country`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine.	Sì
`Connection`	CloudFront sostituisce questa intestazione con `Connection: Keep-Alive` prima di inoltrare la richiesta all'origine.	No
`Content-Length`	CloudFront inoltra l'intestazione alla tua origine.	No
`Content-MD5`	CloudFront inoltra l'intestazione alla tua origine.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`Content-Type`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`Cookie`	Se configuri CloudFront per inoltrare i cookie, inoltrerà il campo di `Cookie` intestazione alla tua origine. In caso contrario, CloudFront rimuove il campo di `Cookie` intestazione. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.	No
`Date`	CloudFront inoltra l'intestazione alla tua origine.	Sì, ma non consigliato
`Expect`	CloudFront rimuove l'intestazione.	Sì
`From`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`Host`	CloudFront imposta il valore sul nome di dominio dell'origine associato all'oggetto richiesto. Non è possibile memorizzare nella cache in base all'intestazione Host per Amazon S3 MediaStore o sulle origini.	Sì (personalizzata) No (S3 e) MediaStore
`If-Match`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`If-Modified-Since`	CloudFront inoltra l'intestazione alla tua origine.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`If-None-Match`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`If-Range`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`If-Unmodified-Since`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`Max-Forwards`	CloudFront inoltra l'intestazione alla tua origine.	No
`Origin`	CloudFront inoltra l'intestazione alla tua origine.	Sì
`Pragma`	CloudFront inoltra l'intestazione alla tua origine.	No
`Proxy-Authenticate`	CloudFront rimuove l'intestazione.	No
`Proxy-Authorization`	CloudFront rimuove l'intestazione.	No
`Proxy-Connection`	CloudFront rimuove l'intestazione.	No
`Range`	CloudFront inoltra l'intestazione alla tua origine. Per ulteriori informazioni, consulta Come CloudFront elabora le richieste parziali per un oggetto (intervalloGETs).	Sì, per impostazione predefinita
`Referer`	CloudFront rimuove l'intestazione.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`Request-Range`	CloudFront inoltra l'intestazione alla tua origine.	No
`TE`	CloudFront rimuove l'intestazione.	No
`Trailer`	CloudFront rimuove l'intestazione.	No
`Transfer-Encoding`	CloudFront inoltra l'intestazione alla tua origine.	No
`Upgrade`	CloudFront rimuove l'intestazione, a meno che tu non abbia stabilito una connessione. WebSocket	No (eccetto per le WebSocket connessioni)
`User-Agent`	CloudFront sostituisce il valore di questo campo di intestazione con. `Amazon CloudFront` Se desideri CloudFront memorizzare nella cache i contenuti in base al dispositivo utilizzato dall'utente, consulta. Configurazione del caching in base al tipo di dispositivo	Sì, ma non consigliato
`Via`	CloudFront inoltra l'intestazione all'origine.	Sì
`Warning`	CloudFront inoltra l'intestazione alla tua origine.	Sì

Header	Comportamento se non configuri la memorizzazione nella cache CloudFront in base ai valori di intestazione	Supporto del caching in base ai valori di intestazione
`X-Amz-Cf-Id`	CloudFront aggiunge l'intestazione alla richiesta del visualizzatore prima di inoltrare la richiesta all'origine. Il valore di intestazione contiene una stringa crittografata che identifica in modo univoco la richiesta.	No
`X-Edge-*`	CloudFront rimuove tutte le intestazioni. `X-Edge-*`	No
`X-Forwarded-For`	CloudFront inoltra l'intestazione alla tua origine. Per ulteriori informazioni, consulta Indirizzi IP client.	Sì
`X-Forwarded-Proto`	CloudFront rimuove l'intestazione.	No
`X-HTTP-Method-Override`	CloudFront rimuove l'intestazione.	Sì
`X-Real-IP`	CloudFront rimuove l'intestazione.	No

Versione HTTP

CloudFront inoltra le richieste all'origine personalizzata utilizzando HTTP/1.1.

Lunghezza massima di una richiesta e lunghezza massima di un URL

La lunghezza massima di una richiesta, inclusi il percorso, l'eventuale stringa di query e le intestazioni, è di 20.480 byte.

CloudFront costruisce un URL dalla richiesta. La lunghezza massima di questo URL è di 8192 byte.

Se una richiesta o un URL supera questi valori massimi, CloudFront restituisce il codice di stato HTTP 413, Request Entity Too Large, al visualizzatore, quindi interrompe la connessione TCP con il visualizzatore.

Stapling OCSP

Quando un visualizzatore invia una richiesta HTTPS per un oggetto, uno dei due CloudFront o il visualizzatore deve confermare con l'autorità di certificazione (CA) che il certificato SSL per il dominio non è stato revocato. OCSP stapling velocizza la convalida dei certificati consentendo di CloudFront convalidare il certificato e di memorizzare nella cache la risposta della CA, in modo che il client non debba convalidare il certificato direttamente con la CA.

Il miglioramento delle prestazioni di OCSP Stapling è maggiore quando CloudFront riceve numerose richieste HTTPS per oggetti nello stesso dominio. Ogni server in una CloudFront edge location deve inviare una richiesta di convalida separata. Quando CloudFront riceve numerose richieste HTTPS per lo stesso dominio, ogni server nella edge location ottiene rapidamente una risposta dalla CA che può "spillare" a un pacchetto nell'handshake SSL; quando il visualizzatore è sicuro della validità del certificato, CloudFront può servire l'oggetto richiesto. Se la distribuzione non riceve molto traffico in una CloudFront edge location, è più probabile che le nuove richieste vengano indirizzate a un server che non ha ancora convalidato il certificato con la CA. In tal caso, il visualizzatore esegue separatamente la fase di convalida e il CloudFront server serve l'oggetto. Tale CloudFront server invia inoltre una richiesta di convalida alla CA, quindi la prossima volta che riceve una richiesta che include lo stesso nome di dominio, riceve una risposta di convalida dalla CA.

Connessioni persistenti

Quando CloudFront riceve una risposta dall'origine, tenta di mantenere la connessione per diversi secondi nel caso in cui arrivi un'altra richiesta durante quel periodo. Una connessione permanente consente di risparmiare il tempo necessario a ristabilire la connessione TCP e a eseguire un altro handshake TLS per le richieste successive.

Per ulteriori informazioni, incluso il modo in cui configurare la durata delle connessioni permanenti, consulta Timeout keep-alive (solo origini personalizzate e VPC) in questa sezione Riferimento a tutte le impostazioni di distribuzione.

Protocolli

CloudFront inoltra le richieste HTTP o HTTPS al server di origine in base a quanto segue:

- Il protocollo della richiesta a cui il visualizzatore invia CloudFront, HTTP o HTTPS.

- Il valore del campo Origin Protocol Policy nella CloudFront console o, se utilizzi l' CloudFront API, l'`OriginProtocolPolicy`elemento nel tipo `DistributionConfig` complesso. Nella CloudFront console, le opzioni sono Solo HTTP, Solo HTTPS e Match Viewer.

Se si specifica Solo HTTP o Solo HTTPS, CloudFront inoltra le richieste al server di origine utilizzando il protocollo specificato, indipendentemente dal protocollo nella richiesta del visualizzatore.

Se si specifica Match Viewer, CloudFront inoltra le richieste al server di origine utilizzando il protocollo nella richiesta del visualizzatore. Nota che CloudFront memorizza l'oggetto nella cache una sola volta anche se i visualizzatori effettuano richieste utilizzando entrambi i protocolli HTTP e HTTPS.

> **Important**
>
> Se CloudFront inoltra una richiesta all'origine utilizzando il protocollo HTTPS e se il server di origine restituisce un certificato non valido o un certificato autofirmato, CloudFront interrompe la connessione TCP.

Per informazioni su come aggiornare una distribuzione utilizzando la console, consulta CloudFront . Aggiornamento di una distribuzione Per informazioni su come aggiornare una distribuzione utilizzando l' CloudFront API, consulta UpdateDistributionAmazon CloudFront API Reference.

Stringhe di query

Puoi configurare se CloudFront inoltrare i parametri della stringa di query alla tua origine. Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

Timeout connessione origine e tentativi

Il timeout della connessione Origin è il numero di secondi che CloudFront attendono quando si tenta di stabilire una connessione all'origine.

I tentativi di connessione all'origine sono il numero di CloudFront tentativi di connessione all'origine.

Insieme, queste impostazioni determinano la durata dei CloudFront tentativi di connessione all'origine prima di passare all'origine secondaria (nel caso di un gruppo di origine) o restituire una risposta

di errore al visualizzatore. Per impostazione predefinita, CloudFront attende fino a 30 secondi (3 tentativi da 10 secondi ciascuno) prima di tentare di connettersi all'origine secondaria o restituire una risposta di errore. Puoi ridurre questo tempo specificando un timeout di connessione più breve, un numero inferiore di tentativi o entrambi.

Per ulteriori informazioni, consulta Controllo dei timeout e dei tentativi di origine.

Timeout di risposta dell'origine

Il timeout di risposta origine, noto anche come timeout di lettura origine o timeout di richiesta origine, si applica a entrambi i valori seguenti:

- La quantità di tempo, in secondi, che CloudFront attende una risposta dopo l'inoltro di una richiesta all'origine.
- La quantità di tempo, in secondi, che CloudFront attende dopo aver ricevuto un pacchetto di risposta dall'origine e prima di ricevere il pacchetto successivo.

CloudFront il comportamento dipende dal metodo HTTP della richiesta del visualizzatore:

- `GET`e `HEAD` richieste: se l'origine non risponde o smette di rispondere entro la durata del timeout di risposta, CloudFront interrompe la connessione. Se il numero specificato di tentativi di connessione all'origine è superiore a 1, CloudFront riprova per ottenere una risposta completa. CloudFront prova fino a 3 volte, in base al valore dell'impostazione dei tentativi di connessione di origine. Se l'origine non risponde durante il terzo tentativo, CloudFront non riprova fino a che non riceve un'altra richiesta per il contenuto sulla stessa origine.
- `DELETE`,`OPTIONS`, `PATCH`PUT, e `POST` richieste: se l'origine non risponde per la durata del timeout di lettura, CloudFront interrompe la connessione e non riprova a contattare l'origine. Il client può inoltrare nuovamente la richiesta, se necessario.

Per ulteriori informazioni, incluso il modo in cui configurare il timeout di risposta origine, consulta Timeout di risposta.

Richieste simultanee per lo stesso oggetto (compressione richieste)

Quando una CloudFront edge location riceve una richiesta per un oggetto e l'oggetto non è presente nella cache o l'oggetto memorizzato nella cache è scaduto, invia CloudFront immediatamente la richiesta all'origine. Tuttavia, se ci sono richieste simultanee per lo stesso oggetto, ovvero se

richieste aggiuntive per lo stesso oggetto (con la stessa chiave di cache) arrivano all'edge location prima di CloudFront ricevere la risposta alla prima richiesta, si CloudFront interrompe prima di inoltrare le richieste aggiuntive all'origine. Questa breve pausa aiuta a ridurre il carico sull'origine. CloudFront invia la risposta dalla richiesta originale a tutte le richieste ricevute mentre era in pausa. Questa operazione è chiamata compressione richieste. Nei CloudFront log, la prima richiesta viene identificata come una `Miss` nel `x-edge-result-type` campo e le richieste compresse vengono identificate come a. `Hit` Per ulteriori informazioni sui CloudFront log, vedere. the section called "CloudFront e registrazione delle funzioni edge"

CloudFront comprime solo le richieste che condividono una chiave di cache. Se le richieste aggiuntive non condividono la stessa chiave di cache perché, ad esempio, hai configurato la cache in base CloudFront alle intestazioni delle richieste o ai cookie o alle stringhe di query, CloudFront inoltra tutte le richieste con una chiave di cache univoca all'origine.

Se desideri impedire la compressione di tutte le richieste, puoi utilizzare la policy della cache gestita `CachingDisabled`, che impedisce anche il caching. Per ulteriori informazioni, consulta Utilizzo delle policy della cache gestite.

Se desideri evitare la compressione delle richieste per oggetti specifici, puoi impostare il TTL minimo per il comportamento cache su 0 e configurare l'origine in modo che invii `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` o `Cache-Control: s-maxage=0`. Queste configurazioni aumenteranno il carico sull'origine e introdurranno una latenza aggiuntiva per le richieste simultanee che vengono messe in pausa durante l' CloudFront attesa della risposta alla prima richiesta.

> **Important**
>
> Attualmente, CloudFront non supporta la compressione della richiesta se si abilita l'inoltro dei cookie nella politica della cache, nella politica di richiesta di origine o nelle impostazioni della cache legacy.

`User-Agent` Intestazione

Se desideri CloudFront memorizzare nella cache diverse versioni dei tuoi oggetti in base al dispositivo utilizzato dall'utente per visualizzare i tuoi contenuti, ti consigliamo di configurare l'inoltro CloudFront di una o più delle seguenti intestazioni all'origine personalizzata:

- `CloudFront-Is-Desktop-Viewer`

- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

In base al valore dell'`User-Agent`intestazione, CloudFront imposta il valore di queste intestazioni su `true` o `false` prima di inoltrare la richiesta all'origine. Se il dispositivo ricade in più di una categoria, allora più di un valore potrebbe essere `true`. Ad esempio, per alcuni dispositivi tablet, CloudFront potrebbe impostare `CloudFront-Is-Mobile-Viewer` e `CloudFront-Is-Tablet-Viewer` su `true`. Per ulteriori informazioni sulla configurazione della cache in base CloudFront alle intestazioni delle richieste, consulta. Caching dei contenuti in base alle intestazioni di richiesta

Puoi CloudFront configurare la memorizzazione nella cache degli oggetti in base ai valori nell'`User-Agent`intestazione, ma non è consigliabile. L'`User-Agent`intestazione ha molti valori possibili e la memorizzazione nella cache basata su tali valori CloudFront comporterebbe l'inoltro di un numero significativamente maggiore di richieste all'origine.

Se non configuri CloudFront per memorizzare nella cache gli oggetti in base ai valori dell'`User-Agent`intestazione, CloudFront aggiunge un'`User-Agent`intestazione con il seguente valore prima di inoltrare una richiesta all'origine:

```
User-Agent = Amazon CloudFront
```

CloudFront aggiunge questa intestazione indipendentemente dal fatto che la richiesta del visualizzatore includa un'intestazione. `User-Agent` Se la richiesta del visualizzatore include un'`User-Agent`intestazione, CloudFront la rimuove.

In che modo CloudFront elabora le risposte dalla tua origine personalizzata

Scopri come CloudFront elabora le risposte dalla tua origine personalizzata.

Indice

- Connessioni TCP interrotte
- Intestazioni di risposta HTTP che CloudFront rimuovono o sostituiscono
- Dimensione massima del file memorizzabile nella cache
- Origine non disponibile
- Reindirizzamenti
- Transfer-Encoding Intestazione

Risposte `100 Continue`

La tua origine non può inviare più di una risposta di 100-Continue a. CloudFront Dopo la prima risposta 100-Continue, CloudFront si aspetta una risposta HTTP 200 OK. Se Origin invia un'altra risposta 100-Continue dopo la prima, CloudFront restituirà un errore.

Caching

- Accertati che il server di origine imposti valori validi e accurati per i campi di intestazione `Date` e `Last-Modified`.
- CloudFront normalmente rispetta un'`Cache-Control: no-cache`intestazione nella risposta dall'origine. Per un'eccezione, consulta Richieste simultanee per lo stesso oggetto (compressione richieste).

Richieste annullate

Se un oggetto non si trova nella cache edge e se un visualizzatore termina una sessione (ad esempio, chiude un browser) dopo aver CloudFront recuperato l'oggetto dall'origine ma prima che possa consegnare l'oggetto richiesto, CloudFront non memorizza l'oggetto nella cache dell'edge location.

Negoziazione di contenuto

Se la tua origine ritorna `Vary:*` nella risposta e se il valore di Minimum TTL per il comportamento della cache corrispondente è 0, CloudFront memorizza l'oggetto nella cache ma inoltra comunque ogni richiesta successiva dell'oggetto all'origine per confermare che la cache contiene la versione più recente dell'oggetto. CloudFront non include intestazioni condizionali, come o. `If-None-Match` `If-Modified-Since` Di conseguenza, la tua origine restituisce l'oggetto a CloudFront in risposta a ogni richiesta.

Se la tua origine ritorna `Vary:*` nella risposta e se il valore di Minimum TTL per il comportamento della cache corrispondente è qualsiasi altro valore, CloudFront elabora l'`Vary`intestazione come descritto in. Intestazioni di risposta HTTP che CloudFront rimuovono o sostituiscono

Cookie

Se abiliti i cookie per un comportamento nella cache e se l'origine restituisce i cookie con un oggetto, CloudFront memorizza nella cache sia l'oggetto che i cookie. Nota che ciò riduce la capacità di memorizzazione nella cache per un oggetto. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.

Connessioni TCP interrotte

Se la connessione TCP tra CloudFront e l'origine si interrompe mentre l'origine restituisce un oggetto CloudFront, CloudFront il comportamento dipende dal fatto che l'origine abbia incluso un'`Content-Length`intestazione nella risposta:

- Intestazione Content-Length: CloudFront restituisce l'oggetto al visualizzatore non appena quest'ultimo lo riceve dall'origine. Tuttavia, se il valore dell'`Content-Length`intestazione non corrisponde alla dimensione dell'oggetto, CloudFront non memorizza l'oggetto nella cache.
- Transfer-Encoding: Chunked: CloudFront restituisce l'oggetto al visualizzatore man mano che lo ottiene dall'origine. Tuttavia, se la risposta suddivisa in blocchi non è completa, l'oggetto non viene memorizzato nella cache. CloudFront
- Nessuna intestazione Content-Length: CloudFront restituisce l'oggetto al visualizzatore e lo memorizza nella cache, ma l'oggetto potrebbe non essere completo. Senza un'intestazione `Content-Length`, CloudFront non è in grado di determinare se la connessione TCP è stata interrotta per errore o intenzionalmente.

Si consiglia di configurare il server HTTP per aggiungere un'`Content-Length`intestazione per impedire CloudFront la memorizzazione nella cache di oggetti parziali.

Intestazioni di risposta HTTP che CloudFront rimuovono o sostituiscono

CloudFront rimuove o aggiorna i seguenti campi di intestazione prima di inoltrare la risposta dall'origine al visualizzatore:

- `Set-Cookie`— Se configuri CloudFront per inoltrare i cookie, inoltrerà il campo di `Set-Cookie` intestazione ai client. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.

- `Trailer`
- `Transfer-Encoding`— Se la tua origine restituisce questo campo di intestazione, CloudFront imposta il valore su `chunked` prima di restituire la risposta allo spettatore.
- `Upgrade`
- `Vary` - Tieni presente quanto segue:
  - Se configuri CloudFront per inoltrare qualsiasi intestazione specifica del dispositivo all'origine (`CloudFront-Is-Desktop-Viewer`,, `CloudFront-Is-Mobile-ViewerCloudFront-Is-SmartTV-Viewer`,`CloudFront-Is-Tablet-Viewer`) e configuri l'origine per tornare a CloudFront, CloudFront ritorna `Vary:User-Agent` al visualizzatore. `Vary:User-Agent` Per ulteriori informazioni, consulta Configurazione del caching in base al tipo di dispositivo.
  - Se configuri l'origine per includere una delle due `Accept-Encoding` o `Cookie` nell'`Vary`intestazione, CloudFront include i valori nella risposta al visualizzatore.
  - Se configuri CloudFront per inoltrare le intestazioni all'origine e se configuri l'origine per restituire i nomi delle intestazioni CloudFront nell'`Vary`intestazione (ad esempio,`Vary:Accept-Charset,Accept-Language`), CloudFront restituisce l'`Vary`intestazione con quei valori al visualizzatore.
  - Per informazioni su come CloudFront elabora un valore di `*` nell'intestazione, consulta`Vary`. Negoziazione di contenuto
  - Se configuri l'origine per includere altri valori nell'`Vary`intestazione, CloudFront rimuove i valori prima di restituire la risposta al visualizzatore.
- `Via`— CloudFront imposta il valore seguente nella risposta al visualizzatore:

  `Via: http-version alphanumeric-string.cloudfront.net (CloudFront)`

  Ad esempio, il valore è simile al seguente:

  `Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)`

Dimensione massima del file memorizzabile nella cache

La dimensione massima di un corpo di risposta che viene CloudFront salvato nella cache è di 50 GB. Questa dimensione include risposte di trasferimento in blocchi che non specificano il valore di intestazione `Content-Length`.

È possibile utilizzare CloudFront per memorizzare nella cache un oggetto di dimensioni maggiori di tali dimensioni utilizzando le richieste di intervallo per richiedere gli oggetti in parti di dimensioni pari

o inferiori a 50 GB ciascuna. CloudFrontmemorizza nella cache queste parti perché ognuna di esse pesa 50 GB o meno. Dopo che il visualizzatore ha recuperato tutte le parti dell'oggetto, può ricostruire l'oggetto originale più grande. Per ulteriori informazioni, consulta Utilizzare richieste di intervallo per memorizzare nella cache oggetti di grandi dimensioni.

Origine non disponibile

Se il server di origine non è disponibile e CloudFront riceve una richiesta per un oggetto che si trova nella cache edge ma che è scaduto (ad esempio, perché è trascorso il periodo di tempo specificato nella `Cache-Control max-age` direttiva), CloudFront fornisce la versione scaduta dell'oggetto o visualizza una pagina di errore personalizzata. Per ulteriori informazioni sul CloudFront comportamento quando hai configurato pagine di errore personalizzate, consulta. In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate

In alcuni casi, un oggetto che viene richiesto raramente viene rimosso e non è più disponibile nella cache edge. CloudFront non può servire un oggetto che è stato sfrattato.

Reindirizzamenti

Se modifichi la posizione di un oggetto nel server di origine, puoi configurare il tuo server Web per reindirizzare le richieste alla nuova posizione. Dopo aver configurato il reindirizzamento, la prima volta che un visualizzatore invia una richiesta per l'oggetto, CloudFront invia la richiesta all'origine e l'origine risponde con un reindirizzamento (ad esempio,). `302 Moved Temporarily` CloudFront memorizza nella cache il reindirizzamento e lo restituisce al visualizzatore. CloudFront non segue il reindirizzamento.

Puoi configurare il server Web per reindirizzare le richieste a una delle seguenti posizioni:

- Il nuovo URL dell'oggetto sul server di origine. Quando il visualizzatore segue il reindirizzamento al nuovo URL, lo ignora CloudFront e passa direttamente all'origine. Di conseguenza, ti consigliamo di non reindirizzare le richieste al nuovo URL dell'oggetto sull'origine.
- Il nuovo CloudFront URL per l'oggetto. Quando il visualizzatore invia la richiesta che contiene il nuovo CloudFront URL, CloudFront ottiene l'oggetto dalla nuova posizione sull'origine, lo memorizza nella cache nella posizione periferica e restituisce l'oggetto al visualizzatore. Le richieste successive per l'oggetto saranno servite dalla edge location. In questo modo, si evita la latenza e il carico associati ai visualizzatori che richiedono l'oggetto dall'origine. Tuttavia, ogni nuova richiesta per l'oggetto comporta spese per due richieste a CloudFront.

`Transfer-Encoding` Intestazione

CloudFront supporta solo il `chunked` valore dell'intestazione. `Transfer-Encoding` Se l'origine viene restituita`Transfer-Encoding: chunked`, CloudFront restituisce l'oggetto al client non appena l'oggetto viene ricevuto dall'edge location e memorizza l'oggetto nella cache in formato a blocchi per le richieste successive.

Se il visualizzatore effettua una `Range GET` richiesta e l'origine viene restituita`Transfer-Encoding: chunked`, CloudFront restituisce l'intero oggetto al visualizzatore anziché l'intervallo richiesto.

Ti consigliamo di utilizzare la codifica Chunked se la lunghezza del contenuto della tua risposta non può essere predeterminata. Per ulteriori informazioni, consulta Connessioni TCP interrotte.

Comportamento di richieste e risposte per i gruppi di origine

Le richieste a un gruppo di origine funzionano allo stesso modo delle richieste a un'origine non impostata come gruppo di origine, tranne quando è presente un failover di origine. Come per qualsiasi altra origine, quando CloudFront riceve una richiesta e il contenuto è già memorizzato nella cache in una posizione periferica, il contenuto viene fornito agli utenti dalla cache. Quando c'è un errore nella cache e l'origine è un gruppo di origine, le richieste dei visualizzatori vengono inoltrate all'origine primaria nel gruppo di origine.

Il comportamento di richiesta e risposta per l'origine primaria è uguale a quella per un'origine che non è inclusa in un gruppo di origine. Per ulteriori informazioni, consulta Comportamento di richieste e risposte per origini Amazon S3 e Comportamento di richieste e risposte per origini personalizzate.

I seguenti descrivono il comportamento per il failover di origine quando l'origine primaria restituisce i codici di stato HTTP specifici:

- Codice di stato HTTP 2xx (operazione riuscita): CloudFront memorizza il file nella cache e lo restituisce al visualizzatore.
- Codice di stato HTTP 3xx (reindirizzamento): CloudFront restituisce il codice di stato al visualizzatore.
- Codice di stato HTTP 4xx o 5xx (errore client/server): se il codice di stato restituito è stato configurato per il failover, CloudFront invia la stessa richiesta all'origine secondaria nel gruppo di origine.

- Codice di stato HTTP 4xx o 5xx (errore client/server): se il codice di stato restituito non è stato configurato per il failover, restituisce l'errore al visualizzatore. CloudFront

CloudFront esegue il failover sull'origine secondaria solo quando il metodo HTTP della richiesta del visualizzatore è, o. `GET` `HEAD` `OPTIONS` CloudFront non esegue il failover quando il visualizzatore invia un metodo HTTP diverso (ad esempio `POSTPUT`, e così via).

Quando CloudFront invia una richiesta a un'origine secondaria, il comportamento di risposta è lo stesso di un' CloudFront origine che non appartiene a un gruppo di origine.

Per ulteriori informazioni sui gruppi di origine, consulta Ottimizzazione dell'elevata disponibilità con il failover di origine CloudFront.

Aggiunta di intestazioni personalizzate alle richieste di origine

È possibile configurare CloudFront per aggiungere intestazioni personalizzate alle richieste inviate all'origine. Puoi utilizzare intestazioni personalizzate per inviare e raccogliere informazioni dall'origine che non si ottengono con richieste tipiche del visualizzatore. Puoi anche personalizzare le intestazioni per ogni origine. CloudFront supporta intestazioni personalizzate per origini personalizzate e origini Amazon S3.

Indice

Casi d'uso

Puoi utilizzare intestazioni personalizzate, come riportato nei seguenti esempi:

Identificazione delle richieste da CloudFront

> È possibile identificare le richieste che l'origine riceve da CloudFront. Ciò è utile per sapere se gli utenti aggirano CloudFront oppure se usano più di un CDN per ottenere informazioni su quali richieste provengono da ogni CDN.

> **Note**
>
> Se utilizzi un'origine Amazon S3 e attivi la registrazione degli accessi al server Amazon S3, i log non includono le informazioni dell'intestazione.

Determinare quali richieste provengono da una particolare distribuzione

Se si configura più di una distribuzione CloudFront per utilizzare la stessa origine, è possibile aggiungere intestazioni personalizzate diverse in ogni distribuzione. È quindi possibile utilizzare i registri dell'origine per determinare quali richieste provengono da quale distribuzione CloudFront.

Abilitazione della funzionalità Cross-Origin Resource Sharing (CORS)

Se alcuni dei visualizzatori non supportano CORS (Cross-origin Resource Sharing), è possibile configurare CloudFront per aggiungere sempre l'intestazione `Origin` alle richieste inviate all'origine. Quindi puoi configurare la tua origine per restituire l'intestazione `Access-Control-Allow-Origin` per ogni richiesta. È inoltre necessario configurare CloudFront per rispettare le impostazioni CORS.

Controllo dell'accesso ai contenuti

È possibile utilizzare intestazioni personalizzate per controllare l'accesso ai contenuti. Configurando l'origine per rispondere alle richieste solo quando includono un'intestazione personalizzata aggiunta da CloudFront, si impedisce agli utenti di ignorare CloudFront e accedere al contenuto direttamente sull'origine. Per ulteriori informazioni, consulta Limitazione dell'accesso ai file su origini personalizzate.

Configurazione di CloudFront per aggiungere intestazioni personalizzate alle richieste origine

Per configurare una distribuzione in modo da aggiungere intestazioni personalizzate alle richieste inviate all'origine, aggiornare la configurazione di origine utilizzando uno dei seguenti metodi:

- Console CloudFront: quando crei o aggiorni una distribuzione, specifica i nomi e i valori delle intestazioni nelle impostazioni Aggiungi intestazioni personalizzate. Per ulteriori informazioni, consulta Aggiunta di intestazioni personalizzate.
- API CloudFront: per ogni origine a cui si desidera aggiungere intestazioni personalizzate, specificare i nomi e i valori dell'intestazione nel campo `CustomHeaders` all'interno di `Origin`. Per

ulteriori informazioni, consulta CreateDistribution o UpdateDistribution nella Documentazione di riferimento delle API di Amazon CloudFront.

Se i nomi e i valori delle intestazioni che specifichi non sono già presenti nella richiesta del visualizzatore, CloudFront li aggiunge alla richiesta di origine. Se un'intestazione è presente, CloudFront sovrascrive il valore dell'intestazione prima di inoltrare la richiesta all'origine.

Per le quote che si applicano alle intestazioni personalizzate di origine, consulta Quote delle intestazioni.

Intestazioni personalizzate che CloudFront non può aggiungere alle richieste di origine

Non è possibile configurare CloudFront per l'aggiunta di una delle seguenti intestazioni alle richieste inviate all'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-Authenticate`
- `Proxy-Authorization`
- `Proxy-Connection`
- `Range`

- `Request-Range`
- `TE`
- `Trailer`
- `Transfer-Encoding`
- `Upgrade`
- `Via`
- Intestazioni che iniziano con `X-Amz-`
- Intestazioni che iniziano con `X-Edge-`
- `X-Real-Ip`

Configurazione di CloudFront per inoltrare l'intestazione **`Authorization`**

Quando CloudFront inoltra una richiesta di visualizzatore all'origine, CloudFront rimuove alcune intestazioni del visualizzatore per impostazione predefinita, inclusa l'intestazione `Authorization`. Per assicurarti che l'origine riceva sempre l'intestazione `Authorization` nelle richieste di origine, sono disponibili le seguenti opzioni:

- Aggiungere l'intestazione `Authorization` alla chiave cache utilizzando una policy di cache. Tutte le intestazioni nella chiave cache vengono incluse automaticamente nelle richieste di origine. Per ulteriori informazioni, consulta Controllo della chiave della cache con una policy.
- Utilizzare una policy di richiesta di origine che inoltra tutte le intestazioni del visualizzatore all'origine. Non è possibile inoltrare l'intestazione `Authorization` singolarmente in una policy di richiesta di origine, ma quando si inoltrano tutte le intestazioni del visualizzatore, CloudFront include l'intestazione `Authorization` nelle richieste del visualizzatore. CloudFront fornisce una policy di richiesta di origine gestita per questo caso d'uso, denominata Managed-AllViewer. Per ulteriori informazioni, consulta Utilizzo delle policy di richiesta origine gestite.

Come CloudFront elabora le richieste parziali per un oggetto (intervalloGETs)

Per un oggetto di grandi dimensioni, il visualizzatore (il browser web o un altro client) può eseguire più richieste `GET` e utilizzare l'intestazione della richiesta `Range` per scaricare l'oggetto in parti più piccole. Queste richieste per intervalli di byte, talvolta note come richieste `Range GET`, migliorano l'efficienza di download parziali e il ripristino da parte di trasferimenti in parte non riusciti.

Quando CloudFront riceve una `Range GET` richiesta, controlla la cache nell'edge location che ha ricevuto la richiesta. Se la cache in quella edge location contiene già l'intero oggetto o la parte dell'oggetto richiesta, serve CloudFront immediatamente l'intervallo richiesto dalla cache.

Se la cache non contiene l'intervallo richiesto, CloudFront inoltra la richiesta all'origine. (Per ottimizzare le prestazioni, CloudFront può richiedere un intervallo più ampio di quello richiesto dal client in`Range GET`.) Cosa succede dopo varia a seconda che il server di origine supporti o meno le richieste `Range GET`:

- Se l'origine supporta **`Range GET`** le richieste, restituisce l'intervallo richiesto. CloudFront serve l'intervallo richiesto e lo memorizza anche nella cache per richieste future. (Amazon S3) supporta le richieste `Range GET`, così come molti server HTTP.)
- Se l'origine non supporta **`Range GET`** le richieste, restituisce l'intero oggetto. CloudFront serve la richiesta corrente inviando l'intero oggetto e memorizzandolo anche nella cache per richieste future. Dopo aver CloudFront memorizzato l'intero oggetto in una cache edge, risponde alle nuove `Range GET` richieste servendo l'intervallo richiesto.

In entrambi i casi, CloudFront inizia a servire l'intervallo o l'oggetto richiesto all'utente finale non appena il primo byte arriva dall'origine.

> **Note**
>
> Se il visualizzatore effettua una `Range GET` richiesta e l'origine CloudFront ritorna`Transfer-Encoding: chunked`, restituisce l'intero oggetto al visualizzatore anziché l'intervallo richiesto.

CloudFront segue generalmente le specifiche RFC per l'`Range`intestazione. Tuttavia, se le intestazioni `Range` non rispettano i seguenti requisiti, CloudFront restituirà il codice di stato `200` con l'oggetto completo invece del codice di stato `206` con gli intervalli specificati:

- Gli intervalli devono essere elencati in ordine crescente. Ad esempio, `100-200,300-400` è valido, `300-400,100-200` non è valido.
- Gli intervalli non devono sovrapporsi. Ad esempio, `100-200,150-250` non è valido.
- Tutti le specifiche degli intervalli devono essere valide. Ad esempio, non puoi specificare un valore negativo come parte di un intervallo.

Per ulteriori informazioni su intestazione della richiesta `Range`, consulta Richieste di intervallo in RFC 7233 oppure Range nei documenti Web MDN.

Utilizzare richieste di intervallo per memorizzare nella cache oggetti di grandi dimensioni

Quando la memorizzazione nella cache è abilitata, CloudFront non recupera o memorizza nella cache un oggetto di dimensioni superiori a 50 GB. Quando un'origine indica che l'oggetto è più grande di questa dimensione (nell'intestazione della `Content-Length` risposta), CloudFront chiude la connessione all'origine e restituisce un errore al visualizzatore. (Con la memorizzazione nella cache disattivata, CloudFront può recuperare un oggetto più grande di questa dimensione dall'origine e passarlo al visualizzatore. Tuttavia, CloudFront non memorizza l'oggetto nella cache.)

Tuttavia, con le richieste di intervallo, è possibile utilizzare CloudFront per memorizzare nella cache un oggetto che è più grande della dimensione massima del file memorizzabile nella cache.

Example Esempio

1. Considera un'origine con un oggetto da 100 GB. Con la memorizzazione nella cache abilitata, CloudFront non recupera o memorizza nella cache un oggetto così grande. Tuttavia, il visualizzatore può inviare più richieste di intervallo per recuperare l'oggetto in parti, con ciascuna parte inferiore a 50 GB.
2. Il visualizzatore può richiedere l'oggetto in parti da 20 GB inviando una richiesta con l'intestazione `Range: bytes=0-21474836480` per recuperare la prima parte, un'altra richiesta con l'intestazione `Range: bytes=21474836481-42949672960` per recuperare la parte successiva e così via.
3. Quando il visualizzatore ha ricevuto tutte le parti, può combinarle per costruire l'oggetto originale da 100 GB.
4. In questo caso, CloudFront memorizza nella cache ciascuna delle parti da 20 GB dell'oggetto e può rispondere alle richieste successive per la stessa parte dalla cache.

Per una richiesta di intervallo relativa a un oggetto compresso, la richiesta di intervallo di byte si basa sulla dimensione compressa e non sulla dimensione originale dell'oggetto. Per ulteriori informazioni su questi file di compressione, consulta Distribuzione di file compressi.

In che modo CloudFront elabora i codici di stato HTTP 3xx dalla tua origine

Quando CloudFront richiede un oggetto dal bucket Amazon S3 o dal server di origine personalizzato, l'origine a volte restituisce un codice di stato HTTP 3xx. Il messaggio generalmente indica di procedere in uno dei seguenti modi:

- L'URL dell'oggetto è stato modificato (ad esempio, codici di stato 301, 302, 307 o 308)
- L'oggetto non è cambiato dall'ultima volta che lo ha CloudFront richiesto (codice di stato 304)

CloudFront memorizza nella cache le risposte 3xx in base alle impostazioni della CloudFront distribuzione e alle intestazioni della risposta. CloudFront memorizza nella cache le risposte 307 e 308 solo quando includi l'`Cache-Control`intestazione nelle risposte dall'origine. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

Se la tua origine restituisce un codice di stato del reindirizzamento (ad esempio 301 o 307), CloudFront non segue il reindirizzamento. CloudFront trasmette la risposta 301 o 307 allo spettatore, che può seguire il reindirizzamento inviando una nuova richiesta.

In che modo CloudFront elabora i codici di stato HTTP 4xx e 5xx dalla tua origine

Quando CloudFront richiede un oggetto dal bucket Amazon S3 o dal server di origine personalizzato, l'origine a volte restituisce un codice di stato HTTP 4xx o 5xx, che indica che si è verificato un errore. CloudFront il comportamento dipende da:

- Se hai configurato le pagine di errore personalizzate.
- Se hai configurato per quanto tempo desideri CloudFront memorizzare nella cache le risposte agli errori dalla tua origine (errore di memorizzazione nella cache, TTL minimo)
- Il codice di stato
- Per i codici di stato 5xx, indica se l'oggetto richiesto si trova attualmente nella cache edge CloudFront
- Per alcuni codici di stato 4xx, se il server di origine restituisce un'intestazione `Cache-Control max-age` o `Cache-Control s-maxage`.

CloudFront memorizza sempre nella cache le risposte `GET` e `HEAD` le richieste. È inoltre possibile configurare CloudFront la memorizzazione nella cache delle risposte alle `OPTIONS` richieste. CloudFront non memorizza nella cache le risposte alle richieste che utilizzano gli altri metodi.

Se l'origine non risponde, la CloudFront richiesta all'origine scade, il che è considerato un errore HTTP 5xx dall'origine, anche se l'origine non ha risposto con quell'errore. In questo scenario, CloudFront continua a fornire contenuti memorizzati nella cache. Per ulteriori informazioni, consulta Origine non disponibile.

Se hai abilitato la registrazione, CloudFront scrive i risultati nei log indipendentemente dal codice di stato HTTP.

Per ulteriori informazioni sulle funzionalità e le opzioni relative al messaggio di errore restituito da CloudFront, consulta quanto segue:

- Per informazioni sulle impostazioni per le pagine di errore personalizzate nella CloudFront console, consultaCustom Error Pages and Error Caching (Pagine di errore personalizzate e caching errori).
- Per informazioni sugli errori relativi alla memorizzazione nella cache del TTL minimo nella CloudFront console, consulta. Error Caching Minimum TTL (seconds) (TTL minimo caching errori) (secondi)
- Per un elenco dei codici di stato HTTP memorizzati nella CloudFront cache, consulta. codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront

Argomenti

- In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate
- Come CloudFront elabora gli errori se non hai configurato pagine di errore personalizzate
- codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront

In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate

Se sono state configurate pagine di errore personalizzate, CloudFront il comportamento dipende dal fatto che l'oggetto richiesto si trovi nella cache edge.

L'oggetto richiesto non è nella cache edge

CloudFront continua a cercare di ottenere l'oggetto richiesto dall'origine quando tutte le seguenti condizioni sono vere:

- Un visualizzatore richiede un oggetto.
- L'oggetto non è nella cache edge.
- L'origine restituisce un codice di stato HTTP 4xx o 5xx e una delle condizioni seguenti è vera:
  - Il tuo server di origine restituisce un codice di stato HTTP 5xx anziché un codice di stato 304 (Non modificato) o una versione aggiornata dell'oggetto.
  - Il tuo server di origine restituisce un codice di stato HTTP 4xx che non è limitato da un'intestazione di controllo cache ed è incluso nell'elenco seguente di codici di stato: codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront .
  - Il server di origine restituisce un codice di stato HTTP 4xx con un'intestazione `Cache-Control max-age` o `Cache-Control s-maxage` e il codice di stato è incluso nel seguente elenco di codici di stato: Control Codici di stato HTTP 4xx che vengono memorizzati CloudFront nella cache in base alle intestazioni `Cache-Control`.

CloudFront fa quanto segue:

1. Nell' CloudFront edge cache che ha ricevuto la richiesta del visualizzatore, CloudFront controlla la configurazione della distribuzione e ottiene il percorso della pagina di errore personalizzata che corrisponde al codice di stato restituito dall'origine.
2. CloudFront trova il primo comportamento della cache nella distribuzione che presenta un modello di percorso che corrisponde al percorso della pagina di errore personalizzata.
3. L' CloudFront edge location invia una richiesta per la pagina di errore personalizzata all'origine specificata nel comportamento della cache.
4. L'origine restituisce la pagina di errore personalizzata alla edge location.
5. CloudFront restituisce la pagina di errore personalizzata al visualizzatore che ha effettuato la richiesta e inoltre memorizza nella cache la pagina di errore personalizzata per il massimo dei seguenti elementi:
   - La quantità di tempo specificata dal TTL minimo di caching degli errori (10 secondi per impostazione predefinita)
   - La quantità di tempo specificata da un'intestazione `Cache-Control max-age` o `Cache-Control s-maxage` restituita dall'origine quando la prima richiesta ha generato l'errore

6. Trascorso il tempo di memorizzazione nella cache (determinato nel passaggio 5), CloudFront riprova a recuperare l'oggetto richiesto inoltrando un'altra richiesta all'origine. CloudFront continua a riprovare a intervalli specificati dal TTL minimo di memorizzazione nella cache degli errori.

> **Note**
>
> Se hai configurato anche un comportamento di cache per la stessa pagina di errore personalizzata, CloudFront utilizza invece il comportamento della cache TTL. In questo caso, CloudFront eseguirà le seguenti operazioni per i passaggi 5 e 6:
>
> - Dopo aver CloudFront restituito la pagina di errore personalizzata al visualizzatore che ha effettuato la richiesta, CloudFront verifica il comportamento della cache TTL (ad esempio, si imposta il TTL predefinito su 5 secondi). CloudFront quindi memorizza nella cache la pagina di errore personalizzata fino a quel massimo.
> - CloudFront Trascorsi 5 secondi, recupera nuovamente la pagina di errore personalizzata dall'origine. CloudFront continuerà a riprovare a intervalli specificati dal comportamento della cache TTL.
>
> Per ulteriori informazioni, consulta Impostazioni TTL del comportamento cache.

L'oggetto richiesto è nella cache edge

CloudFront continua a servire l'oggetto che si trova attualmente nella cache edge quando tutte le seguenti condizioni sono vere:

- Un visualizzatore richiede un oggetto.
- L'oggetto è nella cache edge ma è scaduto.
- Il tuo server di origine restituisce un codice di stato HTTP 5xx anziché un codice di stato 304 (Non modificato) o una versione aggiornata dell'oggetto.

CloudFront fa quanto segue:

1. Se la tua origine restituisce un codice di stato 5xx, CloudFront serve l'oggetto anche se è scaduto. Per tutta la durata della memorizzazione degli errori nella cache, il TTL minimo CloudFront continua a rispondere alle richieste degli utenti servendo l'oggetto dalla cache perimetrale.

Se la tua origine restituisce un codice di stato 4xx, CloudFront restituisce il codice di stato, non l'oggetto richiesto, al visualizzatore.

2. Una volta trascorso il TTL minimo di memorizzazione dell'errore nella cache, CloudFront riprova a recuperare l'oggetto richiesto inoltrando un'altra richiesta all'origine. Tieni presente che se l'oggetto non viene richiesto frequentemente, CloudFront potresti eliminarlo dalla cache edge mentre il server di origine sta ancora restituendo 5xx risposte. Per informazioni sulla durata della permanenza degli oggetti nelle cache CloudFront edge, consulta. Gestione della durata di permanenza dei contenuti nella cache (scadenza)

Come CloudFront elabora gli errori se non hai configurato pagine di errore personalizzate

Se non hai configurato pagine di errore personalizzate, CloudFront il comportamento dipende dal fatto che l'oggetto richiesto si trovi nella cache edge.

Argomenti

- L'oggetto richiesto non è nella cache edge
- L'oggetto richiesto è nella cache edge

L'oggetto richiesto non è nella cache edge

CloudFront continua a cercare di ottenere l'oggetto richiesto dall'origine quando tutte le seguenti condizioni sono vere:

- Un visualizzatore richiede un oggetto.
- L'oggetto non è nella cache edge.
- L'origine restituisce un codice di stato HTTP 4xx o 5xx e una delle condizioni seguenti è vera:
  - Il tuo server di origine restituisce un codice di stato HTTP 5xx anziché un codice di stato 304 (Non modificato) o una versione aggiornata dell'oggetto.
  - Il tuo server di origine restituisce un codice di stato HTTP 4xx che non è limitato da un'intestazione di controllo cache ed è incluso nell'elenco seguente di codici di stato: codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront
  - Il server di origine restituisce un codice di stato HTTP 4xx con un'intestazione `Cache-Control max-age` o `Cache-Control s-maxage` e il codice di stato è incluso nel seguente elenco di

codici di stato: Control [Codici di stato HTTP 4xx che vengono memorizzati CloudFront nella cache in base alle intestazioni `Cache-Control`](#).

CloudFront fa quanto segue:

1. CloudFront restituisce il codice di stato 4xx o 5xx al visualizzatore e memorizza anche nella cache edge il codice di stato che ha ricevuto la richiesta per il massimo dei seguenti elementi:
   - La quantità di tempo specificata dal TTL minimo di caching degli errori (10 secondi per impostazione predefinita)
   - La quantità di tempo specificata da un'intestazione `Cache-Control max-age` o `Cache-Control s-maxage` restituita dall'origine quando la prima richiesta ha generato l'errore
2. Per la durata del TTL minimo di caching degli errori (determinato nella fase 1), CloudFront risponde alle richieste visualizzatore successive per lo stesso oggetto con il codice di stato 4xx o 5xx memorizzato nella cache.
3. Trascorso il tempo di memorizzazione nella cache (determinato nel passaggio 1), CloudFront riprova a recuperare l'oggetto richiesto inoltrando un'altra richiesta all'origine. CloudFront continua a riprovare a intervalli specificati dal TTL minimo di memorizzazione nella cache degli errori.

L'oggetto richiesto è nella cache edge

CloudFront continua a servire l'oggetto che si trova attualmente nella cache edge quando tutte le seguenti condizioni sono vere:

- Un visualizzatore richiede un oggetto.
- L'oggetto è nella cache edge ma è scaduto. Ciò significa che l’oggetto è obsoleto.
- Il tuo server di origine restituisce un codice di stato HTTP 5xx anziché un codice di stato 304 (Non modificato) o una versione aggiornata dell'oggetto.

CloudFront fa quanto segue:

1. Se la tua origine restituisce un codice di errore 5xx, CloudFront serve l'oggetto anche se è scaduto. Per la durata del TTL minimo di memorizzazione nella cache degli errori (10 secondi per impostazione predefinita), CloudFront continua a rispondere alle richieste degli utenti servendo l'oggetto dalla cache edge.

Se la tua origine restituisce un codice di stato 4xx, CloudFront restituisce il codice di stato, non l'oggetto richiesto, al visualizzatore.

2. Una volta trascorso il TTL minimo di memorizzazione dell'errore nella cache, CloudFront riprova a recuperare l'oggetto richiesto inoltrando un'altra richiesta all'origine. Se l'oggetto non viene richiesto frequentemente, è CloudFront possibile eliminarlo dalla cache edge mentre il server di origine restituisce ancora 5xx risposte. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

> **Tip**
>
> - Se configuri la direttiva `stale-if-error` o `Stale-While-Revalidate`, puoi specificare per quanto tempo gli oggetti obsoleti sono disponibili nella cache edge. Ciò consente di continuare a offrire contenuti ai visualizzatori anche quando l'origine non è disponibile. Per informazioni, consulta Fornire contenuti obsoleti (scaduti).
> - CloudFront servirà solo un oggetto obsoleto fino al valore TTL massimo specificato. Dopo questo periodo, l'oggetto non sarà più disponibile dalla cache edge.

codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront

CloudFront memorizza nella cache i codici di stato HTTP 4xx e 5xx restituiti dall'origine, a seconda del codice di stato specifico restituito e del fatto che l'origine restituisca intestazioni specifiche nella risposta.

CloudFront memorizza nella cache i seguenti codici di stato HTTP 4xx e 5xx restituiti dall'origine. Se hai configurato una pagina di errore personalizzata per un codice di stato HTTP, CloudFront memorizza nella cache la pagina di errore personalizzata.

> **Note**
>
> Se utilizzi la politica di cache CachingDisabled gestita, CloudFront non memorizzerà nella cache questi codici di stato o pagine di errore personalizzate.

404	Non trovato
414	URI della richiesta troppo grande
500	Errore interno del server
501	Non ancora disponibile
502	Gateway non valido
503	Servizio non disponibile
504	Timeout gateway

Codici di stato HTTP 4xx che vengono memorizzati CloudFront nella cache in base alle intestazioni **`Cache-Control`**

CloudFront memorizza nella cache solo i seguenti codici di stato HTTP 4xx restituiti dall'origine solo se l'origine restituisce un'intestazione or. `Cache-Control max-age` `Cache-Control s-maxage` Se hai configurato una pagina di errore personalizzata per uno di questi codici di stato HTTP e la tua origine restituisce una delle intestazioni di controllo della cache, memorizza nella cache la pagina di errore personalizzata. CloudFront

400	Richiesta non valida
403	Accesso negato
405	Metodo non consentito
412[1]	Precondizione non riuscita

415[1]	Tipo di supporto non supportato

[1] CloudFront non supporta la creazione di pagine di errore personalizzate per questi codici di stato HTTP.

Generazione di risposte di errore personalizzate

Se un oggetto tramite il quale stai servendo non CloudFront è disponibile per qualche motivo, il tuo server web in genere restituisce un codice di stato HTTP pertinente CloudFront per indicarlo. Ad esempio, se un visualizzatore richiede un URL non valido, il server Web restituisce un codice di stato HTTP 404 (Not Found) a CloudFront, quindi lo CloudFront restituisce al visualizzatore. Invece di utilizzare questa risposta di errore predefinita, è possibile crearne una personalizzata che CloudFront ritorni al visualizzatore.

Se configurate CloudFront per restituire una pagina di errore personalizzata per un codice di stato HTTP ma la pagina di errore personalizzata non è disponibile, CloudFront restituisce al visualizzatore il codice di stato CloudFront ricevuto dall'origine che contiene le pagine di errore personalizzate. Ad esempio, supponiamo che l'origine personalizzata restituisca un codice di stato 500 e che tu abbia configurato CloudFront per ottenere una pagina di errore personalizzata per un codice di stato 500 da un bucket Amazon S3. Tuttavia, qualcuno ha eliminato accidentalmente la pagina di errore personalizzata dal tuo bucket Amazon S3. CloudFront restituisce un codice di stato HTTP 404 (Not Found) al visualizzatore che ha richiesto l'oggetto.

Quando CloudFront restituisci una pagina di errore personalizzata a un visualizzatore, paghi i CloudFront costi standard per la pagina di errore personalizzata, non i costi per l'oggetto richiesto. Per ulteriori informazioni sugli CloudFront addebiti, consulta la pagina CloudFrontdei prezzi di Amazon.

Argomenti

- Configurazione del comportamento di risposta agli errori
- Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici
- Archiviazione degli oggetti e delle pagine di errore personalizzate in diverse sedi
- Modificare i codici di risposta restituiti da CloudFront
- Controlla per quanto tempo CloudFront memorizza gli errori nella cache

Configurazione del comportamento di risposta agli errori

Sono disponibili diverse opzioni per gestire la CloudFront risposta in caso di errore. Per configurare risposte di errore personalizzate, puoi utilizzare la CloudFront console, l' CloudFront API o CloudFormation. Indipendentemente dal modo in cui decidi di aggiornare la configurazione, prendi in considerazione i seguenti suggerimenti e consigli:

- Salva le tue pagine di errore personalizzate in una posizione accessibile a CloudFront. Ti consigliamo di memorizzarle in un bucket Amazon S3 e di non conservarle nello stesso percorso del resto del tuo sito Web o del contenuto dell'applicazione. Se memorizzi le pagine di errore personalizzate sulla stessa origine del sito Web o dell'applicazione e l'origine inizia a restituire errori 5xx, non CloudFront puoi ottenere le pagine di errore personalizzate perché il server di origine non è disponibile. Per ulteriori informazioni, consulta Archiviazione degli oggetti e delle pagine di errore personalizzate in diverse sedi.
- Assicurati che CloudFront disponga dell'autorizzazione per ottenere le tue pagine di errore personalizzate. Se le pagine di errore personalizzate sono archiviate in Amazon S3, le pagine devono essere accessibili pubblicamente oppure è necessario configurare un controllo di accesso all' CloudFront origine (OAC). Se le pagine di errore personalizzate sono memorizzate in un'origine personalizzata, le pagine devono essere accessibili pubblicamente.
- (Facoltativo) Se lo desideri, configura l'origine per aggiungere una intestazione `Cache-Control` o `Expires` insieme alle pagine di errore personalizzate. Puoi anche utilizzare l'impostazione Error Caching Minimum TTL per controllare per quanto tempo vengono memorizzate nella CloudFront cache le pagine di errore personalizzate. Per ulteriori informazioni, consulta Controlla per quanto tempo CloudFront memorizza gli errori nella cache.

Configurazione delle risposte di errore personalizzate

Per configurare risposte di errore personalizzate nella CloudFront console, è necessario disporre di una distribuzione. CloudFront Nella console, le impostazioni di configurazione per le risposte personalizzate agli errori sono disponibili solo per le distribuzioni esistenti. Per informazioni su come creare una distribuzione, consulta Inizia con una distribuzione CloudFront standard.

Console

Per configurare le risposte personalizzate agli errori (console)

1. Accedi Console di gestione AWS e apri la pagina Distribuzioni nella CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home#distributions.
2. Nell'elenco delle distribuzioni, scegli la distribuzione da aggiornare.
3. Seleziona la scheda Pagine errori , quindi Crea risposta personalizzata all'errore.
4. Immetti i valori applicabili. Per ulteriori informazioni, consulta Custom Error Pages and Error Caching (Pagine di errore personalizzate e caching errori).
5. Dopo aver immesso i valori desiderati, seleziona Crea.

CloudFront API or CloudFormation

Per configurare risposte di errore personalizzate con l' CloudFront API oppure CloudFormation, usa il `CustomErrorResponse` tipo in una distribuzione. Per ulteriori informazioni, consulta gli argomenti seguenti:

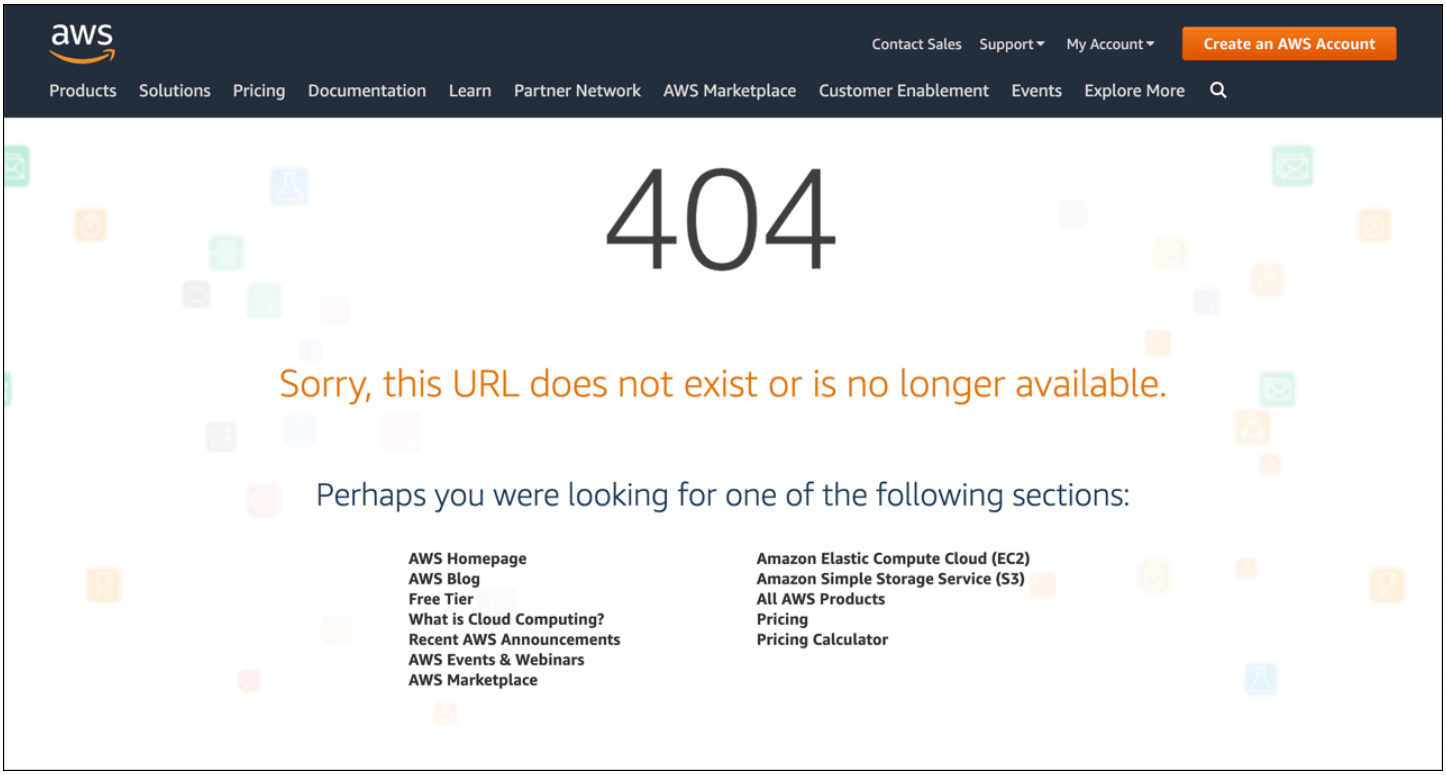
- AWS::CloudFront::Distribution CustomErrorResponse nella Guida per l'utente di AWS CloudFormation
- CustomErrorResponsenell'Amazon CloudFront API Reference

Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici

Se preferisci visualizzare un messaggio di errore personalizzato anziché quello predefinito, ad esempio una pagina che utilizza la stessa formattazione del resto del sito Web, puoi fare in modo che venga CloudFront restituito al visualizzatore un oggetto (come un file HTML) che contiene il tuo messaggio di errore personalizzato.

Per specificare il file che desideri restituire e gli errori per i quali il file deve essere restituito, aggiorni la distribuzione per specificare tali valori. CloudFront Per ulteriori informazioni, consulta Configurazione del comportamento di risposta agli errori.

Di seguito è riportata una pagina di errore personalizzata di esempio:



Puoi specificare un oggetto differente per ciascun codice di stato HTTP supportato, oppure puoi utilizzare lo stesso oggetto per tutti i codici di stato supportati. Puoi decidere di specificare pagine di errore personalizzate per alcuni codici di stato e non per altri.

Gli oggetti tramite i quali stai servendo CloudFront possono non essere disponibili per diversi motivi. Tali opzioni rientrano in due categorie generali:

- Gli errori del client indicano un problema con la richiesta. Ad esempio, l'oggetto con il nome specificato non è disponibile oppure l'utente non possiede le autorizzazioni necessarie per ottenere un oggetto nel bucket Amazon S3. Quando si verifica un errore del client, l'origine restituisce un codice di stato HTTP nell'intervallo 4xx a CloudFront.
- Gli errori del server indicano un problema con il server di origine. Ad esempio, il server HTTP è occupato o non disponibile. Quando si verifica un errore del server, il server di origine restituisce un codice di stato HTTP nell'intervallo 5xx o CloudFront non riceve una risposta dal server di origine per un certo periodo di tempo e presuppone un codice di stato 504 (Gateway Timeout). CloudFront

I codici di stato HTTP per i quali è CloudFront possibile restituire una pagina di errore personalizzata includono i seguenti:

- 400, 403, 404, 405, 414, 416

- 500, 501, 502, 503, 504

> **Note**
>
> - Se CloudFront rileva che la richiesta potrebbe non essere sicura, CloudFront restituisce un errore 400 (Bad Request) anziché una pagina di errore personalizzata.
> - Puoi creare una pagina di errore personalizzata per il codice di stato HTTP 416 (Requested Range Not Satisfiable) e modificare il codice di stato HTTP che CloudFront restituisce agli utenti quando l'origine restituisce un codice di stato 416 a. CloudFront Per ulteriori informazioni, consulta Modificare i codici di risposta restituiti da CloudFront. Tuttavia, CloudFront non memorizza nella cache le risposte del codice di stato 416, quindi anche se specifichi un valore per Error Caching Minimum TTL per il codice di stato 416, non lo utilizza. CloudFront
> - In alcuni casi, CloudFront non restituisce una pagina di errore personalizzata per il codice di stato HTTP 503 anche se si configura in tal senso. CloudFront Se il codice CloudFront di errore è `Capacity Exceeded` o`Limit Exceeded`, CloudFront restituisce un codice di stato 503 al visualizzatore senza utilizzare la pagina di errore personalizzata.
> - Se hai creato una pagina di errore personalizzata, CloudFront restituirà `Connection: close` o `Connection: keep-alive` per i seguenti codici di risposta:
>   - CloudFront restituzioni `Connection: close` per i codici di stato: 400, 405, 414, 416, 500, 501
>   - CloudFront restituisce `Connection: keep-alive` i codici di stato: 403, 404, 502, 503, 504

Per una spiegazione dettagliata di come vengono CloudFront gestite le risposte di errore provenienti dall'origine, consulta. In che modo CloudFront elabora i codici di stato HTTP 4xx e 5xx dalla tua origine

Archiviazione degli oggetti e delle pagine di errore personalizzate in diverse sedi

Se desideri archiviare gli oggetti e le pagine di errore personalizzate in posizioni differenti, la tua distribuzione deve includere un comportamento cache per il quale le seguenti condizioni sono vere:

- Il valore di Path Pattern (Modello di percorso) corrisponde al percorso dei tuoi messaggi di errore personalizzati. Ad esempio, hai salvato pagine di errore personalizzate per errori 4xx in un bucket Amazon S3 in una directory denominata `/4xx-errors`. La tua distribuzione deve includere un comportamento cache per il quale il modello di percorso instrada le richieste per le pagine di errore personalizzate a quella posizione, ad esempi, `/4xx-errors/*`.
- Il valore di Origin (Origine) specifica il valore di Origin ID (ID origine) per l'origine che contiene le tue pagine di errore personalizzate.

Per ulteriori informazioni, consulta Cache Behavior Settings (Impostazioni del comportamento della cache).

Modificare i codici di risposta restituiti da CloudFront

Puoi configurare CloudFront in modo da restituire al visualizzatore un codice di stato HTTP diverso da quello CloudFront ricevuto dall'origine. Ad esempio, se la tua origine restituisce un codice di stato 500 aCloudFront, potresti CloudFront voler restituire una pagina di errore personalizzata e un codice di stato 200 (OK) al visualizzatore. Esistono diversi motivi per cui potresti voler restituire CloudFront al visualizzatore un codice di stato diverso da quello a cui è stato restituito l'origineCloudFront:

- Alcuni dispositivi Internet (ad esempio, alcuni firewall e proxy aziendali) intercettano i codici HTTP 4xx e 5xx e impediscono la restituzione della risposta al visualizzatore. In questo scenario, se si sostituisce `200`, la risposta non viene intercettata.
- Se non ti interessa distinguere tra diversi errori del client o del server, puoi specificare `400` o `500` come valore CloudFront restituito per tutti i codici di stato 4xx o 5xx.
- Potresti scegliere di restituire un codice di stato `200` (OK) e un sito Web statico, in modo che i tuoi clienti non sappiano che il sito Web è inaccessibile.

Se abiliti i log CloudFront standard e configuri CloudFront per modificare il codice di stato HTTP nella risposta, il valore della `sc-status` colonna nei log contiene il codice di stato specificato. Tuttavia, il valore della colonna `x-edge-result-type` non ne è interessato. Contiene il tipo di risultato della risposta dall'origine. Ad esempio, supponete di configurare CloudFront la restituzione di un codice di stato `200` al visualizzatore quando l'origine restituisce `404` (Not Found) a. CloudFront Quando l'origine risponde a una richiesta con un codice di stato `404`, il valore nella colonna `sc-status` nel log sarà `200`, ma il valore nella colonna `x-edge-result-type` sarà `Error`.

È possibile CloudFront configurare la restituzione di uno dei seguenti codici di stato HTTP insieme a una pagina di errore personalizzata:

- 200
- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

Controlla per quanto tempo CloudFront memorizza gli errori nella cache

CloudFront memorizza nella cache le risposte agli errori per una durata predefinita di 10 secondi. CloudFront invia quindi la richiesta successiva per l'oggetto all'origine per verificare se il problema che ha causato l'errore è stato risolto e l'oggetto richiesto è disponibile.

È possibile specificare la durata della memorizzazione nella cache degli errori, ovvero l'Error Caching Minimum TTL, per ogni codice di stato 4xx e 5xx inserito nella cache. CloudFront Per ulteriori informazioni, consulta codici di stato HTTP 4xx e 5xx che vengono memorizzati nella cache CloudFront . Quando specifichi una durata, è importante prestare attenzione alle seguenti informazioni:

- Se specifichi una durata di memorizzazione nella cache degli errori breve, inoltra più richieste all'origine rispetto a quando specifichi una durata più lunga. CloudFront Per gli errori 5xx, questo potrebbe aggravare il problema che ha causato inizialmente l'errore del server di origine.
- Quando l'origine restituisce un errore per un oggetto, CloudFront risponde alle richieste relative all'oggetto con la risposta all'errore o con la pagina di errore personalizzata fino allo scadere del periodo di memorizzazione nella cache degli errori. Se specificate una lunga durata di memorizzazione nella cache degli errori, CloudFront potreste continuare a rispondere alle richieste con una risposta di errore o con la pagina di errore personalizzata per un lungo periodo dopo che l'oggetto sarà nuovamente disponibile.

> **Note**
>
> Puoi creare una pagina di errore personalizzata per il codice di stato HTTP 416 (Impossibile attenersi all'intervallo richiesto) e modificare il codice di stato HTTP che CloudFront restituisce ai visualizzatori quando il server di origine restituisce a CloudFront un codice di stato 416. Per ulteriori informazioni, consulta Modificare i codici di risposta restituiti da CloudFront. Tuttavia, CloudFront non memorizza nella cache le risposte del codice di stato 416, quindi anche se si specifica un valore per Error Caching Minimum TTL per il codice di stato 416, non lo utilizza. CloudFront

Se desideri controllare per quanto tempo CloudFront memorizza nella cache gli errori per i singoli oggetti, puoi configurare il tuo server di origine per aggiungere l'intestazione applicabile alla risposta di errore per quell'oggetto.

Se l'origine aggiunge una **`Cache-Control: s-maxage`** direttiva **`Cache-Control: max-age`** or o un'**`Expires`**intestazione, CloudFront memorizza nella cache le risposte di errore per il valore maggiore tra il valore nell'intestazione o il TTL minimo di Error Caching.

> **Note**
>
> I valori `Cache-Control: max-age` e `Cache-Control: s-maxage` non possono essere maggiori del valore Maximum TTL (TTL massimo) impostato per il comportamento cache per il quale la pagina di errore viene recuperata.

Se l'origine aggiunge una `Cache-Control: private` direttiva `Cache-Control: no-storeCache-Control: no-cache`, o per i codici di errore 404, 410, 414 o 501, CloudFront non memorizza nella cache la risposta all'errore. Per tutti gli altri codici di errore, CloudFront ignora le **`private`** direttive **`no-storeno-cache`**, e e memorizza nella cache la risposta di errore per il valore di Error Caching Minimum TTL.

Se l'origine aggiunge altre **`Cache-Control`** direttive o non aggiunge intestazioni, memorizza nella cache le risposte di errore per il valore di Error CloudFront Caching Minimum TTL.

Se il periodo di scadenza per un codice di stato 4xx o 5xx per un oggetto è più lungo rispetto a quello che desideri attendere, puoi invalidare il codice di errore memorizzato nella cache utilizzando l'URL dell'oggetto richiesto. Se il server di origine restituisce un messaggio di errore per più oggetti, devi invalidare ogni oggetto separatamente. Per ulteriori informazioni sull'invalidamento degli oggetti, consulta Invalidare i file per rimuovere il contenuto.

Se hai abilitato la memorizzazione nella cache per un'origine di bucket S3 e configuri un errore di memorizzazione nella cache di almeno 0 secondi nella tua CloudFront distribuzione, vedrai comunque un errore di memorizzazione nella cache TTL minimo di 1 secondo per gli errori di origine S3. CloudFront lo fa per proteggere la tua origine dagli attacchi S. DDo Non si applica ad altri tipi di origini.

Aggiunta, rimozione o sostituzione di contenuti distribuiti da CloudFront

In questa sezione viene descritto come verificare se CloudFront è in grado di accedere ai contenuti che desideri vengano serviti ai visualizzatori, come specificare gli oggetti nel sito Web o nell'applicazione e come rimuovere o sostituire contenuti.

Argomenti

Aggiunta e accesso ai contenuti distribuiti da CloudFront

Quando desideri configurare CloudFront per distribuire contenuti (oggetti), aggiungi i file a una delle origini specificate per la distribuzione ed esponi un link CloudFront ai file. Una edge location CloudFront non recupera i nuovi file da un'origine finché non riceve le richieste dei visualizzatori per i file. Per ulteriori informazioni, consulta Come CloudFront distribuisce i contenuti.

Quando aggiungi un file che desideri venga distribuito da CloudFront, verifica che venga aggiunto a uno dei bucket Amazon S3 specificato nella tua distribuzione o, per un'origine personalizzata, a una directory nel dominio specificato. Inoltre, conferma che il modello di percorso nel comportamento cache applicabile invii le richieste al server di origine corretto.

Ad esempio, supponiamo che il modello di percorso per un comportamento cache sia `*.html`. Se non disponi di altri comportamenti cache configurati per inoltrare le richieste a tale origine, CloudFront inoltrerà solo i file `*.html`. In questo scenario, ad esempio, CloudFront non distribuirà mai i file .jpg caricati nell'origine, perché non hai creato un comportamento cache che include file .jpg.

I server CloudFront non determinano il tipo MIME per gli oggetti che servono. Quando carichi un file nell'origine, ti consigliamo di impostare il campo di intestazione `Content-Type` relativo.

Utilizzo del controllo delle versioni dei file per aggiornare o rimuovere contenuti con una distribuzione CloudFront

Per aggiornare i contenuti esistenti che vengono distribuiti automaticamente da CloudFront per impostazione predefinita, ti consigliamo di utilizzare un identificatore di versione nei nomi dei file o delle cartelle. Questo consente di controllare la gestione dei contenuti forniti da CloudFront.

Aggiornamento di file esistenti tramite l'utilizzo di nomi file con versione

Quando aggiorni file esistenti in una distribuzione CloudFront, ti consigliamo di includere un identificatore di versione nei nomi dei file o nei nomi delle directory per avere un maggiore controllo sui contenuti. Questo identificatore potrebbe essere un timestamp data, un numero sequenziale o un altro metodo per distinguere due versioni dello stesso oggetto.

Ad esempio, invece di nominare un file grafico image.jpg, potresti chiamarlo image_1.jpg. Quando vuoi iniziare a distribuire una nuova versione del file, puoi chiamare il nuovo file image_2.jpg e aggiornare i link nelle tue applicazioni Web o all'interno del tuo sito per puntare a image_2.jpg. In alternativa, puoi inserire tutte le grafiche in una directory images_v1 e, quando decidi di distribuire una nuova versione di una o più grafiche, puoi creare una nuova directory images_v2 e aggiornare i tuoi link in modo che puntino a quella directory. Grazie alla funzione Versioni multiple, non devi attendere fino alla scadenza di un oggetto per consentire a CloudFront di iniziare a distribuirne una nuova versione e non devi sostenere il costo dell'invalidamento dell'oggetto.

Anche se stabilisci la versione dei file, ti consigliamo comunque di impostare una data di scadenza. Per ulteriori informazioni, consulta Gestione della durata di permanenza dei contenuti nella cache (scadenza).

> **Note**
>
> Specificare i nomi dei file o i nomi delle directory con la versione non è un'operazione legata alla funzione Versioni multiple degli oggetti Amazon S3.

Rimozione dei contenuti in modo che non vengano distribuiti da CloudFront

Puoi rimuovere dall'origine i file che non desideri vengano più inclusi nella distribuzione CloudFront. Tuttavia, CloudFront continuerà a mostrare ai visualizzatori contenuti della cache edge finché i file non scadono.

Se desideri rimuovere un file immediatamente, devi eseguire una delle seguenti operazioni:

- Utilizzare la funzione Versioni multiple. Quando utilizzi la funzione Versioni multiple, versioni diverse di un file hanno nomi diversi che puoi utilizzare nella distribuzione CloudFront per cambiare il file che viene restituito ai visualizzatori. Per ulteriori informazioni, consulta Aggiornamento di file esistenti tramite l'utilizzo di nomi file con versione.
- Invalidare il file. Per ulteriori informazioni, consulta Invalidare i file per rimuovere il contenuto.

Personalizzazione del formato URL per i file in CloudFront

Dopo aver configurato un'origine con gli oggetti (contenuti) che desideri vengano serviti da CloudFront ai visualizzatori, devi utilizzare gli URL corretti per fare riferimento a tali oggetti nel sito Web o codice dell'applicazione in modo che possano essere serviti da CloudFront.

Il nome di dominio utilizzato negli URL per gli oggetti sulle pagine Web o nell'applicazione Web può essere uno dei seguenti:

- Il nome di dominio, ad esempio `d111111abcdef8.cloudfront.net` che CloudFront assegna automaticamente al momento della creazione di una distribuzione
- Il tuo proprio nome di dominio, ad esempio `example.com`

Ad esempio, puoi utilizzare uno dei seguenti URL per restituire il file `image.jpg`:

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

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

Puoi utilizzare lo stesso formato di URL se archivi i contenuti in bucket Amazon S3 o in un server di origine personalizzato, ad esempio uno dei tuoi server Web.

> **Note**
>
> Il formato URL dipende in parte dal valore specificato per Origin Path (Percorso server di origine) nella tua distribuzione. Questo valore fornisce a CloudFront il percorso di directory migliore per i tuoi oggetti. Per ulteriori informazioni su come impostare il percorso di origine al momento della creazione di una distribuzione, vedi Percorso origine.

Per ulteriori informazioni sul formato degli URL, consulta le seguenti sezioni.

Utilizzo del proprio nome di dominio (Example.com)

Invece di utilizzare il nome di dominio predefinito che CloudFront ti assegna al momento della creazione di una distribuzione, puoi aggiungere un nome di dominio alternativo con il quale è più semplice lavorare, ad esempio `example.com`. Per impostare il tuo nome di dominio con CloudFront, puoi usare un URL come questo per gli oggetti presenti nella tua distribuzione:

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

Se prevedi di utilizzare HTTPS tra visualizzatori e CloudFront, consulta Utilizzo di nomi di dominio alternativi e HTTPS.

Utilizzo di una barra finale (/) negli URL

Quando specifichi gli URL per le directory nella tua distribuzione CloudFront, scegli di utilizzare sempre una barra finale o di non utilizzarla mai. Ad esempio, scegli solo uno dei seguenti formati per tutti i tuoi URL:

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

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

Perché è importante?

Entrambi i formati funzionano per collegarsi agli oggetti CloudFront, ma essere coerenti può aiutare a evitare problemi quando, in un secondo momento, desideri invalidare una directory. CloudFront archivia URL esattamente come vengono definiti, incluse le barre finali. Se il formato è incoerente, dovrai quindi invalidare gli URL di directory con e senza la barra, per assicurarti che CloudFront elimini la directory.

È scomodo dover invalidare entrambi i formati di URL e può portare a costi aggiuntivi. Questo perché se devi raddoppiare le invalidazioni per coprire entrambi i tipi di URL, potresti superare il numero massimo di invalidazioni gratuite consentite per il mese. Se questo accade, dovrai pagare tutti gli invalidamenti, anche se in CloudFront esiste solo un formato per ciascun URL delle directory.

Creazione di URL firmati per contenuti con restrizioni

Se disponi di contenuti per i quali desideri limitare l'accesso, puoi creare URL firmati. Ad esempio, se desideri distribuire i contenuti solo per gli utenti che hanno eseguito l'autenticazione, puoi creare URL

validi solo per un periodo di tempo specifico o disponibili solo da un indirizzo IP specifico. Per ulteriori informazioni, consulta Offri contenuti privati con cookie firmati URLs e firmati.

Specifica di un oggetto root predefinito

Puoi configurare CloudFront per restituire un oggetto specifico (l'oggetto root predefinito) quando un utente (visualizzatore) richiede l'URL root per la distribuzione anziché richiedere un oggetto presente nella distribuzione. Puoi utilizzare un oggetto root predefinito per evitare l'esposizione dei contenuti della distribuzione.

Indice

Come specificare un oggetto root predefinito

Per evitare di esporre i contenuti della distribuzione o di ricevere un errore, specifica un oggetto root predefinito per la distribuzione. Puoi specificare il nome esatto del file o il percorso del file. Ad esempio, se l'oggetto root è un file `index.html`, puoi specificare tale nome file. Se il file `index.html` si trova in un'altra cartella, specifica invece il percorso, ad esempio *`exampleFolderName`*`/index.html`. Se si imposta un percorso per l'oggetto root predefinito, le richieste del visualizzatore all'URL root della distribuzione restituiranno il file specificato da tale percorso. Puoi utilizzare un percorso di file per avere maggiore flessibilità nell'organizzazione dei contenuti all'origine, poiché l'oggetto root predefinito può trovarsi in una cartella anziché a livello root.

Per specificare un oggetto root predefinito per la tua distribuzione

1. Carica l'oggetto root predefinito sul server di origine a cui punta la tua distribuzione.

   Il file può essere di qualsiasi tipo supportato da CloudFront. Per un elenco dei vincoli relativi al nome file, consulta l'elemento `DefaultRootObject` in DistributionConfig della Documentazione di riferimento delle API di Amazon CloudFront.

   > **Note**
   >
   > Se il nome del file dell'oggetto root predefinito è troppo lungo o contiene un carattere non valido, CloudFront restituisce l'errore `HTTP 400 Bad Request -`

`InvalidDefaultRootObject`. Inoltre, CloudFront memorizza nella cache il codice per 10 secondi (per impostazione predefinita) e scrive i risultati nei registri di accesso.

2. Conferma che le autorizzazioni per l'oggetto concedono a CloudFront almeno l'accesso in lettura.

   Per ulteriori informazioni sulle autorizzazioni di Amazon S3, consulta Identity and Access Management in Amazon S3 nella Guida per gli sviluppatori di Amazon Simple Storage Service.

3. Aggiorna la distribuzione in modo che faccia riferimento all'oggetto root predefinito utilizzando la console CloudFront o l'API CloudFront.

   Come specificare un oggetto root predefinito utilizzando la console CloudFront:

   a. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
   b. Nell'elenco delle distribuzioni nel riquadro superiore, seleziona la distribuzione da aggiornare.
   c. Nel riquadro Settings (Impostazioni), sulla scheda General (Generale), scegliere Edit (Modifica).
   d. Nella finestra di dialogo Modifica impostazioni, nel campo Oggetto root predefinito, inserisci il nome file o il percorso dell'oggetto root predefinito.

      > **Tip**
      >
      > La stringa non può iniziare con una barra obliqua (`/`). Specifica solo il nome dell'oggetto o il percorso dell'oggetto. Ad esempio, utilizza `index.html` o *`exampleFolderName`*`/index.html`. La specifica di un **`/`***`exampleFolderName`*`/index.html` o **`/`**`index.html` può generare un errore 403 Access Denied.

   e. Scegli Save changes (Salva modifiche).

   Per aggiornare la configurazione utilizzando l'API CloudFront, specifica un valore per l'elemento `DefaultRootObject` nella distribuzione. Per informazioni sull'utilizzo dell'API CloudFront per specificare un oggetto radice predefinito, vedere UpdateDistribution nella Guida di riferimento API Amazon CloudFront.

4. Conferma di aver abilitato l'oggetto root predefinito richiedendo l'URL root. Se il tuo browser non visualizza l'oggetto root predefinito, esegui i seguenti passaggi:

a. Conferma che la tua distribuzione è completamente distribuita visualizzando lo stato della tua distribuzione nella console CloudFront.
b. Ripeti le fasi 2 e 3 per verificare di aver ricevuto le autorizzazioni corrette e aver aggiornato la configurazione della distribuzione come richiesto per specificare l'oggetto root predefinito.

Come funziona un oggetto root predefinito

Supponiamo che la seguente richiesta faccia riferimento all'oggetto `image.jpg`:

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

Al contrario, la seguente richiesta fa riferimento all'URL root della stessa distribuzione anziché a un oggetto specifico, come nel primo esempio:

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

Quando definisci un oggetto root predefinito, la richiesta di un utente finale che chiama il root della distribuzione restituisce l'oggetto root predefinito. Ad esempio, se imposti il file `index.html` come oggetto root predefinito, una richiesta per:

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

Valori restituiti:

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

> **Note**
>
> CloudFront non determina se un URL con più barre finali (`https://d111111abcdef8.cloudfront.net///`) è equivalente a `https://d111111abcdef8.cloudfront.net/`. Il server di origine effettua questo confronto.

Se definisci un oggetto root predefinito, la richiesta di un utente finale per una sottodirectory della distribuzione non restituisce l'oggetto root predefinito. Ad esempio, supponiamo che `index.html` sia il tuo oggetto root predefinito e che CloudFront riceva una richiesta dell'utente finale per la directory `install` nella tua distribuzione CloudFront:

`https://d111111abcdef8.cloudfront.net/install/`

CloudFront non restituisce l'oggetto root predefinito anche se una copia di `index.html` viene visualizzata nella directory `install`. Tuttavia, se hai specificato un percorso per l'oggetto root predefinito, (`install/index.html`) CloudFront restituirà l'oggetto root predefinito per le richieste dell'utente finale per la directory `install`

Se configuri la tua distribuzione per consentire tutti i metodi HTTP che CloudFront supporta, l'oggetto root predefinito si applica a tutti i metodi. Ad esempio, se l'oggetto root predefinito è index.php e scrivi la tua applicazione per inviare una richiesta `POST` alla root del tuo dominio (https://example.com), CloudFront invierà la richiesta a https://example.com/index.php.

Il comportamento degli oggetti root predefiniti di CloudFront è diverso da quello dei documenti di indice di Amazon S3. Quando configuri un bucket Amazon S3 come sito Web e specifichi il documento di indice, Amazon S3 restituisce il documento di indice anche se un utente richiede una sottodirectory nel bucket. (Una copia del documento di indice deve essere inclusa in ogni sottodirectory). Per ulteriori informazioni sulla configurazione dei bucket Amazon S3 come siti Web e sui documenti indicizzati, consulta il capitolo Hosting Siti Web su Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

> **Important**
>
> Ricorda che un oggetto root predefinito si applica solo alla tua distribuzione CloudFront. È comunque necessario gestire la sicurezza per il tuo server di origine. Ad esempio, se stai utilizzando un server di origine Amazon S3, devi comunque impostare le autorizzazioni ACL per il bucket Amazon S3; in modo appropriato per garantire il livello di accesso che desideri avere per il tuo bucket.

Come funziona CloudFront se non si definisce un oggetto root

Se non definisci un oggetto root predefinito, le richieste per il percorso root della distribuzione passa al tuo server di origine. Se stai usando un server di origine Amazon S3, potresti ricevere una delle seguenti risposte:

- Un elenco dei contenuti del tuo bucket Amazon S3 - In una delle condizioni seguenti, i contenuti del tuo server di origine sono visibili da chiunque utilizzi CloudFront per accedere alla tua distribuzione:
  - Il tuo bucket non è configurato correttamente.
  - Le autorizzazioni Amazon S3 per il bucket associato alla distribuzione e per gli oggetti nel bucket concedono l'accesso a tutti gli utenti.

  - Un utente finale accede al server di origine utilizzando l'URL root di origine.
- Un elenco dei contenuti privati del tuo server di origine - Se configuri il server di origine come distribuzione privata (solo tu e &CF; avete accesso), i contenuti del bucket Amazon S3 associati alla tua distribuzione sono visibili a chiunque abbia le credenziali per accedere alla tua distribuzione tramite CloudFront. In questo caso, gli utenti non sono in grado di accedere ai tuoi contenuti tramite l'URL root di origine. Per ulteriori informazioni su come distribuire contenuti privati, consulta the section called “Limita i contenuti con cookie firmati URLs e firmati”.
- `Error 403 Forbidden` - CloudFront restituisce questo errore se le autorizzazioni nel bucket Amazon S3 associato alla distribuzione o le autorizzazioni per gli oggetti nel bucket negano l'accesso a CloudFront e a tutti gli utenti.

Invalidare i file per rimuovere il contenuto

Se devi rimuovere un file dalle edge cache CloudFront prima che scada, puoi eseguire una delle operazioni seguenti:

- Invalida il file dalle edge cache. La volta successiva che un visualizzatore richiede il file, CloudFront ritorna all'origine per recuperare la versione più recente del file.
- Utilizza la funzione Versioni multiple dei file per distribuire un'altra versione del file con un nome diverso. Per ulteriori informazioni, consulta Aggiornamento di file esistenti tramite l’utilizzo di nomi file con versione.

Argomenti

Scelta tra invalidare i file e utilizzare nomi di file con versione

Per controllare le versioni di file che vengono servite dalla distribuzione, puoi invalidare i file o fornire loro nomi di file con versione. Se vuoi aggiornare i file di frequente, ti consigliamo di usare principalmente la funzione Versioni multiple di file per i seguenti motivi:

- La funzione Versioni multiple consente di controllare quale file viene restituito da una richiesta anche quando l'utente dispone di una versione memorizzata nella cache in locale o in un proxy di memorizzazione nella cache aziendale. Se invalidi il file, l'utente potrebbe continuare a vedere la versione precedente fino alla scadenza delle cache.
- I log di accesso di CloudFront includono i nomi dei file, per cui la funzione Versioni multiple rappresenta un modo semplice per analizzare i risultati delle modifiche di file.
- La funzione Versioni multiple offre un modo per servire diverse versioni dei file a utenti diversi.
- La funzione Versioni multiple semplifica il roll back e il forward tra le revisioni del file.
- La funzione Versioni multiple è meno costosa. Devi comunque pagare per il trasferimento eseguito da CloudFront di nuove versioni dei file alle edge location, ma non sono previsti costi per l'invalidamento dei file.

Per ulteriori informazioni sulla funzione Versioni multiple dei file, consulta Aggiornamento di file esistenti tramite l'utilizzo di nomi file con versione.

Determinazione dei file da invalidare

Se desideri invalidare più file, ad esempio tutti i file in una directory o tutti i file che iniziano con gli stessi caratteri, puoi includere il carattere jolly `*` alla fine del percorso di invalidamento. Per ulteriori informazioni sull'utilizzo del carattere `*`, vedi Invalidation paths.

Per invalidare i file, puoi specificare il percorso per singoli file o il percorso che termina con il carattere jolly `*`, che potrebbe essere applicato a un solo file o a molti, come illustrato negli esempi seguenti:

- `/images/image1.jpg`
- `/images/image*`
- `/images/*`

Se desideri invalidare i file selezionati, ma i tuoi utenti non accedono necessariamente a ogni file nella tua origine, puoi stabilire quali file i visualizzatori hanno richiesto a CloudFront e invalidare

solo quelli. Per determinare quali file i visualizzatori hanno richiesto, attiva il log degli accessi di CloudFront. Per ulteriori informazioni sui log degli accessi al, consultare Registri di accesso (registri standard).

Cosa occorre sapere quando si invalidano i file

Quando si specifica un file da invalidare, fai riferimento alle seguenti informazioni:

Distinzione tra lettere maiuscole e minuscole

I percorsi di invalidazione rispettano la distinzione tra lettere maiuscole. Ad esempio, `/images/image.jpg` e `/images/Image.jpg` specificano due file diversi.

Modifica dell'URI utilizzando una funzione Lambda

Se la distribuzione CloudFront attiva una funzione Lambda su eventi di richiesta di visualizzatori e se la funzione modifica l'URI del file richiesto, ti consigliamo di invalidare entrambi gli URI per eliminare il file dalle edge cache CloudFront:

- L'URI nella richiesta del visualizzatore
- L'URI dopo la modifica eseguita dalla funzione

Example Esempio

Si supponga che la funzione Lambda modifichi l'URI per un file da:

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

A un URI che include una directory di linguaggio:

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

Per invalidare il file, devi specificare i seguenti percorsi:

- `/index.html`
- `/en/index.html`

Per ulteriori informazioni, consulta Invalidation paths.

Oggetti root predefiniti

Per invalidare l'oggetto root predefinito (file), specifica il percorso nello stesso modo in cui specifichi il percorso per qualsiasi altro file. Per ulteriori informazioni, consulta Come funziona un oggetto root predefinito.

Inoltro dei cookie

Se CloudFront è stato configurato per inoltrare i cookie all'origine, le cache edge di CloudFront potrebbero contenere diverse versioni del file. Quando invalidi un file, CloudFront invalida ogni versione memorizzata nella cache del file stesso, indipendentemente dai cookie associati. Non puoi selettivamente invalidare alcune versioni e non altre sulla base del cookie associati. Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.

Inoltro di intestazioni

Se hai configurato CloudFront per inoltrare un elenco di intestazioni all'origine e per memorizzare nella cache in base ai valori delle intestazioni, le cache edge di CloudFront potrebbero contenere diverse versioni del file. Quando invalidi un file, CloudFront invalida ogni versione memorizzata nella cache del file stesso, a prescindere dai valori delle intestazioni. Non puoi selettivamente invalidare alcune versioni e non altre sulla base dei valori delle intestazioni. (Se configuri CloudFront per inoltrare tutte le intestazioni alla tua origine, CloudFront non memorizza nella cache i file). Per ulteriori informazioni, consulta Caching dei contenuti in base alle intestazioni di richiesta.

Inoltro di stringhe di query

Se CloudFront è stato configurato per inoltrare le stringhe di query all'origine, includere le stringhe di query durante l'invalidamento dei file, come illustrato negli esempi seguenti:

- `/images/image.jpg?parameter1=a`
- `/images/image.jpg?parameter1=b`

Se le richieste del client includono cinque diverse stringhe di query per lo stesso file, puoi invalidare il file cinque volte, una per ogni stringa di query, oppure utilizzare il carattere jolly * nel percorso di invalidamento, come nell'esempio seguente:

```
/images/image.jpg*
```

Per ulteriori informazioni sull'utilizzo di caratteri jolly nel percorso di invalidamento, consulta Invalidation paths.

Per ulteriori informazioni sulle stringhe di query, vedi Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

Per determinare quale stringhe di query sono in uso, puoi abilitare la registrazione di log di CloudFront. Per ulteriori informazioni, consulta Registri di accesso (registri standard).

Massimo consentito

Per ulteriori informazioni sul numero massimo di invalidazioni consentite, consulta Massima richiesta di invalidamento concorrente.

File Microsoft Smooth Streaming

Non puoi invalidare i file multimediali nel formato Microsoft Smooth Streaming quando hai abilitato Smooth Streaming per il comportamento cache corrispondente.

Caratteri non ASCII o non sicuri nel percorso

Se il percorso include caratteri non ASCII o caratteri non sicuri come indicato in RFC 1738, è necessario codificare tali caratteri in formato URL. Non codificare nell'URL qualsiasi altro carattere presente nel percorso. In caso contrario, CloudFront non invaliderà la versione precedente del file aggiornato.

> **Important**
>
> Non utilizzare il carattere ~ nel percorso. CloudFront non supporta questo carattere per le invalidazioni, a prescindere che sia codificato o meno nell'URL.

Percorsi di invalidamento

Questo percorso è relativo alla distribuzione. Ad esempio, per invalidare il file in `https://d111111abcdef8.cloudfront.net/images/image2.jpg`, devi specificare `/images/image2.jpg`.

> **Note**
>
> Nella console CloudFront, puoi omettere la barra iniziale nel percorso, in questo modo: `images/image2.jpg`. Quando si utilizza direttamente l'API CloudFront, i percorsi di invalidamento devono iniziare con una barra iniziale.

Puoi anche invalidare più file contemporaneamente utilizzando il carattere jolly `*`. Il carattere `*`, che sostituisce 0 o più caratteri, deve essere l'ultimo carattere nel percorso di invalidamento.

> **Important**
>
> Per utilizzare i caratteri jolly (*) nell'invalidazione, è necessario inserire il carattere jolly alla fine del percorso. Gli asterischi (*) inseriti altrove vengono considerati come una corrispondenza letterale di caratteri anziché un carattere jolly di invalidazione.

Se utilizzi AWS Command Line Interface (AWS CLI) per invalidare i file e specifichi un percorso che include il carattere jolly *, devi usare le virgolette (") in tutto il percorso come `"/*"`.

La lunghezza massima di un percorso è 4.000 caratteri.

Example Esempio: percorsi di invalidazione

- Come invalidare tutti i file in una directory:

  */directory-path/**

- Per invalidare una directory, tutte le sottodirectory e tutti i file nella directory e nella sottodirectory:

  */directory-path**

- Per invalidare tutti i file con lo stesso nome, ma estensioni di nome di file diverse, ad esempio logo.jpg, logo.png e logo.gif:

  */directory-path/file-name.**

- Per invalidare tutti i file in una directory per i quali il nome file inizia con gli stessi caratteri (ad esempio tutti i file per un video in formato HLS), indipendentemente dall'estensione del nome file:

  */directory-path/initial-characters-in-file-name**

- Quando configuri CloudFront per memorizzare nella cache in base ai parametri della stringa di query e desideri invalidare ogni versione di un file:

  */directory-path/file-name.file-name-extension**

- Come invalidare tutti i file in una distribuzione:

  /*

Per ulteriori informazioni su come invalidare i file utilizzando una funzione Lambda per modificare l'URI, consulta Changing the URI Using a Lambda Function.

Se il percorso di invalidamento è una directory e se non hai standardizzato un metodo per specificare le directory - con o senza una barra finale (/), ti consigliamo di invalidare la directory con e senza barre finali, ad esempio, `/images` e `/images/`.

URL firmati

Se stai usando URL firmati, invalida un file includendo solo la parte di URL prima del punto interrogativo (?).

Invalidare i file

Puoi utilizzare la console CloudFront per creare ed eseguire un invalidamento, visualizzare un elenco di invalidamenti inviati in precedenza e visualizzare informazioni dettagliate su un singolo invalidamento. Puoi anche copiare un invalidamento esistente, modificare l'elenco dei percorsi dei file ed eseguire l'invalidamento modificato. Non è possibile rimuovere gli invalidamenti dall'elenco.

Indice

Invalidare i file

Per invalidare i file tramite la console CloudFront, esegui la procedura seguente.

Console

Come invalidare i file (console)

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli la distribuzione per la quale desideri invalidare i file.
3. Seleziona la scheda Invalidations (Invalidamenti).
4. Scegli Crea invalidazione.

5. Per i file da invalidare, immetti un percorso di invalidamento per riga. Per informazioni su come specificare i percorsi di invalidamento, consulta Cosa occorre sapere quando si invalidano i file.

   > **Important**
   >
   > Specifica i percorsi dei file attentamente. Non puoi annullare una richiesta di invalidamento dopo l'avvio.

6. Scegli Crea invalidazione.

CloudFront API

Per informazioni sull'invalidazione degli oggetti e sulla visualizzazione delle informazioni sull'invalidazione, consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon CloudFront:

- CreateInvalidation
- ListInvalidations
- GetInvalidation

> **Note**
>
> Se utilizzi AWS Command Line Interface (AWS CLI) per invalidare i file e specifichi un percorso che include il carattere jolly *, devi usare le virgolette (") in tutto il percorso, come nell'esempio seguente:
>
> ```
> aws cloudfront create-invalidation --distribution-id distribution_ID --paths
>  "/*"
> ```

Copiare, modificare e rieseguire un'invalidazione esistente

Puoi copiare un invalidamento creato precedentemente, aggiornare l'elenco dei percorsi di invalidamento ed eseguire l'invalidamento aggiornato. Non puoi copiare un'invalidazione esistente, aggiornare i percorsi di invalidazione e salvare l'invalidazione aggiornata senza eseguirla.

> **Important**
>
> Se copi un'invalidazione ancora in corso, aggiorna l'elenco dei percorsi di invalidazione ed esegui l'invalidazione aggiornata, CloudFront non arresterà o eliminerà l'invalidazione copiata. Se un percorso di invalidamento appare in originale e in copia, CloudFront cercherà di invalidare i file due volte ed entrambi gli invalidamenti saranno conteggiati ai fini del calcolo del numero massimo di invalidamenti mensili gratuiti. Se hai già raggiunto il numero massimo di invalidazioni gratuite, ti verrà addebitato il costo per entrambe le invalidazioni di ogni file. Per ulteriori informazioni, consulta Massima richiesta di invalidamento concorrente.

Per copiare, modificare e rieseguire un invalidamento esistente

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona la distribuzione che contiene l'invalidamento da copiare.
3. Seleziona la scheda Invalidations (Invalidamenti).
4. Scegli l'invalidamento da copiare.

   Se non sei sicuro di quale invalidazione copiare, puoi scegliere un'invalidazione e selezionare Dettagli per visualizzare le informazioni dettagliate relative.
5. Scegli Copia in nuovo.
6. Aggiorna l'elenco dei percorsi di invalidamento, ove applicabile.
7. Scegli Crea invalidazione.

Annullamento delle invalidazioni

Quando invii una richiesta di invalidamento a CloudFront, CloudFront inoltra la richiesta per tutte le edge location entro pochi secondi e ogni edge location avvia immediatamente l'elaborazione dell'invalidamento. Di conseguenza, non puoi annullare una richiesta di invalidamento dopo averla inviata.

Elencare le invalidazioni

Puoi visualizzare l'elenco degli ultimi 100 invalidamenti creati ed eseguiti per una distribuzione utilizzando la console CloudFront. Se desideri ottenere un elenco di più di 100 invalidazioni, utilizza

l'operazione API `ListInvalidations`. Per ulteriori informazioni, consulta ListInValidations nella Guida di riferimento API Amazon CloudFront.

Per elencare gli invalidamenti

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona la distribuzione per la quale desideri visualizzare un elenco degli invalidamenti.
3. Seleziona la scheda Invalidations (Invalidamenti).

> **Note**
>
> Non è possibile rimuovere gli invalidamenti dall'elenco.

Visualizzazione delle informazioni relative a un'invalidazione

Puoi visualizzare informazioni dettagliate su un invalidamento, tra cui l'ID distribuzione, l'ID invalidamento, lo stato di invalidamento, la data e l'ora in cui l'invalidamento è stato creato e un elenco completo dei percorsi di invalidamento.

Per visualizzare informazioni su un invalidamento

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona la distribuzione che contiene l'invalidamento di cui vuoi visualizzare informazioni dettagliate.
3. Seleziona la scheda Invalidations (Invalidamenti).
4. Scegli l'ID di invalidazione applicabile o seleziona l'ID di invalidazione, quindi scegli Visualizza dettagli.

Massima richiesta di invalidamento concorrente

Se stai invalidando i file singolarmente, puoi avere richieste di invalidamento per un massimo di 3000 file per distribuzione in corso alla volta. Questa può essere una richiesta di invalidamento per massimo 3000 file, fino a 3000 richieste per un file ciascuna, o qualsiasi altra combinazione che non superi i 3000 file. Ad esempio, puoi inviare 30 richieste di invalidamento che invalidano 100

file ognuna. Finché tutte e 30 le richieste di invalidamento sono ancora in corso, non puoi inviare eventuali ulteriori richieste di invalidamento. Se si supera il valore massimo, CloudFront restituisce un messaggio di errore.

Se stai utilizzando il carattere jolly *, puoi avere richieste per massimo 15 percorsi di invalidamento in corso alla volta. Puoi anche avere richieste di invalidamento per massimo 3.000 file singoli per distribuzione in corso alla volta; il numero massimo di richieste di invalidamento consentite con carattere jolly è indipendente dal numero massimo di invalidamento singolo dei file.

Pagamento per l'invalidazione dei file

I primi 1.000 percorsi di invalidamento che invii al mese sono gratuiti; pagherai ogni percorso di invalidamento oltre i 1.000 in un mese. Un percorso di invalidamento può essere per un singolo file (ad esempio `/images/logo.jpg`) o per più file (ad esempio `/images/*`). Un percorso che include il carattere jolly `*` conta come un percorso anche se comporta l'invalidamento di migliaia di file da parte di CloudFront.

Il valore massimo di 1000 percorsi di invalidazione gratuiti al mese è valido per il numero totale di percorsi di invalidazione per tutte le distribuzioni create con un Account AWS. Ad esempio, se utilizzi l'Account AWS `john@example.com` per creare tre distribuzioni e invii 600 percorsi di invalidazione per ciascuna distribuzione in un determinato mese (per un totale di 1.800 percorsi di invalidazione), AWS addebiterà la differenza tra il totale dei percorsi di invalidazione e il limite gratuito di 1.000. In questo esempio, AWS addebita 800 percorsi di invalidazione in tale mese.

Il costo per inviare un percorso di invalidamento è lo stesso a prescindere dal numero di file che si stanno invalidando: un singolo file (`/images/logo.jpg`) o tutti i file associati a una distribuzione (`/*`). Poiché nella richiesta di invalidazione viene addebitato un costo per ogni percorso, anche se si raggruppano più percorsi in un'unica richiesta, ai fini della fatturazione ogni percorso viene comunque conteggiato singolarmente.

Per ulteriori informazioni sui prezzi di annullamento dell'invalidazione, consulta la pagina Prezzi di Amazon CloudFront. Per ulteriori informazioni sui percorsi di invalidamento, consulta Invalidation paths.

Distribuzione di file compressi

Quando gli oggetti richiesti sono compressi, i download possono essere più rapidi in quanto gli oggetti sono più piccoli; in alcuni casi, meno di un quarto della dimensione originale. Download più veloci

possono comportare un rendering più rapido delle pagine web per i visitatori, in particolare per i file JavaScript e CSS. Inoltre, il costo del trasferimento dati CloudFront si basa sulla quantità totale di dati forniti. La distribuzione di oggetti compressi può essere meno costosa rispetto alla distribuzione di oggetti non compressi.

Argomenti

Configurazione di CloudFront per comprimere oggetti

Per configurare CloudFront in modo da comprimere gli oggetti, aggiorna il comportamento cache che desideri utilizzare per servire gli oggetti compressi.

Come configurare CloudFront per comprimere oggetti (console)

1. Accedi alla Console CloudFront.
2. Scegli la distribuzione, quindi seleziona il comportamento da modificare.
3. Per l'impostazione Comprimi oggetti automaticamente, scegli Sì.
4. Usa una policy della cache per specificare le impostazioni di caching e abilita entrambi i formati di compressione Gzip e Brotli.

> **Note**
>
> - Per utilizzare la compressione Brotli sono richieste policy della cache. Brotli non supporta le impostazioni cache legacy.
> - Per abilitare la compressione utilizzando CloudFormation o l'API CloudFront, imposta i parametri `Compress`, `EnableAcceptEncodingGzip`, `EnableAcceptEncodingBrotli` su `true`.

Per comprendere come CloudFront comprime gli oggetti, consulta la sezione seguente.

Come funziona la compressione CloudFront

1. Un visualizzatore richiede un oggetto. Il visualizzatore include l'intestazione `Accept-Encoding` HTTP nella richiesta e il valore di intestazione include `gzip`, `br` o entrambi. Questo indica che il visualizzatore supporta gli oggetti compressi. Quando il visualizzatore supporta entrambi i formati Gzip e Brotli, CloudFront utilizza Brotli.

   > **Note**
   >
   > I browser web Chrome e Firefox supportano la compressione Brotli solo quando la richiesta viene inviata utilizzando HTTPS. Non supportano Brotli con richieste HTTP.

2. Nella posizione edge, CloudFront controlla la cache per una copia compressa dell'oggetto richiesto.
3. A seconda che l'oggetto compresso sia presente o meno nella cache, CloudFront esegue una delle seguenti operazioni:
   - Se l'oggetto compresso è già nella cache, CloudFront lo invia al visualizzatore e ignora le fasi rimanenti.
   - Se l'oggetto compresso non si trova nella cache, CloudFront inoltra la richiesta all'origine.

   > **Note**
   >
   > Se una copia non compressa dell'oggetto è già nella cache, CloudFront potrebbe inviarla al visualizzatore senza inoltrare la richiesta all'origine. Ad esempio, ciò può verificarsi quando CloudFront ha precedentemente saltato la compressione. In questo caso, CloudFront memorizza nella cache l'oggetto non compresso e continua a servirlo fino a quando l'oggetto scade, viene espulso o viene invalidato.

4. Se l'origine restituisce un oggetto compresso, come indicato dalla presenza di un'intestazione `Content-Encoding` nella risposta HTTP, CloudFront invia l'oggetto compresso al visualizzatore, lo aggiunge alla cache e ignora le fasi rimanenti. CloudFront non comprime di nuovo l'oggetto.
5. Se l'origine restituisce a CloudFront un oggetto non compresso senza intestazione `Content-Encoding` nella risposta HTTP, CloudFront determina se l'oggetto può essere compresso. Per ulteriori informazioni, consulta Condizioni per la compressione.

6. Se l'oggetto può essere compresso, CloudFront lo comprime, lo invia al visualizzatore e quindi lo aggiunge alla cache.
7. Se ci sono richieste visualizzatore successive per lo stesso oggetto, CloudFront restituisce la prima versione memorizzata nella cache. Ad esempio, se un visualizzatore richiede un oggetto specifico memorizzato nella cache che utilizza la compressione Gzip e accetta il formato Gzip, le richieste successive allo stesso oggetto restituiranno sempre la versione Gzip, anche se il visualizzatore accetta sia Brotli che Gzip.

Alcune origini personalizzate possono anche comprimere gli oggetti. L'origine potrebbe essere in grado di comprimere oggetti non compressi da CloudFront. Per ulteriori informazioni, consulta Tipi di file che CloudFront comprime.

Condizioni per la compressione

Nell'elenco seguente vengono fornite ulteriori informazioni sugli scenari in cui CloudFront comprime gli oggetti.

La richiesta utilizza HTTP 1.0

Se una richiesta a CloudFront utilizza HTTP 1.0, CloudFront rimuove l'intestazione `Accept-Encoding` e non comprime l'oggetto nella risposta.

`Accept-Encoding`Intestazione della richiesta

Se l'intestazione `Accept-Encoding` non è presente nella richiesta del visualizzatore o se non contiene `gzip` o `br` come valore, CloudFront non comprime l'oggetto nella risposta. Se l'intestazione `Accept-Encoding` include ulteriori valori, ad esempio `deflate`, CloudFront li rimuove prima di inoltrare la richiesta al server di origine.

Quando CloudFront è configurato per comprimere oggetti, include automaticamente l'intestazione `Accept-Encoding` nella chiave cache e nelle richieste di origine.

Il contenuto è già memorizzato nella cache quando si configura CloudFront per comprimere oggetti

CloudFront comprime gli oggetti quando li ottiene dall'origine. Quando configuri CloudFront per comprimere gli oggetti, gli oggetti già memorizzati nella cache della posizione edge non vengono compressi da CloudFront. Inoltre, quando un oggetto memorizzato nella cache scade in una posizione edge e CloudFront inoltra un'altra richiesta per l'oggetto all'origine, CloudFront non comprime l'oggetto quando l'origine restituisce un codice di stato HTTP 304. Ciò significa che

la posizione edge dispone già della versione più recente dell'oggetto. Se vuoi che CloudFront comprima gli oggetti già memorizzati nella cache delle posizioni edge, devi invalidare quegli oggetti. Per ulteriori informazioni, consulta Invalidare i file per rimuovere il contenuto.

L'origine è già configurata per comprimere gli oggetti

Se si configura CloudFront per comprimere gli oggetti e l'origine comprime anche gli oggetti, l'origine dovrebbe includere una intestazione `Content-Encoding`. Questa intestazione indica a CloudFront che l'oggetto è già compresso. Quando una risposta da un'origine include l'intestazione `Content-Encoding`, CloudFront non comprime l'oggetto, a prescindere dal valore dell'intestazione. CloudFront invia la risposta al visualizzatore e memorizza l'oggetto nella cache della posizione edge.

Tipi di file che CloudFront comprime

Per un elenco completo, consulta Tipi di file che CloudFront comprime.

Dimensione degli oggetti che CloudFront comprime

CloudFront comprime oggetti la cui dimensione è tra 1.000 byte e 10 milioni di byte.

`Content-Length`Intestazione

L'origine deve includere un'intestazione `Content-Length` nella risposta di modo che CloudFront sia in grado di determinare se la dimensione dell'oggetto rientra nell'intervallo che CloudFront può comprimere. Se l'intestazione `Content-Length` è mancante oppure contiene un valore non valido o al di fuori dell'intervallo di dimensioni che CloudFront può comprimere, CloudFront non comprime l'oggetto. Per ulteriori informazioni su come CloudFront elabora oggetti di grandi dimensioni che possono superare l'intervallo di dimensioni, consulta Come CloudFront elabora le richieste parziali per un oggetto (intervalloGETs).

Il codice di stato HTTP per la risposta

CloudFront comprime gli oggetti solo quando il codice di stato HTTP della risposta è `200`, `403` o `404`.

La risposta non ha corpo

Quando la risposta HTTP dall'origine non ha corpo, non c'è nulla da comprimere per CloudFront.

`ETag`Intestazione

CloudFront a volte modifica l'intestazione `ETag` nella risposta HTTP quando comprime gli oggetti. Per ulteriori informazioni, consulta the section called "`ETag`Conversione dell'intestazione ".

CloudFront salta la compressione

CloudFront comprime gli oggetti in base al miglior tentativo. In rari casi, CloudFront non esegue la compressione di un oggetto quando registra un carico di traffico elevato. CloudFront prende questa decisione sulla base di una varietà di fattori, tra cui la capacità host. Se CloudFront salta la compressione di un oggetto, memorizza l'oggetto non compresso nella cache e continua a servirlo fino a quando l'oggetto scade, viene espulso o viene invalidato.

Tipi di file che CloudFront comprime

Se configuri CloudFront per comprimere gli oggetti, CloudFront comprime solo gli oggetti che hanno i seguenti valori nell'intestazione della risposta `Content-Type`:

- `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

ETagConversione dell'intestazione

Quando l'oggetto non compresso dall'origine include un'intestazione `ETag` HTTP valida e consolidata, e CloudFront comprime l'oggetto, CloudFront converte anche il valore dell'intestazione `ETag` consolidata in un `ETag` debole e restituisce il valore `ETag` debole al visualizzatore. Gli spettatori possono memorizzare il valore `ETag` debole e utilizzarlo per inviare richieste condizionali con l'intestazione `If-None-Match` HTTP. Ciò consente ai visualizzatori, CloudFront, e all'origine di trattare le versioni compresse e non compresse di un oggetto come semanticamente equivalenti, riducendo così il trasferimento di dati non necessari.

Un valore di intestazione `ETag` valido e consolidato inizia e termina con un carattere di virgoletta doppia (`"`). Per convertire il valore `ETag` forte in uno debole, CloudFront aggiunge i caratteri `W/` all'inizio del valore forte `ETag`.

Quando l'oggetto dall'origine include un valore di intestazione debole `ETag` (un valore che inizia con i caratteri `W/`), CloudFront non modifica questo valore e lo restituisce al visualizzatore come ricevuto dall'origine.

Quando l'oggetto dall'origine include un valore di intestazione `ETag` non valido (il valore non inizia con `"` o con `W/`), CloudFront rimuove l'intestazione `ETag` e restituisce l'oggetto al visualizzatore senza l'intestazione di risposta `ETag`.

Per ulteriori informazioni, consulta le pagine seguenti nei documenti web MDN:

- Direttive (intestazione`ETag` HTTP)
- Convalida debole (richieste condizionali HTTP)
- If-None-Match Intestazione HTTP

Utilizzo di protezioni AWS WAF

È possibile usare AWS WAF per proteggere le proprie distribuzioni CloudFront e i server di origine. AWS WAF è un firewall per applicazioni Web che consente di proteggere le applicazioni Web e le API per bloccare le richieste prima che raggiungano i server. Per ulteriori informazioni, consulta Accelerate and protect your websites using CloudFront and AWS WAF e Linee guida per l'implementazione di AWS WAF.

Per abilitare le protezioni AWS WAF, puoi:

- Utilizzare la protezione con un solo clic nella console CloudFront. La protezione con un clic crea una lista di controllo degli accessi Web (Web ACL) AWS WAF, configura regole per proteggere i server dalle minacce Web comuni e collega l'ACL Web alla distribuzione CloudFront per l'utente. Gli argomenti di questa sezione presuppongono l'uso di protezioni con un solo clic.
- Utilizza un ACL Web preconfigurato (elenco di controllo degli accessi) creato nella console AWS WAF o utilizzando le API AWS WAF. Per ulteriori informazioni, consulta le liste di controllo degli accessi Web (ACL) nella Guida per sviluppatori di AWS WAF e AssociateWebACL nella Guida di riferimento alle API AWS WAF

Puoi abilitare AWS WAF quando:

- Creazione di una distribuzione
- Utilizzi la dashboard di Sicurezza per modificare le impostazioni di sicurezza di una distribuzione esistente

Quando utilizzi la protezione con un clic, CloudFront applica un set di protezioni consigliato AWS che:

- Bloccare gli indirizzi IP dalle potenziali minacce basate sull'intelligence di minacce interne Amazon.
- Proteggere dalle vulnerabilità più comuni riscontrate nelle applicazioni Web come descritto nella OWASP Top 10.
- Difendere dagli utenti che rilevano le vulnerabilità delle applicazioni.

> **Important**
>
> È necessario abilitare AWS WAF se si desidera visualizzare i parametri di sicurezza nella dashboard di Sicurezza di CloudFront. Se AWS WAF non è abilitato, puoi utilizzare la

dashboard di Sicurezza solo per abilitare AWS WAF o configurare le restrizioni geografiche di CloudFront. Per ulteriori informazioni sulla dashboard, consulta Gestione delle protezioni di sicurezza AWS WAF nella dashboard di sicurezza CloudFront, più avanti in questa sezione.

Argomenti

Abilitazione di AWS WAF per le distribuzioni

Puoi abilitare AWS WAF durante la creazione di una distribuzione oppure abilitare le protezioni di sicurezza per una lista di controllo degli accessi (ACL) esistente.

Se abiliti AWS WAF per la distribuzione CloudFront, puoi anche abilitare il rilevamento dei bot e configurare la protezione di sicurezza in base alla categoria di bot.

Argomenti

Abilitazione di AWS WAF per una nuova distribuzione

Nella procedura seguente viene illustrato come abilitare AWS WAF quando si crea una nuova distribuzione CloudFront.

Come abilitare AWS WAF per una nuova distribuzione

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi seleziona Crea distribuzione.

3. Se necessario, segui i passaggi indicati in Creazione di una distribuzione.
4. Nella sezione Web Application Firewall, seleziona Modifica, quindi scegli Abilita le protezioni di sicurezza.
5. Completare i seguenti campi:

   - Usa la modalità di monitoraggio: puoi abilitare la modalità di monitoraggio se desideri prima raccogliere dati per verificare il funzionamento della protezione. Quando la modalità di monitoraggio è abilitata, le richieste non vengono bloccate se le protezioni erano attive. Invece, la modalità di monitoraggio raccoglie dati sulle richieste che verrebbero bloccate se le protezioni fossero attive. Quando sei pronto per iniziare il blocco, puoi abilitarlo nella pagina Sicurezza.
   - Protezioni aggiuntive: scegli le opzioni che desideri abilitare. Se abiliti la limitazione della velocità, consulta the section called “Impostare la limitazione della velocità” per ulteriori informazioni.
   - Stima del prezzo: puoi aprire la sezione per visualizzare un campo in cui inserire un numero diverso di richieste/mese e visualizzare una nuova stima.
6. Esamina le impostazioni di distribuzione rimanenti, quindi scegli Crea distribuzione.

Dopo aver creato una distribuzione, CloudFront crea una dashboard di sicurezza. Puoi usare questa dashboard per disabilitare o abilitare AWS WAF. Se non hai ancora abilitato AWS WAF, i grafici e i diagrammi nella dashboard rimangono vuoti.

Utilizzo di una ACL Web esistente

Se disponi di un ACL Web esistente, puoi utilizzarlo al posto della protezione offerta da AWS WAF.

Utilizzo di una configurazione AWS WAF esistente

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Esegui una di queste operazioni:

   a. Scegli Crea distribuzione e segui i passaggi indicati in Creazione di una distribuzione, quindi torna a questo argomento.

   b. Scegli una configurazione esistente, quindi seleziona la scheda Sicurezza.
3. Nella sezione Web Application Firewall (WAF), scegli Modifica, quindi Abilita le protezioni di sicurezza.

4. Scegliere Usa la configurazione WAF esistente. Questa opzione viene visualizzata solo se sono configurati gli ACL Web.
5. Scegliere l'ACL Web esistente dalla tabella Scegli un'ACL web.
6. Esamina le impostazioni di distribuzione rimanenti, quindi scegli Crea distribuzione.

Abilitazione del rilevamento dei bot

Se abiliti AWS WAF per la tua distribuzione CloudFront, puoi visualizzare le richieste di bot per un determinato intervallo di tempo nella dashboard di sicurezza nella console CloudFront. Puoi anche abilitare o disabilitare il rilevamento dei bot qui.

L'abilitazione del rilevamento dei bot comporta l'addebito di costi. La dashboard di sicurezza fornisce una stima dei costi.

Se abiliti il rilevamento dei bot, la dashboard di sicurezza mostra il traffico dei bot per ogni tipo e categoria di bot. Se disabiliti il rilevamento dei bot, il traffico dei bot viene visualizzato in base al campionamento delle richieste.

Per abilitare il Rilevamento dei bot

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione scegliere Distribuzioni, quindi scegliere la distribuzione da modificare.
3. Scegliere la scheda Sicurezza .
4. Scorri verso il basso fino alla sezione Richieste bot per un determinato intervallo di tempo e scegli Abilita rilevamento dei bot.
5. Nella finestra di dialogo Rilevamento dei bot, in Configurazione, seleziona la casella di controllo Abilita rilevamento dei bot per i bot comuni.
6. Scegli Save changes (Salva modifiche).

Configurazione della protezione per categoria di bot

Quando abiliti il rilevamento dei bot, puoi configurare il modo in cui ogni bot non verificato viene gestito per categoria di bot. Ad esempio, puoi impostare un bot della libreria HTTP in Modalità di monitoraggio e assegnare una Richiesta di verifica a uno strumento di controllo del collegamento.

> **Note**
>
> I bot noti da AWS per essere comuni e verificabili, come i crawler dei motori di ricerca noti, non sono soggetti alle azioni che hai impostato qui. Il Rilevamento dei bot conferma che i bot convalidati provengono dalla fonte dichiarata prima di contrassegnarli come verificati.

Come configurare la protezione per una categoria di bot

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione scegliere Distribuzioni, quindi scegliere la distribuzione da modificare.
3. Scegliere la scheda Sicurezza .
4. Nel grafico Richieste per categoria di bot, posiziona il puntatore su uno degli elementi nella colonna Azione bot non verificata e scegli l'icona della matita per modificarla.
5. Apri l'elenco ottenuto e scegli uno dei seguenti modi:
   - Blocco
   - Consenso
   - Modalità monitorata
   - CAPTCHA
   - Challenge
6. Seleziona il segno di spunta accanto all'elenco per salvare la modifica.

Gestione delle protezioni di sicurezza AWS WAF nella dashboard di sicurezza CloudFront

CloudFront crea una dashboard di sicurezza per ciascuna delle tue distribuzioni. Usi le dashboard nella console CloudFront. Con le dashboard, puoi utilizzare CloudFront e AWS WAF insieme in un'unica posizione per monitorare e gestire le protezioni di sicurezza comuni per le applicazioni Web. Le dashboard forniscono le seguenti attività e dati:

- Configurazione di sicurezza: puoi abilitare e disabilitare le protezioni AWS WAF e visualizzare tutte le protezioni specifiche dell'app, come quelle di WordPress.

- Tendenze in materia di sicurezza: questa categoria include le richieste consentite e bloccate, le richieste di verifica e CAPTCHA e i principali tipi di attacco. Puoi vedere i rapporti di traffico e come cambiano nel tempo. Ad esempio, se tutte le richieste aumentano del 3%, ma le richieste consentite aumentano del 14%, significa che hai consentito il passaggio di una parte maggiore del traffico nel periodo corrente.
- Richieste da bot: puoi vedere quanto traffico proviene dai bot, da quali tipi di bot (verificati o non verificati) e come cambiano le allocazioni percentuali dei tipi di bot (verificati o non verificati) nel tempo. Per ulteriori informazioni sull'abilitazione del rilevamento dei bot, consulta Abilitazione del rilevamento dei bot.
- Log delle richieste: i dati di log possono aiutare a rispondere a domande sulle tendenze della sicurezza o sulle richieste dei bot. È possibile effettuare ricerche nei log senza scrivere query e visualizzare grafici aggregati per determinare se un set di log filtrato è basato principalmente su un sottoinsieme di metodi HTTP, indirizzi IP, percorsi URI o paesi. Puoi passare il mouse sui valori nei grafici e bloccare indirizzi IP e Paesi. Per ulteriori informazioni, consulta Abilitazione dei log AWS WAF.
- Gestione delle restrizioni geografiche: CloudFront e AWS WAF offrono funzionalità di restrizione geografica. CloudFront offre gratuitamente restrizioni geografiche, ma le metriche relative alle restrizioni geografiche di CloudFront non vengono visualizzate nella dashboard di sicurezza. Per visualizzare le metriche relative alle richieste provenienti da paesi bloccati, è necessario utilizzare le restrizioni geografiche di AWS WAF. A tale scopo, passa il mouse su una barra del paese nella dashboard di sicurezza e blocca il paese. Per ulteriori informazioni, consulta Usa restrizioni CloudFront geografiche.
  - L'opzione Blocca potrebbe non essere disponibile se in precedenza hai creato una regola AWS WAF personalizzata al di fuori della console CloudFront per bloccare i paesi.

Argomenti

Prerequisiti

È necessario abilitare AWS WAF se si desidera visualizzare i parametri di sicurezza nella dashboard di Sicurezza di CloudFront. Se non abiliti AWS WAF, puoi utilizzare la dashboard di Sicurezza solo per abilitare AWS WAF o configurare le restrizioni geografiche di CloudFront.

Per ulteriori informazioni sull'abilitazione di AWS WAF, consulta Abilitazione di AWS WAF per le distribuzioni.

Abilitazione dei log AWS WAF

I dati dei log AWS WAF possono aiutarti a isolare modelli di traffico specifici. Ad esempio, i log possono mostrarti da dove proviene un determinato traffico o a cosa serve.

Se abiliti la registrazione di log AWS WAF su CloudWatch, la dashboard di sicurezza di CloudFront esegue query, aggrega e visualizza gli approfondimenti dai log di CloudWatch. Non addebitiamo costi per l'utilizzo della dashboard di sicurezza, ma i prezzi di CloudWatch si applicano ai log richiesti tramite la dashboard. Per ulteriori informazioni, consulta la pagina Prezzi di Amazon CloudWatch.

Per attivare i log

1. Inserisci il volume di richieste previsto nella casella Numero di richieste/mese per stimare i costi di abilitazione dei log.
2. Seleziona la casella di controllo Abilita log di AWS WAF.
3. Scegli Enable (Abilita).

CloudFront crea un gruppo di log di CloudWatch e aggiorna la configurazione AWS WAF per iniziare la registrazione su CloudWatch. Al primo utilizzo, i dati di log possono richiedere alcuni minuti ptima di essere visualizzati. La sezione Richieste del grafico elenca ogni richiesta. Sotto le singole richieste, i grafici a barre aggregano i dati per metodo HTTP, percorsi URI principali, indirizzi IP principali e Paesi principali. I grafici possono aiutarti a trovare modelli. Ad esempio, potresti visualizzare un volume sproporzionato di richieste da un singolo indirizzo IP o dati provenienti da un Paese che non hai mai visto in precedenza nei tuoi registri. Puoi filtrare le richieste in base a Paese, Intestazione host e altri attributi per individuare il traffico indesiderato. Una volta identificato il traffico, passa il mouse su una singola richiesta o su un elemento del grafico e blocca un indirizzo IP o un Paese.

> **Note**
>
> Le metriche visualizzate si basano sull'ACL Web. Pertanto, se associ lo stesso ACL Web a più distribuzioni, vedrai tutte le metriche relative all'ACL Web, non solo le richieste AWS WAF elaborate per tale distribuzione.

Impostare la limitazione della velocità

La limitazione della velocità è una delle raccomandazioni che potresti ricevere durante la configurazione delle protezioni di sicurezza.

CloudFront abilita sempre la limitazione della velocità in modalità monitoraggio. Quando la modalità monitoraggio è abilitata, CloudFront acquisisce metriche che indicano se la velocità configurata nel campo Limitazione velocità è stata superata, con quale frequenza e in che misura.

Dopo aver salvato la distribuzione, CloudFront inizia a raccogliere dati in base al numero nel campo Limitazione della velocità.

Puoi abilitare o gestire le impostazioni di limitazione della velocità nella sezione Sicurezza - Web Application Firewall (WAF) della scheda Sicurezza di qualsiasi distribuzione CloudFront.

> **Note**
>
> L'opzione Limitazione della velocità viene visualizzata nella console CloudFront solo se hai specificato un'origine personalizzata non S3 per la distribuzione. Altrimenti, vedrai solo le protezioni Core abilitate per la distribuzione. Per ulteriori informazioni sui tipi di origine, consulta Usa origini diverse con le distribuzioni CloudFront.

Come impostare la limitazione della velocità

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi seleziona la distribuzione da modificare.
3. Scegliere la scheda Sicurezza .
4. Nella sezione Sicurezza - Web Application Firewall (WAF), scegli Modifica.
5. In Protezioni aggiuntive, seleziona Limitazione della velocità. Puoi facoltativamente modificare il limite di velocità. Dopo aver eseguito il fine-tuning della tariffa, scegli Salva modifiche.
6. Nella sezione Sicurezza — Web Application Firewall (WAF), accanto a Limitazione della velocità, puoi scegliere Modalità di monitoraggio e quindi selezionare Abilita blocco per disattivare la modalità di monitoraggio. CloudFront inizierà a bloccare le richieste che superano il limite di velocità specificato.

Per ulteriori informazioni sull'abilitazione di AWS WAF e la limitazione della velocità, consulta il post del blog Introducing CloudFront Security Dashboard, a Unified CDN and Security Experience.

Disabilitazione delle protezioni di sicurezza AWS WAF

Se la distribuzione non richiede protezioni di sicurezza AWS WAF, puoi disabilitare questa funzionalità utilizzando la console CloudFront.

Se in precedenza hai abilitato la protezione AWS WAF e non hai scelto una configurazione WAF esistente (nota anche come protezione con un clic), CloudFront ha creato automaticamente un'ACL Web. Per gli ACL Web creati in questo modo, la console CloudFront dissocerà la risorsa ed eliminerà l'ACL Web.

Dissociare un ACL Web è diverso dall'eliminarlo. La dissociazione rimuove l'ACL Web dalla distribuzione, ma non lo elimina dall'Account AWS. Per ulteriori informazioni, consulta Associazione o dissociazione di un'ACL Web con una risorsa AWS nella Guida per gli sviluppatori di AWS WAF, AWS Firewall Manager e AWS Shield Advanced.

Consulta la seguente procedura per disabilitare le protezioni AWS WAF e dissociare l'ACL Web dalla distribuzione.

Come disabilitare le protezioni di sicurezza AWS WAF in CloudFront

1. Aprire la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi seleziona la distribuzione da modificare.
3. Scegli la scheda Sicurezza, quindi seleziona la scheda Modifica.
4. Nella sezione Web Application Firewall (WAF), scegli Disabilita protezione AWS WAF.
5. Scegli Save changes (Salva modifiche).

> **Note**
>
> - Se hai disabilitato la protezione di sicurezza AWS WAF e desideri comunque eliminare l'ACL Web dall'Account AWS, puoi eliminarlo manualmente. Segui la procedura per eliminare un'ACL Web. Nella console AWS WAF e Shield, per la pagina ACL Web, devi scegliere l'elenco Globale (CloudFront) per trovare gli ACL Web.

- Quando elimini una distribuzione dalla console CloudFront, CloudFront tenterà di eliminare anche l'ACL Web se hai scelto la protezione con un clic. Questo è il risultato massimo e non è sempre garantito. Per ulteriori informazioni, consulta Eliminazione di una distribuzione .

Configurazione dell’accesso sicuro e restrizione dell’accesso ai contenuti

CloudFront offre diverse opzioni per proteggere i contenuti che fornisce. Di seguito sono riportati alcuni metodi che è possibile utilizzare CloudFront per proteggere e limitare l'accesso ai contenuti:

- Configurazione di connessioni HTTPS.
- Impedire agli utenti in località geografiche specifiche di accedere ai contenuti
- Richiedi agli utenti di accedere ai contenuti utilizzando cookie CloudFront firmati URLs o firmati
- Impostare la crittografia a livello di campo per campi di contenuti specifici
- AWS WAF Utilizzalo per controllare l'accesso ai tuoi contenuti

È inoltre necessario implementare un'architettura DDo S-resiliente per l'infrastruttura e le applicazioni. Per ulteriori informazioni, consulta AWS Best Practices for DDo S Resiliency.

Per ulteriori informazioni, consulta la seguente documentazione:

- Proteggi la distribuzione dei contenuti con CloudFront
- SIEM su Amazon Service OpenSearch

Argomenti

Usa HTTPS con CloudFront

Puoi configurare CloudFront in modo che gli spettatori utilizzino HTTPS in modo che le connessioni siano crittografate quando CloudFront comunicano con gli spettatori. Puoi anche configurare l'utilizzo CloudFront di HTTPS con la tua origine in modo che le connessioni siano crittografate quando CloudFront comunica con la tua origine.

Se configuri CloudFront in modo da richiedere HTTPS sia per comunicare con gli spettatori sia per comunicare con l'origine, ecco cosa succede quando si CloudFront riceve una richiesta:

1. Un visualizzatore invia una richiesta HTTPS a. CloudFront C'è qualche SSL/TLS negoziazione qui tra lo spettatore e. CloudFront Alla fine, il visualizzatore invia la richiesta in formato crittografato.
2. Se la CloudFront edge location contiene una risposta memorizzata nella cache, CloudFront crittografa la risposta e la restituisce al visualizzatore, che la decrittografa.
3. Se l' CloudFront edge location non contiene una risposta memorizzata nella cache, CloudFront esegue la negoziazione SSL/TLS con l'origine e, una volta completata la negoziazione, inoltra la richiesta all'origine in un formato crittografato.
4. L'origine decrittografa la richiesta, la elabora (genera una risposta), crittografa la risposta e restituisce la risposta a. CloudFront
5. CloudFront decrittografa la risposta, la cripta nuovamente e la inoltra al visualizzatore. CloudFrontmemorizza inoltre nella cache la risposta nell'edge location in modo che sia disponibile la prossima volta che viene richiesta.
6. Il visualizzatore decripta la risposta.

Il processo funziona fondamentalmente allo stesso modo indipendentemente dal fatto che l'origine sia un bucket Amazon S3 o un'origine personalizzata come un server HTTP/S. MediaStore

> **Note**
>
> Per contribuire a contrastare gli attacchi di tipo SSL, non supporta la rinegoziazione per le richieste di visualizzazione e origine. CloudFront

In alternativa, puoi attivare l'autenticazione reciproca per la tua distribuzione. CloudFront Per ulteriori informazioni, consulta Visualizzatore TLS reciproco (mTLS).

Per informazioni su come richiedere l'HTTPS tra i visualizzatori e tra i CloudFront destinatari CloudFront e tra i destinatari, consulta i seguenti argomenti.

Argomenti

Richiedi HTTPS per la comunicazione tra gli spettatori e CloudFront

Puoi configurare uno o più comportamenti della cache nella tua CloudFront distribuzione per richiedere HTTPS per la comunicazione tra i visualizzatori e. CloudFront Puoi anche configurare uno o più comportamenti della cache per consentire sia HTTP che HTTPS, in modo che sia CloudFront necessario HTTPS per alcuni oggetti ma non per altri. I passaggi di configurazione dipendono dal nome di dominio che stai utilizzando nell'oggetto URLs:

- Se utilizzi il nome di dominio CloudFront assegnato alla tua distribuzione, ad esempio d111111abcdef8.cloudfront.net, modifichi l'impostazione della Viewer Protocol Policy per uno o più comportamenti della cache in modo da richiedere la comunicazione HTTPS. In CloudFront tale configurazione, fornisce il certificato. SSL/TLS

  Per modificare il valore di Viewer Protocol Policy utilizzando la CloudFront console, consulta la procedura riportata più avanti in questa sezione.

  Per informazioni su come utilizzare l' CloudFront API per modificare il valore dell'`ViewerProtocolPolicy`elemento, consulta UpdateDistributionAmazon CloudFront API Reference.
- Se utilizzi il tuo nome di dominio, ad esempio example.com, devi modificare diverse impostazioni CloudFront. È inoltre necessario utilizzare un SSL/TLS certificato fornito da AWS Certificate Manager (ACM) o importare un certificato da un'autorità di certificazione di terze parti in ACM o nell'archivio certificati IAM. Per ulteriori informazioni, consulta Utilizzo di nomi di dominio alternativi e HTTPS.

> **Note**
>
> Se vuoi assicurarti che gli oggetti da cui gli utenti ottengono i dati siano CloudFront crittografati quando li CloudFront hai ottenuti dall'origine, utilizza sempre il protocollo HTTPS tra l'origine CloudFront e l'origine. Se di recente sei passato da HTTP a HTTPS tra CloudFront e l'origine, ti consigliamo di invalidare gli oggetti nelle CloudFront edge location. CloudFront restituirà un oggetto a un visualizzatore indipendentemente dal fatto che il protocollo utilizzato dal visualizzatore (HTTP o HTTPS) corrisponda al protocollo CloudFront utilizzato per ottenere l'oggetto. Per ulteriori informazioni su come rimuovere o sostituire gli oggetti in una distribuzione, vedi Aggiunta, rimozione o sostituzione di contenuti distribuiti da CloudFront.

Richiesta di HTTPS per visualizzatori

Per richiedere HTTPS tra i visualizzatori e CloudFront per uno o più comportamenti della cache, effettuate la procedura seguente.

Per configurare la richiesta CloudFront di HTTPS tra i visualizzatori e CloudFront

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro superiore della CloudFront console, scegli l'ID della distribuzione che desideri aggiornare.
3. Nella scheda Comportamenti, seleziona il comportamento cache che desideri aggiornare, quindi seleziona Modifica.
4. Specifica uno dei valori seguenti per Policy protocollo visualizzatore:

   Reindirizza HTTP a HTTPS

   I visualizzatori possono utilizzare entrambi i protocolli. HTTP `GET` e `HEAD` le richieste vengono reindirizzate automaticamente alle richieste HTTPS. CloudFront restituisce il codice di stato HTTP 301 (Spostato permanentemente) insieme al nuovo URL HTTPS. Il visualizzatore invia quindi nuovamente la richiesta CloudFront utilizzando l'URL HTTPS.

> **Important**
>
> Se inviiPOST,, PUT DELETEOPTIONS, o PATCH tramite HTTP con un comportamento di cache da HTTP a HTTPS e una versione del protocollo di richiesta HTTP 1.1 o successiva, CloudFront reindirizza la richiesta a una posizione HTTPS con un codice di stato HTTP 307 (reindirizzamento temporaneo). Questo garantisce che la richiesta venga inviata di nuovo alla nuova posizione utilizzando lo stesso metodo e payload del corpo.
> Se inviiPOST,, PUT DELETEOPTIONS, o PATCH richieste tramite il comportamento della cache da HTTP a HTTPS con una versione del protocollo di richiesta inferiore a HTTP 1.1, CloudFront restituisce un codice di stato HTTP 403 (Proibito).

Quando un visualizzatore invia una richiesta HTTP che viene reindirizzata a una richiesta HTTPS, CloudFront addebita entrambe le richieste. Per la richiesta HTTP, l'addebito riguarda solo la richiesta e le intestazioni che vengono CloudFront restituite al visualizzatore. Per la richiesta HTTPS, l'addebito è per la richiesta, per le intestazioni e per l'oggetto che vengono restituiti dal server di origine.

Solo HTTPS

I visualizzatori possono accedere ai contenuti solo se utilizzano connessioni HTTPS. Se un visualizzatore invia una richiesta HTTP anziché una richiesta HTTPS, CloudFront restituisce il codice di stato HTTP 403 (Forbidden) e non restituisce l'oggetto.

5. Scegli Save changes (Salva modifiche).
6. Ripeti i passaggi da 3 a 5 per ogni comportamento aggiuntivo nella cache per cui desideri richiedere HTTPS tra i visualizzatori e. CloudFront
7. Conferma ciò che segue prima di utilizzare la configurazione aggiornata in un ambiente di produzione:

   - Il modello di percorso in ciascun comportamento cache si applica solo alle richieste per le quali desideri che i visualizzatori utilizzino una connessione HTTPS.
   - I comportamenti della cache sono elencati nell'ordine in cui desideri CloudFront valutarli. Per ulteriori informazioni, consulta Modello di percorso.
   - I comportamenti cache sono richieste di routing ai server di origine corretti.

Richiedi HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata

Puoi richiedere HTTPS per la comunicazione tra CloudFront e la tua origine.

> **Note**
>
> Se la tua origine è un bucket Amazon S3 configurato come endpoint del sito Web, non puoi configurare l'utilizzo di HTTPS con la tua origine perché Amazon S3 non supporta HTTPS CloudFront per gli endpoint dei siti Web.

Per richiedere HTTPS tra CloudFront e l'origine, segui le procedure in questo argomento per effettuare le seguenti operazioni:

1. Nella distribuzione, modifica l'impostazione Policy protocollo di origine per l'origine.
2. Installa un SSL/TLS certificato sul tuo server di origine (non è necessario quando utilizzi un'origine Amazon S3 o determinate altre AWS origini).

Argomenti

Richiesta di HTTPS per origini personalizzate

La procedura seguente spiega come configurare l'utilizzo di HTTPS CloudFront per comunicare con un sistema di bilanciamento del carico ELB, un' EC2 istanza Amazon o un'altra origine personalizzata. Per informazioni sull'utilizzo dell' CloudFront API per aggiornare una distribuzione, UpdateDistributionconsulta Amazon CloudFront API Reference.

Per configurare CloudFront in modo che richieda HTTPS tra CloudFront e la tua origine personalizzata

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro superiore della CloudFront console, scegli l'ID della distribuzione che desideri aggiornare.

3. Nella scheda Comportamenti, seleziona l'origine che desideri aggiornare, quindi scegli Modifica.
4. Aggiorna le seguenti impostazioni:

   Origin Protocol Policy (Policy protocollo origine)

   Cambia la Origin Protocol Policy (Policy protocollo server di origine) per i server di origine applicabili alla distribuzione:

   - Solo HTTPS: CloudFront utilizza solo HTTPS per comunicare con la tua origine personalizzata.
   - Match Viewer: CloudFront comunica con l'origine personalizzata tramite HTTP o HTTPS, a seconda del protocollo della richiesta del visualizzatore. Ad esempio, se scegli Match Viewer per Origin Protocol Policy e il visualizzatore utilizza HTTPS per richiedere un oggetto CloudFront, utilizza CloudFront anche HTTPS per inoltrare la richiesta all'origine.

     Seleziona Match Viewer (Abbina visualizzatore) solo se specifichi Redirect HTTP to HTTPS (Reindirizza HTTP a HTTPS) o HTTPS Only (solo HTTPS) per la Viewer Protocol Policy (Policy protocollo visualizzatore).

     CloudFront memorizza l'oggetto nella cache una sola volta anche se i visualizzatori effettuano richieste utilizzando entrambi i protocolli HTTP e HTTPS.

   Protocolli origine SSL

   Seleziona Origin SSL Protocols (Protocolli origine SSL) per i server di origine applicabili alla tua distribuzione. Il SSLv3 protocollo è meno sicuro, quindi ti consigliamo di scegliere SSLv3 solo se la tua origine non supporta TLSv1 o versioni successive. L' TLSv1 handshake è compatibile sia con le versioni precedenti che successive SSLv3, ma TLSv1 .1 e versioni successive no. Se lo desideri SSLv3, invia CloudFront solo richieste di handshake. SSLv3
5. Scegli Save changes (Salva modifiche).
6. Ripeti i passaggi da 3 a 5 per ogni origine aggiuntiva per la quale desideri richiedere HTTPS tra CloudFront e l'origine personalizzata.
7. Conferma ciò che segue prima di utilizzare la configurazione aggiornata in un ambiente di produzione:

   - Il modello di percorso in ciascun comportamento cache si applica solo alle richieste per le quali desideri che i visualizzatori utilizzino una connessione HTTPS.
   - I comportamenti della cache sono elencati nell'ordine in cui CloudFront desideri valutarli. Per ulteriori informazioni, consulta Modello di percorso.

- I comportamenti cache sono le richieste di routing ai server di origine per cui hai modificato la Origin Protocol Policy (Policy protocollo server di origine).

Installa un SSL/TLS certificato sulla tua origine personalizzata

Puoi utilizzare un SSL/TLS certificato proveniente dalle seguenti fonti sulla tua origine personalizzata:

- Se l'origine è un sistema di bilanciamento del carico ELB, è possibile utilizzare un certificato fornito da AWS Certificate Manager (ACM). Puoi inoltre utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti affidabile e importato in ACM.
- Per origini diverse dai sistemi di bilanciamento del carico ELB, è necessario utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti attendibile, ad esempio Comodo o Symantec. DigiCert

Il certificato restituito dall'origine deve includere uno dei seguenti nomi di dominio:

- Il nome di dominio nel campo Dominio di origine (il `DomainName` campo dell'API). CloudFront
- Il nome di dominio nell'intestazione `Host`, se il comportamento della cache è configurato per inoltrare l'intestazione `Host` all'origine.

Quando CloudFront utilizza HTTPS per comunicare con l'origine, CloudFront verifica che il certificato sia stato emesso da un'autorità di certificazione attendibile. CloudFront supporta le stesse autorità di certificazione di Mozilla. Per l'elenco corrente, consulta l'elenco dei certificati CA inclusi in Mozilla. Non è possibile utilizzare un certificato autofirmato per la comunicazione HTTPS tra CloudFront e l'origine.

> **Important**
>
> Se il server di origine restituisce un certificato scaduto, un certificato non valido o un certificato autofirmato oppure se restituisce la catena di certificati nell'ordine sbagliato, CloudFront interrompe la connessione TCP, restituisce il codice di stato HTTP 502 (Bad Gateway) al visualizzatore e imposta l'intestazione su. `X-Cache Error from cloudfront` Inoltre, se l'intera catena di certificati, incluso il certificato intermedio, non è presente, la connessione TCP viene interrotta. CloudFront

Richiedi HTTPS per la comunicazione tra CloudFront e la tua origine Amazon S3

Se la tua origine è un bucket Amazon S3, le opzioni di utilizzo di HTTPS per le comunicazioni CloudFront dipendono da come utilizzi il bucket. Se il tuo bucket Amazon S3 è configurato come endpoint di un sito Web, non puoi configurare l'utilizzo di HTTPS CloudFront per comunicare con la tua origine perché Amazon S3 non supporta le connessioni HTTPS in quella configurazione.

Se la tua origine è un bucket Amazon S3 che supporta la comunicazione HTTPS, CloudFront inoltra le richieste a S3 utilizzando il protocollo utilizzato dai visualizzatori per inviare le richieste. L'impostazione predefinita per Protocollo (solo origini personalizzate) è Match Viewer (Visualizzatore abbinamento) e non può essere modificata. Tuttavia, se abiliti il controllo dell'accesso all'origine (OAC) per la tua origine Amazon S3, la comunicazione utilizzata CloudFront tra Amazon S3 e Amazon S3 dipende dalle tue impostazioni. Per ulteriori informazioni, consulta Creazione di un nuovo controllo di accesso origine.

Se desideri richiedere HTTPS per la comunicazione tra Amazon S3 CloudFront e Amazon, devi modificare il valore di Viewer Protocol Policy per reindirizzare HTTP su HTTPS o solo HTTPS. La procedura riportata più avanti in questa sezione spiega come utilizzare la CloudFront console per modificare la Viewer Protocol Policy. Per informazioni sull'utilizzo dell' CloudFront API per aggiornare l'`ViewerProtocolPolicy`elemento per una distribuzione, UpdateDistributionconsulta Amazon CloudFront API Reference.

Quando usi HTTPS con un bucket Amazon S3 che supporta la comunicazione HTTPS, Amazon S3 fornisce il SSL/TLS certificato, quindi non devi farlo tu.

Richiesta di HTTPS per un'origine Amazon S3

La procedura seguente mostra come configurare la richiesta CloudFront di HTTPS alla tua origine Amazon S3.

CloudFront Per configurare la richiesta di HTTPS alla tua origine Amazon S3

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro superiore della CloudFront console, scegli l'ID della distribuzione che desideri aggiornare.
3. Nella scheda Behaviors (Comportamenti), seleziona il comportamento cache che desideri aggiornare, quindi seleziona Edit (Modifica).

4. Specifica uno dei valori seguenti per Viewer Protocol Policy (Policy protocollo visualizzatore):

   Reindirizza HTTP a HTTPS

   Gli spettatori possono utilizzare entrambi i protocolli, ma le richieste HTTP vengono reindirizzate automaticamente alle richieste HTTPS. CloudFront restituisce il codice di stato HTTP 301 (Spostato permanentemente) insieme al nuovo URL HTTPS. Il visualizzatore invia quindi nuovamente la richiesta CloudFront utilizzando l'URL HTTPS.

   > **Important**
   >
   > CloudFront non reindirizza`DELETE`, `OPTIONS` `PATCH``POST`, o `PUT` le richieste da HTTP a HTTPS. Se configuri un comportamento della cache per il reindirizzamento a HTTPS, CloudFront risponde a HTTP,`DELETE`, `OPTIONS` `PATCH``POST`, o alle `PUT` richieste relative a tale comportamento nella cache con il codice di stato HTTP 403 (Proibito).

   Quando un visualizzatore invia una richiesta HTTP che viene reindirizzata a una richiesta HTTPS, CloudFront addebita entrambe le richieste. Per la richiesta HTTP, l'addebito riguarda solo la richiesta e le intestazioni che vengono CloudFront restituite al visualizzatore. Per la richiesta HTTPS, l'addebito è per la richiesta, per le intestazioni e per l'oggetto restituiti dal server di origine.

   Solo HTTPS

   I visualizzatori possono accedere ai contenuti solo se utilizzano connessioni HTTPS. Se un visualizzatore invia una richiesta HTTP anziché una richiesta HTTPS, CloudFront restituisce il codice di stato HTTP 403 (Forbidden) e non restituisce l'oggetto.

5. Seleziona Yes, Edit (Sì, modifica).
6. Ripeti i passaggi da 3 a 5 per ogni comportamento aggiuntivo nella cache per cui desideri richiedere HTTPS tra i visualizzatori e CloudFront tra CloudFront e S3.
7. Conferma ciò che segue prima di utilizzare la configurazione aggiornata in un ambiente di produzione:

   - Il modello di percorso in ciascun comportamento cache si applica solo alle richieste per le quali desideri che i visualizzatori utilizzino una connessione HTTPS.

- I comportamenti della cache sono elencati nell'ordine in cui desideri CloudFront valutarli. Per ulteriori informazioni, consulta Modello di percorso.
- I comportamenti cache sono richieste di routing ai server di origine corretti.

Protocolli e cifrari supportati tra visualizzatori e CloudFront

Quando richiedi l'HTTPS tra i visualizzatori e la tua CloudFront distribuzione, devi scegliere una politica di sicurezza che determini le seguenti impostazioni:

- Il SSL/TLS protocollo minimo CloudFront utilizzato per comunicare con gli spettatori.
- I codici che è CloudFront possibile utilizzare per crittografare la comunicazione con gli spettatori.

Per scegliere una policy di sicurezza, specifica il valore applicabile per Policy di sicurezza (versione minima SSL/TLS). La tabella seguente elenca i protocolli e i codici che è CloudFront possibile utilizzare per ogni politica di sicurezza.

Un visualizzatore deve supportare almeno uno dei codici supportati con cui stabilire una connessione HTTPS. CloudFront CloudFront sceglie un codice nell'ordine elencato tra i codici supportati dal visualizzatore. Consulta anche Nomi di cifratura OpenSSL, s2n e RFC.

	Policy di sicurezza								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
Protocolli supportati SSL/TLS									
TLSv13.	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLSv12.	♦	♦	♦	♦	♦	♦	♦	♦	
TLSv11.	♦	♦	♦	♦					
TLSv1	♦	♦	♦						
SSLv3	♦								
TLSv1Cifre 3.0 supportate									

	Policy di sicurezza								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_ 0_05_ CHACHA2 POLY13 SHA256	♦	♦	♦	♦	♦	♦	♦		♦
Crittografie ECDSA supportate									
ECDHE-ECDSA- -GCM- AES128 SHA256	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-ECSA- - AES128 SHA256	♦	♦	♦	♦	♦	♦			
ECDHE-ECDSA- - SHA AES128	♦	♦	♦	♦					
ECDHE-ECDSA- -GCM- AES256 SHA384	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA CHACHA2 - 0-05 POLY13	♦	♦	♦	♦	♦	♦	♦		
ECDHE-ECDSA- AES256 - SHA384	♦	♦	♦	♦	♦	♦			

	Policy di sicurezza								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ECDHE-ECDSA- - SHA AES256	♦	♦	♦	♦					
Crittografie RSA supportate									
ECDH-RSA- -GCM-AES128 SHA256	♦	♦	♦	♦	♦	♦	♦	♦	
ECDH-RSA- AES128 - SHA256	♦	♦	♦	♦	♦	♦			
ECDHE-RSA-AES128 -SHA	♦	♦	♦	♦					
ECDHE-RSA-AES256 -GCM-SHA384	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-RSA CHACHA2 - 0-05 POLY13	♦	♦	♦	♦	♦	♦	♦		
ECDHE-RSA AES256 - - SHA384	♦	♦	♦	♦	♦	♦			
ECDHE-RSA-AES256 -SHA	♦	♦	♦	♦					
AES128-GCM-SHA256	♦	♦	♦	♦	♦				
AES256-GCM-SHA384	♦	♦	♦	♦	♦				
AES128-SHA256	♦	♦	♦	♦	♦				

	Policy di sicurezza								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
AES256-SHA	♦	♦	♦	♦					
AES128-SHA	♦	♦	♦	♦					
DES- -SHA CBC3	♦	♦							
RC4-MD5	♦								

Nomi di cifratura OpenSSL, s2n e RFC

OpenSSL e s2n utilizzano nomi diversi per i cifrari rispetto agli standard TLS (RFC 2246, RFC 4346, RFC 5246 e RFC 8446). La tabella seguente mappa i nomi OpenSSL e s2n al nome RFC per ogni crittografia.

CloudFront supporta scambi di chiavi classici e sicuri da un punto di vista quantistico. Per gli scambi di chiavi classici che utilizzano curve ellittiche, supporta quanto segue: CloudFront

- `prime256v1`
- `X25519`
- `secp384r1`

Per gli scambi di chiavi sicuri da un punto di vista quantistico, supporta quanto segue: CloudFront

- `X25519MLKEM768`
- `SecP256r1MLKEM768`

> **Note**
>
> Gli scambi di chiavi Quantum-safe sono supportati solo con TLS 1.3. TLS 1.2 e le versioni precedenti non supportano lo scambio di chiavi a sicurezza quantistica.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Crittografia post-quantistica
- Algoritmi di crittografia e Servizi AWS
- Scambio di chiavi ibrido in TLS 1.3

Per ulteriori informazioni sui requisiti dei certificati per CloudFront, vedere. Requisiti per l'utilizzo di certificati con SSL/TLS CloudFront

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
TLSv1Cifre 3.0 supportate	
TLS_AES_128_GCM_ SHA256	TLS_AES_128_GCM_ SHA256
TLS_AES_256_GCM_ SHA384	TLS_AES_256_GCM_ SHA384
TLS_ 0_05_ CHACHA2 POLY13 SHA256	TLS_ CHACHA2 POLY13 0_05_ SHA256
Crittografie ECDSA supportate	
ECDHE-ECDSA- -GCM- AES128 SHA256	TLS_ECDHE_ECDSA_CON_AES_128_GCM_ SHA256
ECDHE-ECDSA- - AES128 SHA256	TLS_ECDHE_ECDSA_CON_AES_128_CBC_ SHA256
ECDHE-ECDSA- -SHA AES128	TLS_ECDHE_ECDSA_WITH_AES_12 8_CBC_SHA
ECDHE-ECDSA- -GCM- AES256 SHA384	TLS_ECDHE_ECDSA_CON_AES_256_GCM_ SHA384
ECDHE-ECDSA- 0-05 CHACHA2 POLY13	TLS_ECDHE_ECDSA_CON_ CHACHA2 POLY13 0_ 05_ SHA256
ECDHE-ECDSA- - AES256 SHA384	TLS_ECDHE_ECDSA_CON_AES_256_CBC_ SHA384
ECDHE-ECDSA- -SHA AES256	TLS_ECDHE_ECDSA_WITH_AES_25 6_CBC_SHA

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
Crittografie RSA supportate	
ECDH-RSA- -GCM- AES128 SHA256	TLS_ECDHE_RSA_CON_AES_128_GCM_ SHA256
ECDHE-RSA- - AES128 SHA256	TLS_ECDHE_RSA_CON_AES_128_CBC_ SHA256
ECDHE-RSA- -SHA AES128	TLS_ECDHE_RSA_WITH_AES_128_ CBC_SHA
ECDHE-RSA- AES256 -GCM- SHA384	TLS_ECDHE_RSA_CON_AES_256_GCM_ SHA384
ECDHE-RSA- 0-05 CHACHA2 POLY13	CHACHA2TLS_ECDHE_RSA_CON_ POLY13 0_ 05_ SHA256
ECDHE-RSA- - AES256 SHA384	TLS_ECDHE_RSA_CON_AES_256_CBC_ SHA384
ECDHE-RSA- -SHA AES256	TLS_ECDHE_RSA_WITH_AES_256_ CBC_SHA
AES128-GCM- SHA256	TLS_RSA_CON_AES_128_GCM_ SHA256
AES256-GCM- SHA384	TLS_RSA_CON_AES_256_GCM_ SHA384
AES128-SHA256	TLS_RSA_CON_AES_128_CBC_ SHA256
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES- -SHA CBC3	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_CON_ _128_ RC4 MD5

Schemi di firma supportati tra spettatori e CloudFront

CloudFront supporta i seguenti schemi di firma per le connessioni tra spettatori e. CloudFront

	Policy di sicurezza								
Schemi di firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
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	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Policy di sicurezza								
Schemi di firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_RSA_ _ PKCS1 SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ SHA224	♦	♦	♦	♦	♦	♦	♦		
TLS_SIGNATURE_SCHEME_ECDSA_ SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_ SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_ SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Policy di sicurezza								
Schemi di firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_ECDSA_SHA224	♦	♦	♦	♦	♦	♦	♦		
TLS_SIGNATURE_SCHEME_ECDSA_R1_SECP256 SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_SECP384 R1_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
PKCS1TLS_SIGNATURE_SCHEME_RSA_ _SHA1	♦	♦	♦	♦					
TLS_SIGNATURE_SCHEME_ECDSA_SHA1	♦	♦	♦	♦					

Protocolli e cifrari supportati tra e l'origine CloudFront

Se scegli di richiedere HTTPS tra CloudFront e la tua origine, puoi decidere quale SSL/TLS protocollo consentire la connessione sicura e CloudFront puoi connetterti all'origine utilizzando uno dei codici ECDSA o RSA elencati nella tabella seguente. L'origine deve supportare almeno uno di questi codici per stabilire una connessione HTTPS CloudFront all'origine.

OpenSSL e s2n utilizzano nomi diversi per i cifrari rispetto agli standard TLS (RFC 2246, RFC 4346, RFC 5246 e RFC 8446). La tabella seguente mappa i nomi OpenSSL e s2n e il nome RFC per ogni cifrario.

Per i cifrari con algoritmi di scambio di chiavi a curva ellittica, supporta le seguenti curve ellittiche: CloudFront

- prime256v1
- secp384r1
- X25519

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
Crittografie ECDSA supportate	
AES256ECDHE-ECDSA- -GCM- SHA384	TLS_ECDHE_ECDSA_CON_AES_256_GCM_SHA384
ECDHE-ECDSA- - AES256 SHA384	TLS_ECDHE_ECDSA_CON_AES_256_CBC_SHA384
ECDHE-ECDSA- -SHA AES256	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA- -GCM- AES128 SHA256	TLS_ECDHE_ECDSA_CON_AES_128_GCM_SHA256
ECDHE-ECDSA- - AES128 SHA256	TLS_ECDHE_ECDSA_CON_AES_128_CBC_SHA256
ECDHE-ECDSA- -SHA AES128	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
Crittografie RSA supportate	
ECDH-RSA- -GCM- AES256 SHA384	TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
ECDHE-RSA- - AES256 SHA384	TLS_ECDHE_RSA_CON_AES_256_CBC_ SHA384
ECDHE-RSA- -SHA AES256	TLS_ECDHE_RSA_WITH_AES_256_ CBC_SHA
ECDHE-RSA- AES128 -GCM- SHA256	TLS_ECDHE_RSA_CON_AES_128_GCM_ SHA256
ECDHE-RSA- - AES128 SHA256	TLS_ECDHE_RSA_CON_AES_128_CBC_ SHA256
ECDHE-RSA- -SHA AES128	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- -SHA CBC3	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_CON_ _128_ RC4 MD5

Schemi di firma supportati tra e l'origine CloudFront

CloudFront supporta i seguenti schemi di firma per le connessioni tra CloudFront e l'origine.

- TLS_SIGNATURE_SCHEME_RSA_ _ PKCS1 SHA256
- PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ SHA384
- PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ SHA512
- PKCS1TLS_SIGNATURE_SCHEME_RSA_ _ 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

Utilizzo di nomi di dominio alternativi e HTTPS

Se desideri utilizzare il tuo nome di dominio URLs per i tuoi file (ad esempio`https://www.example.com/image.jpg`) e desideri che i tuoi utenti utilizzino HTTPS, devi completare i passaggi descritti nei seguenti argomenti. (Se, ad esempio, utilizzi il nome di dominio di CloudFront distribuzione predefinito nel tuo URLs, ad esempio`https://d111111abcdef8.cloudfront.net/image.jpg`, segui invece le indicazioni riportate nel seguente argomento:Richiedi HTTPS per la comunicazione tra gli spettatori e CloudFront.)

> **Important**
>
> Quando aggiungi un certificato alla tua distribuzione, lo propaga CloudFront immediatamente a tutte le sue edge location. Quando saranno disponibili nuove edge location, CloudFront propagherà il certificato anche a tali posizioni. Non è possibile limitare le edge location verso cui CloudFront vengono propagati i certificati.

Argomenti

- Scegli in che modo CloudFront vengono servite le richieste HTTPS
- Requisiti per l'utilizzo di certificati con SSL/TLS CloudFront
- Quote sull'utilizzo di SSL/TLS certificati con CloudFront (HTTPS solo tra visualizzatori e CloudFront solo tra visualizzatori)
- Configurazione di nomi di dominio alternativi e HTTPS
- Determina la dimensione della chiave pubblica in un certificato SSL/TLS RSA
- Aumento delle quote per certificati SSL/TLS
- Ruota SSL/TLS i certificati
- Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront
- Passaggio da un certificato SSL/TLS personalizzato con indirizzi IP dedicati a SNI

Scegli in che modo CloudFront vengono servite le richieste HTTPS

Se desideri che i tuoi spettatori utilizzino HTTPS e utilizzino nomi di dominio alternativi per i tuoi file, scegli una delle seguenti opzioni per il modo in cui vengono gestite le richieste CloudFront HTTPS:

- Utilizzare la Server Name Indication (SNI): scelta consigliata
- Utilizzare un indirizzo IP dedicato in ogni edge location

Questa sezione spiega come funziona ciascuna opzione.

Utilizzo di SNI per servire le richieste HTTPS (funziona per la maggior parte dei client)

Server Name Indication (SNI) è un'estensione del protocollo TLS supportato da browser e client rilasciati dopo il 2010. Se configuri CloudFront per servire le richieste HTTPS utilizzando SNI, CloudFront associa il nome di dominio alternativo a un indirizzo IP per ogni edge location. Quando un visualizzatore invia una richiesta HTTPS per i tuoi contenuti, il DNS instrada la richiesta all'indirizzo IP per la edge location corretta. L'indirizzo IP del nome di dominio viene determinato durante la negoziazione dell' SSL/TLS handshake; l'indirizzo IP non è dedicato alla distribuzione.

La SSL/TLS negoziazione avviene all'inizio del processo di creazione di una connessione HTTPS. Se non è CloudFront possibile determinare immediatamente a quale dominio si riferisce la richiesta, la connessione viene interrotta. Quando un visualizzatore che supporta la SNI invia una richiesta HTTPS per i tuoi contenuti, ecco cosa succede:

1. Il visualizzatore ottiene automaticamente il nome di dominio dall'URL della richiesta e lo aggiunge all'estensione SNI del messaggio di saluto del client TLS.
2. Quando CloudFront riceve il client TLS, utilizza il nome di dominio nell'estensione SNI per trovare la CloudFront distribuzione corrispondente e restituisce il certificato TLS associato.
3. Il visualizzatore ed CloudFront eseguono la negoziazione. SSL/TLS
4. CloudFront restituisce il contenuto richiesto al visualizzatore.

Per un elenco aggiornato dei browser che supportano la SNI, vedi la voce Wikipedia Server Name Indication.

Se desideri utilizzare la SNI ma alcuni browser degli utenti non supportano le SNI, hai diverse opzioni:

- Configura CloudFront per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati anziché SNI. Per ulteriori informazioni, consulta Utilizzo di un indirizzo IP dedicato per servire le richieste HTTPS (funziona per tutti i client).
- Utilizza il certificato CloudFront SSL/TLS anziché un certificato personalizzato. Ciò richiede che tu utilizzi il nome di CloudFront dominio per la distribuzione in per i tuoi file, URLs ad esempio,. `https://d111111abcdef8.cloudfront.net/logo.png`

  Se utilizzi il CloudFront certificato predefinito, gli utenti devono supportare il protocollo SSL TLSv1 o versioni successive. CloudFront non supporta il SSLv3 certificato predefinitoCloudFront .

  È inoltre necessario modificare il SSL/TLS certificato in CloudFront uso da un certificato personalizzato a un CloudFront certificato predefinito:

  - Se non hai utilizzato la tua distribuzione per distribuire i contenuti, puoi modificare la configurazione. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
  - Se hai utilizzato la tua distribuzione per distribuire i contenuti, devi creare una nuova CloudFront distribuzione e modificare i file URLs per ridurre o eliminare il periodo di indisponibilità dei contenuti. Per ulteriori informazioni, consulta Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront .
- Se puoi verificare qual è il browser utilizzato dagli utenti, allora aggiornalo a una versione che supporta la SNI.
- Utilizza HTTP anziché HTTPS.

Utilizzo di un indirizzo IP dedicato per servire le richieste HTTPS (funziona per tutti i client)

Server Name Indication (SNI) costituisce un modo per associare una richiesta a un dominio. Un altro modo consiste nell'utilizzare un indirizzo IP dedicato. Se gli utenti non sono in grado di effettuare l'aggiornamento a un browser o un client rilasciato dopo il 2010, puoi utilizzare un indirizzo IP dedicato per fornire le richieste HTTPS. Per un elenco aggiornato dei browser che supportano la SNI, vedi la voce Wikipedia Server Name Indication.

> **Important**
>
> Se CloudFront configuri per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati, dovrai sostenere un costo mensile aggiuntivo. L'addebito inizia quando si associa il SSL/TLS certificato a una distribuzione e si abilita la distribuzione. Per ulteriori informazioni sui

CloudFront prezzi, consulta la pagina CloudFront dei prezzi di Amazon. Inoltre, fai riferimento a Using the Same Certificate for Multiple CloudFront Distributions.

Quando configuri CloudFront per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati, CloudFront associa il certificato a un indirizzo IP dedicato in ogni CloudFront edge location. Quando un visualizzatore invia una richiesta HTTPS per i tuoi contenuti, ecco cosa succede:

1. DNS instrada la richiesta all'indirizzo IP della tua distribuzione nella edge location di riferimento.
2. Se una richiesta client fornisce l'estensione SNI nel `ClientHello` messaggio, CloudFront cerca una distribuzione associata a tale SNI.
   - Se c'è una corrispondenza, CloudFront risponde alla richiesta con il certificato SSL/TLS.
   - Se non c'è alcuna corrispondenza, CloudFront utilizza invece l'indirizzo IP per identificare la distribuzione e determinare quale certificato SSL/TLS restituire al visualizzatore.
3. Il visualizzatore ed CloudFront eseguiamo la SSL/TLS negoziazione utilizzando il certificato SSL/TLS.
4. CloudFront restituisce il contenuto richiesto al visualizzatore.

Questo metodo funziona per ogni richiesta HTTPS, indipendentemente dal browser o da un altro visualizzatore che l'utente sta utilizzando.

> **Note**
>
> IPs I dedicati non sono statici IPs e possono cambiare nel tempo. L'indirizzo IP restituito per l'edge location viene allocato dinamicamente dagli intervalli di indirizzi IP dell'elenco dei server CloudFront periferici.
> Gli intervalli di indirizzi IP per i server CloudFront edge sono soggetti a modifiche. Per ricevere notifiche sulle modifiche all'indirizzo IP, iscriviti a AWS Public IP Address Changes tramite Amazon SNS.

Richiedi l'autorizzazione per utilizzare tre o più certificati IP SSL/TLS dedicati

Se hai bisogno dell'autorizzazione per associare permanentemente tre o più certificati IP dedicati SSL/TLS a CloudFront, esegui la procedura seguente. Per ulteriori informazioni sulle richieste HTTPS, consulta Scegli in che modo CloudFront vengono servite le richieste HTTPS.

> **Note**
>
> Questa procedura consente di utilizzare tre o più certificati IP dedicati tra le distribuzioni. CloudFront Il valore predefinito è 2. Tieni presente che non è possibile associare più di un certificato SSL a una distribuzione.
> È possibile associare un solo SSL/TLS certificato alla volta a una CloudFront distribuzione. Questo numero indica il numero totale di certificati SSL IP dedicati che puoi utilizzare in tutte le tue CloudFront distribuzioni.

Per richiedere l'autorizzazione per l'utilizzo di tre o più certificati con una distribuzione CloudFront

1. Visita il Centro di supporto e immetti una richiesta.
2. Indica il numero di certificati per i quali hai bisogno dell'autorizzazione all'utilizzo e descrivi le circostanze nella tua richiesta. Aggiorneremo il tuo account appena possibile.
3. Continua con la procedura successiva.

Requisiti per l'utilizzo di certificati con SSL/TLS CloudFront

I requisiti per SSL/TLS i certificati sono descritti in questo argomento. Si applicano, ad eccezione di quanto indicato sopra, nei seguenti casi:

- Certificati per l'utilizzo di HTTPS tra visualizzatori e CloudFront
- Certificati per l'utilizzo di HTTPS tra CloudFront e l'origine

Argomenti

- Autorità di certificazione
- Regione AWS per AWS Certificate Manager
- Formato del certificato
- Certificati intermedi
- Tipo di chiavi
- Chiave privata
- Permissions
- Dimensioni della chiave di certificato

- Tipi di certificati supportati
- Data di scadenza e rinnovo certificati
- Nomi di dominio nella CloudFront distribuzione e nel certificato
- Versione minima SSL/TLS del protocollo
- Versioni HTTP supportate

Autorità di certificazione

Ti consigliamo di usare un certificato rilasciato da AWS Certificate Manager (ACM). Per informazioni su come ottenere un certificato da ACM, consulta la Guida per l'utente di AWS Certificate Manager. Per utilizzare un certificato ACM con una CloudFront distribuzione, assicurati di richiedere (o importare) il certificato nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

CloudFront supporta le stesse autorità di certificazione (CAs) di Mozilla, quindi se non usi ACM, usa un certificato emesso da una CA presente nell'elenco dei certificati CA inclusi di Mozilla.

I certificati TLS utilizzati dall'origine specificata per la CloudFront distribuzione devono essere emessi anche dalla CA presente nell'elenco dei certificati CA inclusi da Mozilla.

Per ulteriori informazioni su come ottenere e installare un certificato SSL/TLS, consulta la documentazione del software del server HTTP e la documentazione relativa all'autorità di certificazione.

Regione AWS per AWS Certificate Manager

Per utilizzare un certificato in AWS Certificate Manager (ACM) per richiedere HTTPS tra i visualizzatori eCloudFront, assicurati di richiedere (o importare) il certificato nella regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1`

Se desideri richiedere l'HTTPS tra CloudFront e la tua origine e utilizzi un sistema di bilanciamento del carico in ELB come origine, puoi richiedere o importare il certificato in qualsiasi formato. Regione AWS

Formato del certificato

Il certificato deve essere in formato PEM X.509. Questo è il formato di default se si utilizza AWS Certificate Manager.

Certificati intermedi

Se stai utilizzando un'autorità di certificazione (CA) di terza parte, nel file `.pem` elenca tutti i certificati intermedi della catena di certificati, a partire da uno per la CA che ha firmato il certificato per il tuo dominio. Di solito, puoi trovare un file sul sito Web della CA in cui vengono elencati i certificati intermedi e root concatenati nel giusto ordine.

> **Important**
>
> Non includere i seguenti certificati: il certificato root, i certificati intermedi che non sono nel percorso attendibile oppure il certificato della chiave pubblica della CA.

Ecco un esempio:

```
-----BEGIN CERTIFICATE-----
Intermediate certificate 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate certificate 1
-----END CERTIFICATE-----
```

Tipo di chiavi

CloudFront supporta coppie di chiavi pubbliche-private RSA ed ECDSA.

CloudFront supporta connessioni HTTPS sia verso i visualizzatori che verso le origini utilizzando certificati RSA ed ECDSA. Con AWS Certificate Manager (ACM), puoi richiedere e importare certificati RSA o ECDSA e quindi associarli alla tua distribuzione. CloudFront

Per gli elenchi dei codici RSA ed ECDSA supportati da cui è possibile negoziare in connessioni HTTPS, CloudFront vedere e. the section called “Protocolli e cifrari supportati tra visualizzatori e CloudFront” the section called “Protocolli e cifrari supportati tra e l'origine CloudFront ”

Chiave privata

Se utilizzi un certificato di un'autorità di certificazione (CA) esterna, tieni presente quanto segue:

- La chiave privata deve corrispondere alla chiave pubblica presente nel certificato.

- La chiave privata deve essere nel formato PEM.
- La chiave privata non può essere crittografata con una password.

Se AWS Certificate Manager (ACM) ha fornito il certificato, ACM non rilascia la chiave privata. La chiave privata viene archiviata in ACM per essere utilizzata dai AWS servizi integrati con ACM.

Permissions

È necessario disporre dell'autorizzazione per utilizzare e importare il SSL/TLS certificato. Se utilizzi AWS Certificate Manager (ACM), ti consigliamo di utilizzare AWS Identity and Access Management le autorizzazioni per limitare l'accesso ai certificati. Per ulteriori informazioni, consulta Identity and Access Management nella Guida per l'utente di AWS Certificate Manager .

Dimensioni della chiave di certificato

La dimensione della chiave del certificato CloudFront supportata dipende dal tipo di chiave e di certificato.

Per i certificati RSA:

CloudFront supporta chiavi RSA a 1024 bit, 2048 bit, 3072 bit e 4096 bit. La lunghezza massima della chiave per un certificato RSA da utilizzare è di 4096 bit. CloudFront

Nota che ACM emette certificati RSA con chiavi fino a 2048 bit. Per utilizzare un certificato RSA a 3072 o 4096 bit, è necessario ottenere il certificato esternamente e importarlo in ACM, dopodiché sarà disponibile per l'uso. CloudFront

Per informazioni su come stabilire le dimensioni di una chiave RSA, consulta Determina la dimensione della chiave pubblica in un certificato SSL/TLS RSA.

Per i certificati ECDSA:

CloudFront supporta chiavi a 256 bit. Per utilizzare un certificato ECDSA in ACM per richiedere HTTPS tra i visualizzatori e CloudFront, usa la curva ellittica prime256v1.

Tipi di certificati supportati

CloudFront supporta tutti i tipi di certificati emessi da un'autorità di certificazione affidabile.

Data di scadenza e rinnovo certificati

Se utilizzi certificati ottenuti da un'autorità di certificazione (CA) di terze parti, devi monitorare le date di scadenza dei certificati e rinnovare i certificati importati in AWS Certificate Manager (ACM) o caricati nell'archivio AWS Identity and Access Management certificati prima della scadenza.

> **Important**
>
> Per evitare problemi legati alla scadenza del certificato, rinnovalo o reimportalo almeno 24 ore prima del valore `NotAfter` del certificato attuale. Se il certificato scade entro 24 ore, richiedi un nuovo certificato ad ACM o importa un nuovo certificato in ACM. Successivamente, associa il nuovo certificato alla distribuzione. CloudFront CloudFront potrebbe continuare a utilizzare il certificato precedente mentre è in corso il rinnovo o la reimportazione del certificato. Si tratta di un processo asincrono che può richiedere fino a 24 ore prima CloudFront che vengano visualizzate le modifiche.

Se utilizzi certificati forniti da ACM, ACM gestisce automaticamente il rinnovo dei certificati. Per ulteriori informazioni, consulta Rinnovo gestito nella Guida per l'utente di AWS Certificate Manager .

Nomi di dominio nella CloudFront distribuzione e nel certificato

Quando utilizzi un'origine personalizzata, il SSL/TLS certificato relativo alla tua origine include un nome di dominio nel campo Nome comune e probabilmente molti altri nel campo Nomi alternativi dell'oggetto. (CloudFront supporta caratteri jolly nei nomi di dominio dei certificati.)

Uno dei nomi di dominio nel certificato deve corrispondere al nome di dominio specificato per Nome dominio origine. Se nessun nome di dominio corrisponde, CloudFront restituisce il codice di stato HTTP `502 (Bad Gateway)` al visualizzatore.

> **Important**
>
> Quando aggiungi un nome di dominio alternativo a una distribuzione, CloudFront verifica che il nome di dominio alternativo sia coperto dal certificato che hai allegato. Il certificato deve coprire il nome di dominio alternativo nel campo del nome alternativo dell'oggetto (SAN) del certificato. Ciò significa che il campo SAN deve contenere una corrispondenza esatta del nome di dominio alternativo o contenere un carattere jolly allo stesso livello del nome di dominio alternativo che si sta aggiungendo.

Per ulteriori informazioni, consulta Requisiti per l'utilizzo di nomi di dominio alternativi.

Versione minima SSL/TLS del protocollo

Se utilizzi indirizzi IP dedicati, imposta la versione minima del SSL/TLS protocollo per la connessione tra gli spettatori e CloudFront scegli una politica di sicurezza.

Per ulteriori informazioni, consulta Policy di sicurezza (versione minima SSL/TLS) nell'argomento Riferimento a tutte le impostazioni di distribuzione.

Versioni HTTP supportate

Se associ un certificato a più di una CloudFront distribuzione, tutte le distribuzioni associate al certificato devono utilizzare la stessa opzione per. Versioni HTTP supportate Questa opzione viene specificata quando si crea o si aggiorna una CloudFront distribuzione.

Quote sull'utilizzo di SSL/TLS certificati con CloudFront (HTTPS solo tra visualizzatori e CloudFront solo tra visualizzatori)

Nota le seguenti quote sull'utilizzo SSL/TLS dei certificati conCloudFront. Queste quote si applicano solo ai SSL/TLS certificati forniti utilizzando AWS Certificate Manager (ACM), importati in ACM o caricati nell'archivio certificati IAM per la comunicazione HTTPS tra i visualizzatori e. CloudFront

Per ulteriori informazioni, consulta Aumento delle quote per certificati SSL/TLS.

Numero massimo di certificati per distribuzione CloudFront

È possibile associare un massimo di un SSL/TLS certificato a ciascuna CloudFront distribuzione.

Numero massimo di certificati che puoi importare in ACM o caricare nello store certificati IAM

Se i SSL/TLS certificati sono stati ottenuti da una CA di terze parti, è necessario archiviarli in una delle seguenti posizioni:

- AWS Certificate Manager: per la quota corrente sul numero di certificati ACM, consulta Quote nella Guida per l'utente di AWS Certificate Manager . La quota elencata è un totale che include i certificati di cui è stato effettuato il provisioning utilizzando ACM e certificati importati in ACM.
- Archivio certificati IAM: per la quota attuale (precedentemente nota come limite) sul numero di certificati che puoi caricare nell'archivio certificati IAM per un AWS account, consulta IAM and

STS Limits nella IAM User Guide. Puoi richiedere un aumento della quota utilizzando la console Service Quotas.

Numero massimo di certificati per AWS account (solo indirizzi IP dedicati)

Se desideri servire le richieste HTTPS utilizzando indirizzi IP dedicati, tieni presente quanto segue:

- Per impostazione predefinita, ti CloudFront consente di utilizzare due certificati con il tuo AWS account, uno per l'uso quotidiano e uno per quando devi ruotare i certificati per più distribuzioni.
- Se hai bisogno di più di due SSL/TLS certificati personalizzati per il tuo AWS account, puoi richiedere una quota più alta nella console Service Quotas.

Utilizza lo stesso certificato per CloudFront le distribuzioni create utilizzando account diversi AWS

Se utilizzi una CA di terze parti e desideri utilizzare lo stesso certificato con più CloudFront distribuzioni create utilizzando AWS account diversi, devi importare il certificato in ACM o caricarlo nell'archivio certificati IAM una volta per ogni account. AWS

Se utilizzi certificati forniti da ACM, non puoi configurare l'utilizzo CloudFront di certificati creati da un account diverso. AWS

Utilizza lo stesso certificato per CloudFront e per altri servizi AWS

Se hai acquistato un certificato da un'autorità di certificazione affidabile come Comodo o Symantec, puoi utilizzare lo stesso certificato per CloudFront e per altri AWS servizi. DigiCert Se stai importando il certificato in ACM, è necessario importarlo solo una volta per utilizzarlo per più servizi AWS .

Se usi certificati forniti da ACM, i certificati vengono archiviati in ACM.

Usa lo stesso certificato per più distribuzioni CloudFront

È possibile utilizzare lo stesso certificato per una o per tutte le distribuzioni CloudFront utilizzate per elaborare le richieste HTTPS. Tenere presente quanto segue:

- Puoi utilizzare lo stesso certificato sia per l'elaborazione di richieste tramite indirizzi IP dedicati sia per l'elaborazione di richieste tramite la SNI.
- È possibile associare solo un certificato a ogni distribuzione.
- Ogni distribuzione deve includere uno o più nomi di dominio alternativi che appariranno anche nel campo Common Name (Nome comune) o nel campo Subject Alternative Names (Nomi alternativi oggetto) del certificato.

- Se gestisci richieste HTTPS utilizzando indirizzi IP dedicati e hai creato tutte le distribuzioni utilizzando lo stesso AWS account, puoi ridurre significativamente i costi utilizzando lo stesso certificato per tutte le distribuzioni. CloudFront costi per ogni certificato, non per ogni distribuzione.

  Ad esempio, supponiamo di creare tre distribuzioni utilizzando lo stesso AWS account e di utilizzare lo stesso certificato per tutte e tre le distribuzioni. Ti verrà addebitata solo una tariffa per l'utilizzo di indirizzi IP dedicati.

  Tuttavia, se gestisci richieste HTTPS utilizzando indirizzi IP dedicati e utilizzi lo stesso certificato per creare CloudFront distribuzioni in AWS account diversi, a ciascun account viene addebitata la tariffa per l'utilizzo di indirizzi IP dedicati. Ad esempio, se crei tre distribuzioni utilizzando tre AWS account diversi e utilizzi lo stesso certificato per tutte e tre le distribuzioni, a ciascun account viene addebitata l'intera tariffa per l'utilizzo di indirizzi IP dedicati.

Configurazione di nomi di dominio alternativi e HTTPS

Per utilizzare nomi di dominio alternativi URLs per i file e utilizzare HTTPS tra i visualizzatori CloudFront, esegui le procedure applicabili.

Argomenti

Ottieni un certificato SSL/TLS

Richiedi un SSL/TLS certificato se non ne hai già uno. Per ulteriori informazioni, consulta la documentazione relativa:

- Per utilizzare un certificato fornito da AWS Certificate Manager (ACM), consulta la Guida per l'AWS Certificate Manager utente. Quindi passa a Aggiorna la tua CloudFront distribuzione.

> **Note**
>
> Si consiglia di utilizzare ACM per fornire, gestire e distribuire SSL/TLS certificati su AWS risorse gestite. È necessario richiedere un certificato ACM nella regione degli Stati Uniti orientali (Virginia settentrionale).

- Per ottenere un certificato da un'autorità di certificazione esterna (CA), consulta la documentazione fornita dall'autorità di certificazione. Quando hai il certificato, continua con la procedura.

Importazione di un certificato SSL/TLS

Se hai ricevuto il tuo certificato da un'autorità di certificazione di terze parti, importa il certificato in ACM o caricalo nello store certificati IAM:

ACM (consigliato)

ACM ti consente di importare certificati di terze parti dalla console ACM, nonché in modo programmatico. Per informazioni sull'importazione di un certificato in ACM, consulta Importazione di certificati in AWS Certificate Manager nella Guida per l'utente di AWS Certificate Manager . È necessario importare il certificato nella regione Stati Uniti orientali (Virginia settentrionale).

Archivio certificati IAM

(Non consigliato) Utilizza il seguente AWS CLI comando per caricare il certificato di terze parti nell'archivio certificati 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/
```

Tenere presente quanto segue:

- AWS account: devi caricare il certificato nell'archivio certificati IAM utilizzando lo stesso AWS account che hai usato per creare la tua CloudFront distribuzione.
- --parametro del percorso - Quando si carica il certificato in IAM, il valore del parametro `--path` (percorso certificato) deve iniziare con `/cloudfront/`, ad esempio `/cloudfront/production/` o `/cloudfront/test/`. Il percorso deve terminare con una /.

- Certificati esistenti: devi specificare i valori per i parametri `--server-certificate-name` e `--path` diversi dai valori associati ai certificati esistenti.
- Utilizzo della CloudFront console: il valore specificato per il `--server-certificate-name` parametro, ad esempio AWS CLI`myServerCertificate`, viene visualizzato nell'elenco dei certificati SSL della CloudFront console.
- Utilizzo dell' CloudFront API: prendi nota della stringa alfanumerica che AWS CLI restituisce, ad esempio. `AS1A2M3P4L5E67SIIXR3J` Questo è il valore che verrà specificato nell'elemento `IAMCertificateId`. Non hai bisogno dell'ARN IAM che viene restituito dalla CLI.

Per ulteriori informazioni su AWS CLI, consulta la Guida per l'AWS Command Line Interface utente e il AWS CLI Command Reference.

Aggiorna la tua CloudFront distribuzione

Per aggiornare le impostazioni della distribuzione, esegui la procedura seguente:

Per configurare la CloudFront distribuzione per nomi di dominio alternativi

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli l'ID della distribuzione che intendi aggiornare.
3. Nella scheda General (Generale), seleziona Edit (Modifica).
4. Aggiorna i seguenti valori:

   Nome di dominio alternativo (CNAME)

   Selezionare Aggiungi elemento per aggiungere i nomi di dominio alternativi applicabili. Separa i nomi di dominio con le virgole o digita ogni nome di dominio su una riga.

   Certificato SSL personalizzato

   Seleziona un certificato dall'elenco a discesa.

   Di seguito sono elencati fino a 100 certificati. Se disponi di più di 100 certificati e non riesci a visualizzare il certificato che desideri aggiungere, puoi digitare un ARN del certificato nel campo per la selezione.

Se hai caricato un certificato nell'archivio certificati IAM ma non è elencato e non puoi selezionarlo digitandone il nome nel campo, consulta la procedura Importazione di un certificato SSL/TLS per avere la conferma del suo corretto caricamento.

> **Important**
>
> Dopo aver associato il SSL/TLS certificato alla CloudFront distribuzione, non eliminarlo da ACM o dall'archivio certificati IAM finché non lo rimuovi da tutte le distribuzioni e tutte le distribuzioni non sono state distribuite.

5. Scegli Save changes (Salva modifiche).
6. Configura CloudFront per richiedere HTTPS tra i visualizzatori e: CloudFront

   a. Nella scheda Behaviors (Comportamenti), seleziona il comportamento cache che desideri aggiornare, quindi seleziona Edit (Modifica).

   b. Specifica uno dei valori seguenti per Viewer Protocol Policy (Policy protocollo visualizzatore):

      Reindirizza HTTP a HTTPS

      I visualizzatori possono utilizzare entrambi i protocolli, ma le richieste HTTP vengono automaticamente reindirizzate alle richieste HTTPS. CloudFront restituisce il codice di stato HTTP `301 (Moved Permanently)` con il nuovo URL HTTPS. Il visualizzatore invia quindi nuovamente la richiesta CloudFront utilizzando l'URL HTTPS.

      > **Important**
      >
      > CloudFront non reindirizza`DELETE`, `OPTIONS` `PATCHPOST`, o `PUT` le richieste da HTTP a HTTPS. Se configuri un comportamento della cache per il reindirizzamento a HTTPS, CloudFront risponde a HTTP,`DELETE`, `OPTIONS` `PATCHPOST`, o `PUT` alle richieste relative a tale comportamento della cache con il codice di stato HTTP. `403 (Forbidden)`

      Quando un visualizzatore effettua una richiesta HTTP che viene reindirizzata a una richiesta HTTPS, vengono CloudFront addebitati i costi per entrambe le richieste. Per la richiesta HTTP, l'addebito è solo per la richiesta e per le intestazioni che CloudFront

restituisce al visualizzatore. Per la richiesta HTTPS, l'addebito è per la richiesta, le intestazione e il file restituiti dal server di origine.

Solo HTTPS

I visualizzatori possono accedere ai contenuti solo se utilizzano connessioni HTTPS. Se un visualizzatore invia una richiesta HTTP anziché una richiesta HTTPS, CloudFront restituisce il codice di stato HTTP `403 (Forbidden)` e non restituisce il file.

c. Seleziona Yes, Edit (Sì, modifica).

d. Ripeti le fasi da "a" a "c" per ciascun comportamento cache aggiuntivo per il quale desideri richiedere una connessione HTTPS tra visualizzatori e CloudFront.

7. Conferma ciò che segue prima di utilizzare la configurazione aggiornata in un ambiente di produzione:

- Il modello di percorso in ciascun comportamento cache si applica solo alle richieste per le quali desideri che i visualizzatori utilizzino una connessione HTTPS.
- I comportamenti cache sono elencati nell'ordine in cui desideri vengano valutati da CloudFront. Per ulteriori informazioni, consulta Modello di percorso.
- I comportamenti cache sono richieste di routing ai server di origine corretti.

Determina la dimensione della chiave pubblica in un certificato SSL/TLS RSA

Quando utilizzi nomi di dominio CloudFront alternativi e HTTPS, la dimensione massima della chiave pubblica in un certificato SSL/TLS RSA è di 4096 bit. (Questa è la dimensione della chiave, non si riferisce al numero di caratteri nella chiave pubblica.) Se utilizzi AWS Certificate Manager per i tuoi certificati, sebbene ACM supporti chiavi RSA più grandi, non puoi utilizzare le chiavi più grandi con. CloudFront

Puoi stabilire le dimensioni della chiave pubblica RSA eseguendo il seguente comando OpenSSL:

```
openssl x509 -in path and filename of SSL/TLS certificate -text -noout
```

Dove:

- `-in`specifica il percorso e il nome del file del certificato RSA. SSL/TLS
- `-text` fa sì che OpenSSL visualizzi la lunghezza della chiave pubblica RSA in bit.

- `-noout` impedisce a OpenSSL di visualizzare la chiave pubblica.

Output di esempio:

```
Public-Key: (2048 bit)
```

Aumento delle quote per certificati SSL/TLS

Esistono quote sul numero di SSL/TLS certificati che è possibile importare in AWS Certificate Manager (ACM) o caricare su (IAM). AWS Identity and Access Management Esiste anche una quota sul numero di SSL/TLS certificati che è possibile utilizzare Account AWS quando si configura CloudFront per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati. Tuttavia, puoi richiedere quote più elevate.

Argomenti

Aumento della quota sui certificati importati in ACM

Per la quota relativa al numero di certificati che puoi importare in ACM, consulta Quote nella Guida per l'utente di AWS Certificate Manager .

Per richiedere una quota più elevata, utilizza la console Service Quotas. Per ulteriori informazioni, consulta Richiesta di un aumento delle quote nella Guida per l'utente di Service Quotas.

Aumento della quota sui certificati caricati su IAM

Per la quota (precedentemente nota come limite) sul numero di certificati che puoi caricare su IAM, consulta IAM e quote STS nella Guida per l'utente IAM.

Per richiedere una quota più elevata, utilizza la console Service Quotas. Per ulteriori informazioni, consulta Richiesta di un aumento delle quote nella Guida per l'utente di Service Quotas.

Aumento della quota sui certificati utilizzati con indirizzi IP dedicati

Per la quota relativa al numero di certificati SSL che puoi utilizzare per ciascuno di essi Account AWS quando gestisci richieste HTTPS utilizzando indirizzi IP dedicati, Quote sui certificati SSL consulta.

Per richiedere una quota più elevata, utilizza la console Service Quotas. Per ulteriori informazioni, consulta Richiesta di un aumento delle quote nella Guida per l'utente di Service Quotas.

Ruota SSL/TLS i certificati

Quando i SSL/TLS certificati sono prossimi alla scadenza, devi ruotarli per garantire la sicurezza della distribuzione ed evitare interruzioni del servizio per i tuoi spettatori. Puoi ruotarli nei modi seguenti:

- Per SSL/TLS i certificati forniti da AWS Certificate Manager (ACM), non è necessario ruotarli. ACM gestisce automaticamente i rinnovi dei certificati. Per ulteriori informazioni, consulta Rinnovo dei certificati gestiti nella Guida per l'utente di AWS Certificate Manager .
- Se si utilizza un'autorità di certificazione di terze parti e si sono importati i certificati in ACM (consigliato) o li si è caricati nell'archivio certificati IAM, è necessario sostituire occasionalmente un certificato con un altro.

> **Important**
>
> - ACM non gestisce i rinnovi di certificati acquisiti da autorità di certificazione di terze parti e importati in ACM.
> - Se sei configurato CloudFront per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati, potresti incorrere in un costo aggiuntivo proporzionale per l'utilizzo di uno o più certificati aggiuntivi durante la rotazione dei certificati. Ti consigliamo di aggiornare le distribuzioni per ridurre al minimo i costi aggiuntivi.

Ruota i certificati SSL/TLS

Per ruotare i certificati, esegui la procedura seguente. I visualizzatori possono continuare ad accedere ai tuoi contenuti mentre ruoti i certificati e una volta completato il processo.

Rotazione di certificati SSL/TLS

1. Aumento delle quote per certificati SSL/TLS per stabilire se hai bisogno dell'autorizzazione per utilizzare altri certificati SSL. In questo caso, richiedi l'autorizzazione e attendi fino a quando non l'hai ricevuta prima di continuare con la fase 2.

2. Importa il nuovo certificato in ACM o caricalo su IAM. Per ulteriori informazioni, consulta Importazione di un SSL/TLS certificato nella Amazon CloudFront Developer Guide.
3. (Solo per certificati IAM) Aggiorna le distribuzioni una alla volta per utilizzare il nuovo certificato. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
4. (Facoltativo) Elimina il certificato precedente da ACM o IAM.

> **Important**
>
> Non eliminare un SSL/TLS certificato finché non lo rimuovi da tutte le distribuzioni e finché lo stato delle distribuzioni che hai aggiornato non è cambiato. `Deployed`

Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront

Se hai configurato CloudFront l'uso di HTTPS tra i visualizzatori e CloudFront hai configurato CloudFront per utilizzare un SSL/TLS certificato personalizzato, puoi modificare la configurazione per utilizzare il certificato CloudFront SSL/TLS predefinito. Il processo dipende dal fatto se hai utilizzato la tua distribuzione per distribuire i tuoi contenuti:

- Se non hai utilizzato la tua distribuzione per distribuire i contenuti, puoi semplicemente modificare la configurazione. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
- Se hai utilizzato la tua distribuzione per distribuire i contenuti, devi creare una nuova CloudFront distribuzione e modificare i file URLs per ridurre o eliminare il periodo di indisponibilità dei contenuti. A questo scopo, esegui la procedura seguente.

Ripristina il certificato predefinito CloudFront

La procedura seguente mostra come tornare da un SSL/TLS certificato personalizzato al certificato predefinito CloudFront .

Per tornare al certificato predefinito CloudFront

1. Crea una nuova CloudFront distribuzione con la configurazione desiderata. Come Certificato SSL, seleziona Certificato CloudFront predefinito (*.cloudfront.net).

   Per ulteriori informazioni, consulta Creazione di una distribuzione.

2. Per i file che stai distribuendo utilizzando CloudFront, aggiorna l'applicazione URLs in modo da utilizzare il nome di dominio CloudFront assegnato alla nuova distribuzione. Ad esempio, modifica `https://www.example.com/images/logo.png` in `https://d111111abcdef8.cloudfront.net/images/logo.png`.
3. Elimina la distribuzione associata a un certificato SSL/TLS personalizzato o aggiorna la distribuzione per modificare il valore del certificato SSL in Certificato predefinito (*.cloudfront.net). CloudFront Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.

   > **Important**
   >
   > Finché non completerai questo passaggio, continuerai ad addebitarti i costi per l'utilizzo di un certificato personalizzato. AWS SSL/TLS

4. (Facoltativo) Elimina il SSL/TLS certificato personalizzato.

   a. Esegui il AWS CLI comando `list-server-certificates` per ottenere l'ID del certificato che desideri eliminare. Per ulteriori informazioni, consulta list-server-certificates nella documentazione di riferimento dei comandi della AWS CLI .

   b. Esegui il AWS CLI comando `delete-server-certificate` per eliminare il certificato. Per ulteriori informazioni, consulta delete-server-certificate nella documentazione di riferimento dei comandi della AWS CLI .

Passaggio da un certificato SSL/TLS personalizzato con indirizzi IP dedicati a SNI

Se hai configurato CloudFront per utilizzare un SSL/TLS certificato personalizzato con indirizzi IP dedicati, puoi invece passare all'utilizzo di un SSL/TLS certificato personalizzato con SNI ed eliminare i costi associati agli indirizzi IP dedicati.

> **Important**
>
> Questo aggiornamento della CloudFront configurazione non ha alcun effetto sui visualizzatori che supportano SNI. Gli utenti possono accedere ai contenuti prima e dopo la modifica, nonché durante la propagazione della modifica verso le sedi periferiche. CloudFront I visualizzatori che non supportano SNI non possono accedere ai contenuti dopo la modifica.

Per ulteriori informazioni, consulta Scegli in che modo CloudFront vengono servite le richieste HTTPS.

Passaggio da un certificato personalizzato a SNI

La procedura seguente mostra come passare da un SSL/TLS certificato personalizzato con indirizzi IP dedicati a SNI.

Per passare da un SSL/TLS certificato personalizzato con indirizzi IP dedicati a SNI

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona l'ID della distribuzione che desideri visualizzare o aggiornare.
3. Seleziona Distribution Settings (Impostazioni distribuzione).
4. Nella scheda General (Generale), seleziona Edit (Modifica).
5. In Certificazione SSL personalizzata – facoltativa, deseleziona Supporto per client legacy.
6. Seleziona Yes, Edit (Sì, modifica).

Visualizzatore TLS reciproco (mTLS)

L'autenticazione TLS reciproca (Mutual Transport Layer Security Authentication — MTLS) è un protocollo di sicurezza che estende l'autenticazione TLS standard richiedendo l'autenticazione bidirezionale basata su certificati, in cui sia il client che il server devono dimostrare la propria identità prima di stabilire una connessione sicura. Utilizzando Mutual TLS, puoi garantire che solo i client che presentano certificati TLS affidabili abbiano accesso alle tue distribuzioni. CloudFront

Come funziona

In un handshake TLS standard, solo il server presenta un certificato per dimostrare la propria identità al client. Con il TLS reciproco, il processo di autenticazione diventa bidirezionale. Quando un client tenta di connettersi alla tua CloudFront distribuzione, CloudFront richiede un certificato client durante l'handshake TLS. Il client deve presentare un certificato X.509 valido che sia CloudFront convalidato rispetto all'archivio di fiducia configurato prima di stabilire la connessione sicura.

CloudFront esegue la convalida del certificato presso le AWS edge location, alleggerendo la complessità dell'autenticazione dai server di origine e mantenendo CloudFront al contempo i vantaggi

in termini di prestazioni globali. È possibile configurare gli MTL in due modalità: modalità di verifica (che richiede a tutti i client di presentare certificati validi) o modalità opzionale (che convalida i certificati quando vengono presentati ma consente anche connessioni senza certificati).

Casi d'uso

L'autenticazione TLS reciproca CloudFront risolve diversi scenari di sicurezza critici in cui i metodi di autenticazione tradizionali sono insufficienti:

- Autenticazione dei dispositivi con memorizzazione nella cache dei contenuti: puoi autenticare console di gioco, dispositivi IoT o hardware aziendale prima di consentire l'accesso agli aggiornamenti del firmware, ai download di giochi o alle risorse interne. Ogni dispositivo contiene un certificato unico che ne dimostra l'autenticità sfruttando al contempo le funzionalità di memorizzazione nella cache. CloudFront
- API-to-API autenticazione: è possibile proteggere le machine-to-machine comunicazioni tra partner commerciali, sistemi di pagamento o microservizi affidabili. L'autenticazione basata su certificati elimina la necessità di chiavi API o segreti condivisi, fornendo al contempo una solida verifica dell'identità per gli scambi automatici di dati.

Argomenti

Archivi di fiducia e gestione dei certificati

La creazione e la configurazione di un trust store è un requisito obbligatorio per implementare l'autenticazione TLS reciproca con. CloudFront I trust store contengono i certificati Certificate Authority (CA) CloudFront utilizzati per convalidare i certificati client durante il processo di autenticazione.

Cos'è un trust store?

Un trust store è un archivio di certificati CA CloudFront utilizzato per convalidare i certificati client durante l'autenticazione TLS reciproca. Gli archivi di fiducia contengono i certificati CA root e intermedi che costituiscono la catena di fiducia per l'autenticazione dei certificati client.

Quando si implementa il TLS reciproco con CloudFront, il trust store definisce le autorità di certificazione attendibili per l'emissione di certificati client validi. CloudFront convalida ogni certificato client confrontandolo con il trust store durante l'handshake TLS. Solo i client che presentano certificati collegati a uno dei certificati presenti CAs nel tuo trust store verranno autenticati correttamente.

I trust store in CloudFront sono risorse a livello di account che puoi associare a più distribuzioni. Ciò consente di mantenere politiche di convalida dei certificati coerenti durante l'intera CloudFront distribuzione, semplificando al contempo la gestione dei certificati CA.

Supporto dell'Autorità di Certificazione

CloudFront supporta i certificati emessi da autorità di certificazione AWS private e autorità di certificazione private di terze parti. Questa flessibilità consente di utilizzare l'infrastruttura di certificazione esistente o di sfruttare i servizi di certificazione AWS gestiti in base ai requisiti organizzativi.

- AWS Autorità di certificazione privata: è possibile utilizzare i certificati emessi da AWS Private CA, che fornisce un servizio gestito di autorità di certificazione privata. Questa integrazione semplifica la gestione del ciclo di vita dei certificati e offre una perfetta integrazione con altri servizi. AWS
- Autorità di certificazione private di terze parti: puoi anche utilizzare i certificati della tua infrastruttura di autorità di certificazione privata esistente, inclusi fornitori di certificati aziendali CAs o di altri fornitori di certificati di terze parti. Ciò consente di mantenere gli attuali processi di gestione dei certificati aggiungendo CloudFront al contempo le funzionalità mTLS.

Requisiti e specifiche del certificato

I trust store hanno requisiti specifici per i certificati CA che contengono:

Requisiti di formato dei certificati CA

- Formato: formato PEM (Privacy Enhanced Mail)
- Limiti del contenuto: i certificati devono essere racchiusi entro i limiti -----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----

- Commenti: deve essere preceduto da un carattere # e non può contenere alcun carattere -
- Interruzioni di riga: non sono consentite righe vuote tra i certificati

Specifiche dei certificati supportate

- Tipo di certificato: X.509v3
- Tipi di chiavi pubbliche:
  - RSA 2048, RSA 4096
  - ECDSA: secp256r1
- Algoritmi di firma:
  - SHA256 SHA384, SHA512 con RSA
  - SHA256 SHA384, SHA512 con EC
  - SHA256 SHA384, SHA512 con RASSA-PSS con MGF1

Esempio di formato del pacchetto di certificati

Certificati multipli (con codifica PEM):

```
# Root CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqiMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
# Intermediate CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqjMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
```

Crea un trust store

Prima di creare un trust store, devi caricare il tuo pacchetto di certificati CA in formato PEM in un bucket Amazon S3. Il pacchetto di certificati deve contenere tutti i certificati CA root e intermedi affidabili necessari per convalidare i certificati client.

Il pacchetto di certificati CA viene letto solo una volta da S3 durante la creazione di un trust store. Se verranno apportate modifiche future al pacchetto di certificati CA, il trust store dovrà essere aggiornato manualmente. Non viene mantenuta alcuna sincronizzazione tra il trust store e il pacchetto di certificati CA S3.

Prerequisiti

- Un pacchetto di certificati della tua Certificate Authority (CA) caricato in un bucket Amazon S3
- Le autorizzazioni necessarie per creare risorse CloudFront

Per creare un trust store (Console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Trust stores.
3. Scegli Create Trust Store.
4. Per il nome del Trust Store, inserisci un nome per il tuo Trust Store.
5. Per il pacchetto Certificate Authority (CA), inserisci il percorso Amazon S3 del tuo pacchetto di certificati CA in formato PEM.
6. Scegli Create trust store.

Per creare un trust store (AWS CLI)

```
aws cloudfront create-trust-store \
  --name MyTrustStore \
  --certificate-authority-bundle-s3-location Bucket=my-bucket,Key=ca-bundle.pem \
  --tags Items=[{Key=Environment,Value=Production}]
```

Associa il trust store alle distribuzioni

Dopo aver creato un trust store, è necessario associarlo a una CloudFront distribuzione per abilitare l'autenticazione TLS reciproca.

Prerequisiti

- Una CloudFront distribuzione esistente con la politica del protocollo di visualizzazione solo HTTPS abilitata e HTTP3 il supporto disabilitato.

Per associare un trust store (Console)

Esistono due modi per associare un trust store all'interno della CloudFront console: tramite la pagina dei dettagli del trust store o tramite la pagina delle impostazioni di distribuzione.

Associare un trust store tramite la pagina dei dettagli del trust store:

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Trust stores.
3. Scegli il nome del trust store che desideri associare.
4. Scegli Associa alla distribuzione.
5. Configura le opzioni Viewer MTLs disponibili:
   - Modalità di convalida del certificato client: scegli tra la modalità obbligatoria e quella opzionale. Nella modalità richiesta, tutti i client devono presentare i certificati. In modalità opzionale, i client che presentano certificati vengono convalidati, mentre ai client che non presentano certificati è consentito l'accesso.
   - Pubblicizza i nomi delle CA del trust store: scegli se pubblicizzare i nomi delle CA nel tuo trust store ai clienti durante l'handshake TLS.
   - Ignora la data di scadenza del certificato: scegli se consentire le connessioni con certificati scaduti (valgono ancora altri criteri di convalida).
   - Funzione di connessione: una funzione di connessione opzionale può essere associata alle allow/deny connessioni basate su altri criteri personalizzati.
6. Seleziona una o più distribuzioni da associare al trust store. Solo le distribuzioni con comportamenti di cache HTTP3 disabilitati e con comportamento di cache basato solo su HTTPS possono supportare Viewer MTL.
7. Selezionare Associate (Associa).

Associazione di un trust store tramite la pagina delle impostazioni di distribuzione:

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Seleziona la distribuzione che desideri associare
3. Nella scheda Generale, all'interno del contenitore Impostazioni, scegli Modifica nell'angolo in alto a destra
4. Scorri verso il basso fino alla fine della pagina, all'interno del contenitore Connectivity, attiva l'opzione Viewer MTLs
5. Configura le opzioni Viewer MTLs disponibili:
   - Modalità di convalida del certificato client: scegli tra la modalità obbligatoria e quella opzionale. Nella modalità richiesta, tutti i client devono presentare i certificati. In modalità opzionale, i client che presentano certificati vengono convalidati, mentre ai client che non presentano certificati è consentito l'accesso.
   - Pubblicizza i nomi delle CA del trust store: scegli se pubblicizzare i nomi delle CA nel tuo trust store ai clienti durante l'handshake TLS.
   - Ignora la data di scadenza del certificato: scegli se consentire le connessioni con certificati scaduti (valgono ancora altri criteri di convalida).
   - Funzione di connessione: una funzione di connessione opzionale può essere associata alle allow/deny connessioni basate su altri criteri personalizzati.
6. Scegli Salva modifiche nell'angolo in basso a destra.

Per associare un trust store (AWS CLI)

I trust store possono essere associati alle distribuzioni tramite. DistributionConfig ViewerMtlsConfig proprietà. Ciò significa che dobbiamo prima recuperare la configurazione della distribuzione e poi fornirla ViewerMtlsConfig in una richiesta successiva UpdateDistribution .

```
// First fetch the distribution
aws cloudfront get-distribution {DISTRIBUTION_ID}

// Update the distribution config, for example:
Distribution config, file://distConf.json:
{
  ...other fields,
  ViewerMtlsConfig: {
    Mode: 'required',
    TrustStoreConfig: {
```

```
        AdvertiseTrustStoreCaNames: false,
        IgnoreCertificateExpiry: true,
        TrustStoreId: {TRUST_STORE_ID}
    }
  }
}

aws cloudfront update-distribution \
   --id {DISTRIBUTION_ID} \
   --if-match {ETAG} \
   --distribution-config file://distConf.json
```

Gestisci gli archivi di fiducia

Visualizza i dettagli del Trust Store

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Trust stores.
3. Scegli il nome del trust store per visualizzarne la pagina dei dettagli.

La pagina dei dettagli mostra:

- Nome e ID del Trust Store
- Numero di certificati CA
- Data di creazione e data dell'ultima modifica
- Distribuzioni associate
- Tag

Modificare un trust store

Per sostituire il pacchetto di certificati CA:

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Trust stores.
3. Scegli il nome del trust store.

4. Scegli Azioni, quindi Modifica.
5. Per il pacchetto Certificate Authority (CA), inserisci la posizione Amazon S3 del file PEM del pacchetto CA aggiornato.
6. Scegli Update trust store.

Elimina un trust store

Prerequisiti: è innanzitutto necessario dissociare il trust store da tutte le CloudFront distribuzioni.

1. Accedi a Console di gestione AWS e apri la console all' CloudFront indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Nel pannello di navigazione, scegli Trust stores.
3. Scegli il nome del trust store.
4. Scegli Elimina trust store.
5. Seleziona Elimina per confermare.

Fasi successive

Dopo aver creato e associato il tuo trust store a una CloudFront distribuzione, puoi procedere ad abilitare l'autenticazione TLS reciproca sulla tua distribuzione e configurare impostazioni aggiuntive come l'inoltro delle intestazioni dei certificati alle tue origini. Per istruzioni dettagliate sull'abilitazione degli MTL sulle distribuzioni, consulta. Abilita il TLS reciproco per le distribuzioni CloudFront

Abilita il TLS reciproco per le distribuzioni CloudFront

Prerequisiti e requisiti

CloudFrontla modalità di verifica TLS reciproca richiede che tutti i client presentino certificati validi durante l'handshake TLS e rifiuta le connessioni senza certificati validi. Prima di abilitare il TLS reciproco su una CloudFront distribuzione, assicurati di avere:

- Hai creato un trust store con i tuoi certificati di Certificate Authority
- Hai associato il trust store alla tua CloudFront distribuzione
- È stato garantito che tutti i comportamenti della cache di distribuzione utilizzino una politica del protocollo di visualizzazione solo HTTPS

- Assicurati che la tua distribuzione utilizzi HTTP/2 (l'impostazione predefinita, Viewer MTLs non è supportata su HTTP/3)

> **Note**
>
> L'autenticazione TLS reciproca richiede connessioni HTTPS tra i visualizzatori e. CloudFront Non è possibile abilitare MTL su una distribuzione con comportamenti di cache che supportano le connessioni HTTP.

Abilita il TLS reciproco (Console)

Per nuove distribuzioni

I Viewer MTL non possono essere configurati durante il processo di creazione di una nuova distribuzione nella CloudFront console. Innanzitutto crea la distribuzione con qualsiasi mezzo (console, CLI, API), quindi modifica le impostazioni di distribuzione per abilitare Viewer MTL secondo le istruzioni di distribuzione esistenti riportate di seguito.

Per le distribuzioni esistenti

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dalla lista di distribuzione, seleziona la distribuzione che desideri modificare.
3. Assicurati che la politica del protocollo Viewer sia impostata su Reindirizza HTTP su HTTPS o Solo HTTPS per tutti i comportamenti della cache. (Puoi scegliere la scheda Comportamenti della cache per visualizzare e aggiornare qualsiasi comportamento della cache con le politiche del protocollo HTTP).
4. Scegli la scheda Generale.
5. Nella sezione Settings (Impostazioni), scegli Edit (Modifica).
6. Nella sezione Connettività, trova Viewer Mutual Authentication (MTLs).
7. Attiva Abilita l'autenticazione reciproca.
8. Per la modalità di convalida del certificato client, seleziona Obbligatorio (tutti i client devono presentare certificati) o Facoltativo (i client possono facoltativamente presentare certificati).
9. Per Trust store, seleziona il trust store creato in precedenza.

10. (Facoltativo) Seleziona Pubblicizza i nomi CA del trust store se desideri CloudFront inviare i nomi CA ai client durante l'handshake TLS.
11. (Facoltativo) Attiva Ignora la data di scadenza del certificato se desideri consentire le connessioni con certificati scaduti.
12. Scegli Save changes (Salva modifiche).

Abilita TLS reciproco (AWS CLI)

Per nuove distribuzioni

L'esempio seguente mostra come creare un file di configurazione della distribuzione (distribution-config.json) che includa le impostazioni MTLS:

```
{
  "CallerReference": "cli-example-1",
  "Origins": {
    "Quantity": 1,
    "Items": [
      {
        "Id": "my-origin",
        "DomainName": "example.com",
        "CustomOriginConfig": {
          "HTTPPort": 80,
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        }
      }
    ]
  },
  "DefaultCacheBehavior": {
    "TargetOriginId": "my-origin",
    "ViewerProtocolPolicy": "https-only",
    "MinTTL": 0,
    "ForwardedValues": {
      "QueryString": false,
      "Cookies": {
        "Forward": "none"
      }
    }
  },
  "ViewerCertificate": {
```

```
    "CloudFrontDefaultCertificate": true
  },
  "ViewerMtlsConfig": {
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
  },
  "Enabled": true
}
```

Crea la distribuzione con MTL abilitati utilizzando il seguente comando di esempio:

```
aws cloudfront create-distribution --distribution-config file://distribution-
config.json
```

Per le distribuzioni esistenti

Ottieni la configurazione corrente della distribuzione utilizzando il seguente comando di esempio:

```
aws cloudfront get-distribution-config --id E1A2B3C4D5E6F7 --output json > dist-
config.json
```

Modifica il file per aggiungere le impostazioni mTLS. Aggiungete la seguente sezione di esempio alla configurazione della distribuzione:

```
"ViewerMtlsConfig": {
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
}
```

Rimuovi il ETag campo dal file ma salva il suo valore separatamente.

Aggiorna la distribuzione con la nuova configurazione usando il seguente comando di esempio:

```
aws cloudfront update-distribution \
```

```
    --id E1A2B3C4D5E6F7 \
    --if-match YOUR-ETAG-VALUE \
    --distribution-config file://dist-config.json
```

Politiche del protocollo Viewer

Quando si utilizza il protocollo TLS reciproco, tutti i comportamenti della cache di distribuzione devono essere configurati con una politica del protocollo di visualizzazione basata esclusivamente su HTTPS:

- Reindirizza da HTTP a HTTPS: reindirizza le richieste HTTP a HTTPS prima di eseguire la convalida del certificato.
- Solo HTTPS: accetta solo richieste HTTPS ed esegue la convalida dei certificati.

> **Note**
>
> La politica del protocollo di visualizzazione HTTP e HTTPS non è supportata con TLS reciproco poiché le connessioni HTTP non possono eseguire la convalida dei certificati.

Fasi successive

Dopo aver abilitato Viewer TLS sulla tua CloudFront distribuzione, puoi associare le funzioni di connessione per implementare una logica di convalida dei certificati personalizzata. Le funzioni di connessione consentono di estendere le funzionalità di autenticazione MTLS integrate con regole di convalida personalizzate, controllo della revoca dei certificati e registrazione. Per i dettagli sulla creazione e l'associazione delle funzioni di connessione, vedere. Associare una funzione di CloudFront connessione

Associare una funzione di CloudFront connessione

CloudFront Le funzioni di connessione consentono di implementare una logica di convalida dei certificati personalizzata durante gli handshake TLS, fornendo estensioni alle funzionalità di autenticazione MTLS integrate.

Cosa sono le funzioni di connessione?

Le funzioni di connessione sono JavaScript funzioni che vengono eseguite durante l'handshake TLS dopo la convalida dei certificati client. Il certificato client convalidato viene passato alla funzione di

connessione, a quel punto la funzione di connessione può determinare ulteriormente se concedere o meno l'accesso. Per informazioni dettagliate sulle funzioni di connessione, vedere[Personalizza a 360° con CloudFront Functions](#).

Come funzionano le funzioni di connessione con le MTL

Quando un client tenta di stabilire una connessione mTLS alla CloudFront distribuzione, si verifica la seguente sequenza:

1. Il client avvia l'handshake TLS con edge location. CloudFront
2. CloudFront richiede e riceve il certificato del cliente.
3. CloudFront esegue la convalida standard dei certificati rispetto al trust store.
4. Se il certificato supera la convalida standard, CloudFront richiama la funzione di connessione. Se IgnoreCertificateExpiryè abilitato all'interno del tuo ViewerMtlsConfig, anche i certificati scaduti, ma per il resto validi, vengono passati alla Funzione di connessione. Se i certificati client non sono validi, le funzioni di connessione non verranno richiamate.
5. La tua funzione di connessione riceve informazioni sui certificati e dettagli di connessione analizzati.
6. La tua funzione prende una allow/deny decisione in base a una logica personalizzata.
7. CloudFront completa o termina la connessione TLS in base alla tua decisione.

Le funzioni di connessione vengono richiamate sia per la modalità di verifica che per la modalità opzionale (quando i client presentano certificati).

Richiedi un aumento della quota della funzione di connessione

Richiedi un aumento della quota della Funzione di connessione per il tuo Account AWS.

Per richiedere un aumento della quota della funzione di connessione

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, seleziona Funzioni.
3. Scegli la scheda Funzioni di connessione
4. Per Richiesta, scegli il link per contattare l' CloudFront assistenza tecnica.
5. CloudFront support engineering esamina la tua richiesta. Il processo di revisione può richiedere fino a due giorni.

Dopo l'approvazione della richiesta, puoi creare una funzione di connessione nel tuo account e associarla a una o più distribuzioni utilizzando il TLS reciproco.

Crea una funzione di connessione

È possibile creare funzioni di connessione utilizzando la CloudFront console o la AWS CLI.

Per creare una funzione di connessione (console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, seleziona Funzioni.
3. Scegli la scheda Funzioni di connessione e scegli Crea funzione di connessione.
4. Inserisci un nome di funzione univoco all'interno del tuo AWS account.
5. Scegli Continua.
6. Nell'editor delle funzioni, scrivi il JavaScript codice per la convalida del certificato. Il gestore della funzione deve chiamare allow o deny.
7. Facoltativo: è possibile associare un KeyValue archivio alla funzione di connessione per implementare il controllo delle revoce.
8. Scegli Save changes (Salva modifiche).

Per creare una funzione di connessione (AWS CLI)

L'esempio seguente mostra come creare una funzione di connessione:

Scrivi il codice della funzione in un file separato, ad esempio code.js:

```
function connectionHandler(connection) {
  connection.allow();
}
```

```
aws cloudfront create-connection-function \
  --name "certificate-validator" \
  --connection-function-config '{
      "Comment": "Client certificate validation function",
      "Runtime": "cloudfront-js-2.0"
  }' \
```

```
  --connection-function-code fileb://code.js
```

Struttura del codice della funzione di connessione

Le funzioni di connessione implementano la funzione ConnectionHandler che riceve un oggetto di connessione contenente il certificato e le informazioni di connessione. La funzione deve utilizzare una delle due `connection.allow()` opzioni o `connection.deny()` per prendere una decisione sulla connessione.

Esempio di funzione di connessione di base

L'esempio seguente mostra una semplice funzione di connessione che verifica il campo dell'oggetto dei certificati client:

```
function connectionHandler(connection) {
    // Only process if a certificate was presented
    if (!connection.clientCertificate) {
        console.log("No certificate presented");
        connection.deny();
    }

    // Check the subject field for specific organization
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("O=ExampleCorp")) {
        console.log("Certificate not from authorized organization");
       connection.deny();
    } else {
        // All checks passed
        console.log("Certificate validation passed");
        connection.allow();
    }
}
```

La specifica completa delle proprietà dei certificati client disponibili sull'oggetto di connessione è disponibile qui:

```
{
  "connectionId": "Fdb-Eb7L9gVn2cFakz7wWyBJIDAD4-oNO6g8r3vXDV132BtnIVtqDA==", // Unique
 identifier for this TLS connection
  "clientIp": "203.0.113.42", // IP address of the connecting client (IPv4 or IPv6)
  "clientCertificate": {
```

```
    "certificates": {
      "leaf": {
        "subject": "CN=client.example.com,O=Example Corp,C=US", // Distinguished Name
 (DN) of the certificate holder
        "issuer": "CN=Example Corp Intermediate CA,O=Example Corp,C=US", //
 Distinguished Name (DN) of the certificate authority that issued this certificate
        "serialNumber": "4a:3f:5c:92:d1:e8:7b:6c", // Unique serial number assigned by
 the issuing CA (hexadecimal)
        "validity": {
          "notBefore": "2024-01-15T00:00:00Z", // Certificate validity start date (ISO
 8601 format)
          "notAfter": "2025-01-14T23:59:59Z"   // Certificate expiration date (ISO 8601
 format)
        },
        "sha256Fingerprint": "a1b2c3d4e5f6...abc123def456", // SHA-256 hash of the
 certificate (64 hex characters)
      },
    },
  },
}
```

Associa una funzione di connessione

Dopo aver creato la funzione di connessione, è necessario pubblicarla nella fase LIVE e associarla alla distribuzione.

Per pubblicare e associare una funzione di connessione (console)

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Funzioni
3. Scegli la scheda Funzioni di connessione e seleziona la tua funzione di connessione.
4. Scegli Pubblica per spostarlo nella fase LIVE.
5. Scegli Aggiungi associazione nella tabella delle distribuzioni associate sotto la sezione di pubblicazione.
6. Seleziona la distribuzione con Viewer MTLs abilitato che desideri associare.

In alternativa, è possibile associare le funzioni di connessione pubblicate anche dalla pagina dei dettagli della distribuzione.

1. Vai alla home page della console dove sono elencate tutte le tue distribuzioni.
2. Seleziona la distribuzione che desideri associare.
3. Scegli la scheda Generale.
4. Nella sezione Settings (Impostazioni), scegli Edit (Modifica).
5. Nella sezione Connettività, trova Viewer Mutual Authentication (MTLs).
6. Per Funzione di connessione, seleziona la tua funzione.
7. Scegli Save changes (Salva modifiche).

Per associare una funzione di connessione (AWS CLI)

L'esempio seguente mostra come associare una funzione di connessione a una distribuzione:

```
// DistributionConfig:
{
   ...other settings,
    "ConnectionFunctionAssociation": {
        "Id": "cf_30c2CV2elHwCoInb3LtcaUJkZeD"
    }
}
```

Casi d'uso per le funzioni di connessione

Le funzioni di connessione consentono diversi casi d'uso avanzati di MTL:

- Convalida degli attributi del certificato: verifica campi specifici nei certificati client, come i requisiti delle unità organizzative o i modelli di denominazione alternativi dei soggetti.
- Controllo della revoca dei certificati: implementa il controllo personalizzato della revoca dei certificati utilizzando KeyValueStore per archiviare i numeri di serie dei certificati revocati.
- Politiche di certificazione basate su IP: applica politiche di certificazione diverse in base agli indirizzi IP dei client o alle restrizioni geografiche.
- Convalida multi-tenant: implementa regole di convalida specifiche del tenant in cui si applicano requisiti di certificato diversi in base ai nomi host o agli attributi del certificato.

> **Note**
>
> Le funzioni di connessione vengono eseguite una volta per connessione client durante l'handshake TLS.
> Le funzioni di connessione possono solo consentire o negare le connessioni, non modificare le richieste/risposte HTTP.
> Solo le funzioni LIVE stage (pubblicate) possono essere associate alle distribuzioni.
> Ogni distribuzione può avere al massimo una funzione di connessione.

Fasi successive

Dopo aver associato una funzione di connessione alla CloudFront distribuzione, è possibile configurare impostazioni opzionali per personalizzare il comportamento dell'implementazione di MTLS. Per istruzioni dettagliate sulla configurazione di impostazioni aggiuntive come una modalità opzionale di convalida del certificato client, consulta. Configurazione di impostazioni aggiuntive

Configurazione di impostazioni aggiuntive

Dopo aver abilitato l'autenticazione TLS reciproca di base, è possibile configurare impostazioni aggiuntive per personalizzare il comportamento di autenticazione per casi d'uso e requisiti specifici.

Convalida del certificato client (modalità opzionale)

CloudFront offre una modalità alternativa di convalida dei certificati client opzionale che convalida i certificati client presentati ma consente l'accesso ai client che non presentano certificati.

Comportamento in modalità opzionale

- Concede la connessione ai client con certificati validi (i certificati non validi vengono negati).
- Consente la connessione a client senza certificati
- Consente scenari di autenticazione client misti tramite un'unica distribuzione.

La modalità opzionale è ideale per la migrazione graduale all'autenticazione MTLS, per supportare client con certificati e client senza certificati o per mantenere la retrocompatibilità con i client legacy.

> **Note**
>
> In modalità opzionale, le funzioni di connessione vengono ancora richiamate anche quando i client non presentano certificati. Ciò consente di implementare una logica personalizzata come la registrazione degli indirizzi IP dei client o l'applicazione di politiche diverse in base alla presentazione dei certificati.

Per configurare la modalità opzionale (console)

1. Nelle impostazioni di distribuzione, vai alla scheda Generale, scegli Modifica.
2. Scorri fino alla sezione Viewer Mutual Authentication (mTLS) all'interno del contenitore Connectivity.
3. Per la modalità di convalida del certificato Client, seleziona Opzionale.
4. Salva le modifiche.

Per configurare la modalità opzionale (AWS CLI)

L'esempio seguente mostra come configurare la modalità opzionale:

```
"ViewerMtlsConfig": {
   "Mode": "optional",
   ...other settings
}
```

Pubblicità dell'Autorità di Certificazione

Il AdvertiseTrustStoreCaNames campo controlla se CloudFront inviare l'elenco di nomi CA affidabili ai client durante l'handshake TLS, aiutandoli a selezionare il certificato appropriato.

Per configurare CA advertising (Console)

1. Nelle impostazioni di distribuzione, vai alla scheda Generale, scegli Modifica.
2. Scorri fino alla sezione Viewer Mutual Authentication (mTLS) all'interno del contenitore Connectivity.
3. Seleziona o deseleziona la casella di controllo Advertise trust store CA names.

4. Scegli Save changes (Salva modifiche).

Per configurare la pubblicità CA (AWS CLI)

L'esempio seguente mostra come abilitare la pubblicità CA:

```
"ViewerMtlsConfig": {
   "Mode": "required", // or "optional"
   "TrustStoreConfig": {
      "AdvertiseTrustStoreCaNames": true,
      ...other settings
   }
}
```

Gestione della scadenza dei certificati

La IgnoreCertificateExpiry proprietà determina la modalità di CloudFront risposta ai certificati client scaduti. Per impostazione predefinita, CloudFront rifiuta i certificati client scaduti, ma è possibile configurarlo per accettarli quando necessario. In genere è abilitato per i dispositivi con certificati scaduti che non possono essere aggiornati prontamente.

Per configurare la gestione della scadenza dei certificati (Console)

1. Nelle impostazioni di distribuzione, vai alla scheda Generale, scegli Modifica.
2. Scorri fino alla sezione Viewer Mutual Authentication (mTLS) del contenitore Connectivity.
3. Seleziona o deseleziona la casella di controllo Ignora la data di scadenza del certificato.
4. Scegli Save changes (Salva modifiche).

Per configurare la gestione della scadenza dei certificati (AWS CLI)

L'esempio seguente mostra come ignorare la scadenza dei certificati:

```
"ViewerMtlsConfig": {
  "Mode": "required", // or "optional"
  "TrustStoreConfig": {
     "IgnoreCertificateExpiry": false,
     ...other settings
  }
}
```

> **Note**
>
> IgnoreCertificateExpirysi applica solo alle date di validità dei certificati. Tutti gli altri controlli di convalida dei certificati sono ancora validi (catena di fiducia, convalida della firma).

Fasi successive

Dopo aver configurato impostazioni aggiuntive, è possibile configurare l'inoltro delle intestazioni per trasmettere le informazioni del certificato alle origini, implementare la revoca dei certificati utilizzando Connection Functions e KeyValueStore abilitare i log di connessione per il monitoraggio. Per i dettagli sull'inoltro delle informazioni sui certificati alle origini, consulta Forward Headers to origin.

Visualizza le intestazioni MTLS per le politiche della cache e le inoltrate all'origine

Quando si utilizza l'autenticazione TLS reciproca, CloudFront è possibile estrarre informazioni dai certificati client e inoltrarle alle origini come intestazioni HTTP. Ciò consente ai server di origine di accedere ai dettagli dei certificati senza implementare la logica di convalida dei certificati.

Le seguenti intestazioni sono disponibili per la creazione di comportamenti di cache:

Nome intestazione	Description	Valore di esempio
CloudFront-Viewer-Cert-Serial-Number	Rappresentazione esadecimale del numero di serie del certificato	4a:3f:5c:92:d1:e 8:7b:6c
CloudFront-Viewer-Cert-Emittente	RFC2253 rappresentazione in formato stringa del nome distinto (DN) dell'emittente	CN=rootcamtls.com, OU=RootCA, o=MTLS, L=Seattle, ST=Washington, C=USA
CloudFront-Viewer-Cert-Subject	RFC2253 rappresentazione in formato stringa del nome distinto (DN) del soggetto	CN=client_.com, OU=Client-3, o=MTLS, ST=Washington, C=US

Nome intestazione	Description	Valore di esempio
CloudFront-Viewer-Cert-Present	1 (presente) o 0 (non presente) indica se il certificato è presente. Questo valore è sempre 1 in modalità Obbligatoria.	1
CloudFront-Viewer-Cert-Sha256	L'hash del certificato client SHA256	01fbf94fef5569753420c349f49adbfd80af5275377816e3ab1fb371b29cb586

Per le richieste di origine, vengono fornite due intestazioni aggiuntive, oltre alle intestazioni sopra riportate rese disponibili per i comportamenti della cache:

Nome intestazione	Description	Valore di esempio
CloudFront-Viewer-Cert-Validity	ISO86Formato 01 della data NotBefore e NotAfter	CloudFront-Viewer-Cert-Validità: =2023-09-21T 01:50:17 Z; =2024-09-20T 01:50:17 Z NotBefore NotAfter
CloudFront-Viewer-Cert-Pem	Formato PEM con codifica URL del certificato leaf	CloudFront-Viewer-Cert-Pem: -----BEGIN%20CERTIFICATE-----%0AMIIG<... ridotto... -Viewer-Cert-Pem: -----INIZIO%20CERTIFICATO-----%0AMIIG %0A-----FINE NmrUlw CERTIFICATO-----%0A

Configura l'inoltro degli header

Console

In modalità di verifica, aggiunge CloudFront automaticamente le intestazioni CloudFront-Viewer-Cert-* a tutte le richieste dei visualizzatori. Per inoltrare queste intestazioni alla tua origine:

1. Dalla pagina principale delle distribuzioni dell'elenco, seleziona la tua distribuzione con i viewer MTL abilitati e vai alla scheda Comportamenti
2. Seleziona il comportamento della cache e scegli Modifica
3. Nella sezione Politica di richiesta Origin, scegli Crea policy o seleziona una policy esistente
4. Assicurati che le seguenti intestazioni siano incluse nella politica di richiesta di origine:
   - CloudFront-Viewer-Cert-Serial-Number
   - CloudFront-Viewer-Cert-Issuer
   - CloudFront-Viewer-Cert-Subject
   - CloudFront-Viewer-Cert-Present
   - Cloudfront-Viewer-Cert-Sha256
   - CloudFront-Viewer-Cert-Validity
   - CloudFront-Visualizzatore-Cert-Pem
5. Scegli Crea (per nuove politiche) o Salva modifiche (per le politiche esistenti)
6. Seleziona la politica all'interno del comportamento della cache e salva le modifiche

Utilizzo della AWS CLI

L'esempio seguente mostra come creare una policy di richiesta di origine che includa le intestazioni MTL per la modalità di verifica:

```
aws cloudfront create-origin-request-policy \
  --origin-request-policy-config '{
    "Name": "MTLSHeadersPolicy",
    "HeadersConfig": {
      "HeaderBehavior": "whitelist",
      "Headers": {
        "Quantity": 5,
        "Items": [
          "CloudFront-Viewer-Cert-Serial-Number",
          "CloudFront-Viewer-Cert-Issuer",
          "CloudFront-Viewer-Cert-Subject",
          "CloudFront-Viewer-Cert-Validity",
          "CloudFront-Viewer-Cert-Pem"
        ]
      }
    },
    "CookiesConfig": {
```

```
      "CookieBehavior": "none"
    },
    "QueryStringsConfig": {
      "QueryStringBehavior": "none"
    }
  }'
```

Considerazioni sull'elaborazione delle intestazioni

Quando lavori con le intestazioni dei certificati, prendi in considerazione queste best practice:

- Convalida dell'intestazione: verifica i valori dell'intestazione del certificato all'origine come misura di sicurezza aggiuntiva
- Limiti di dimensione delle intestazioni: le intestazioni dei certificati PEM possono essere grandi, assicuratevi che il server di origine sia in grado di gestirle
- Considerazioni sulla cache: l'utilizzo delle intestazioni dei certificati nella chiave della cache aumenta la frammentazione della cache
- Richieste provenienti da più origini: se l'applicazione utilizza CORS, potrebbe essere necessario configurarla per consentire le intestazioni dei certificati

Fasi successive

Dopo aver configurato l'inoltro delle intestazioni, è possibile implementare il controllo della revoca dei certificati utilizzando Connection Functions e. CloudFront KeyValueStore Per i dettagli sull'implementazione dei controlli di revoca, vedere. Revoca tramite CloudFront Connection Function e KVS

Revoca tramite CloudFront Connection Function e KVS

È possibile implementare il controllo della revoca dei certificati per l'autenticazione TLS reciproca combinando CloudFront Connection Functions con. KeyValueStore Questo approccio fornisce un meccanismo di revoca dei certificati scalabile e in tempo reale che integra CloudFront la convalida dei certificati integrata.

Le funzioni di connessione sono JavaScript funzioni che vengono eseguite durante la creazione della connessione TLS nelle sedi CloudFront periferiche e consentono di implementare una logica di convalida dei certificati personalizzata per l'autenticazione MTLS. Per informazioni dettagliate sulle funzioni di connessione, vedere. Associare una funzione di CloudFront connessione

Come funziona la revoca dei certificati con Connection Functions

CloudFrontla convalida standard dei certificati verifica la catena, la firma e la scadenza del certificato, ma non include il controllo integrato della revoca del certificato. Utilizzando Connection Functions, è possibile implementare un controllo di revoca personalizzato durante l'handshake TLS.

Il processo di revoca del certificato funziona come segue:

1. Memorizza i numeri di serie dei certificati revocati in un. CloudFront KeyValueStore
2. Quando un client presenta un certificato, viene richiamata la funzione di connessione.
3. La funzione confronta il numero di serie del certificato con il KeyValueStore.
4. Se il numero di serie viene trovato nell'archivio, il certificato viene revocato.
5. La tua funzione nega la connessione per i certificati revocati.

Questo approccio fornisce il controllo near-real-time delle revoche attraverso la rete CloudFront perimetrale globale.

Configurazione KeyValueStore per i certificati revocati

Innanzitutto, crea un file KeyValueStore per memorizzare i numeri di serie dei certificati revocati:

Per creare una KeyValueStore (Console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Key value stores.
3. Scegli Crea archivio di valori chiave.
4. Inserisci un nome per il tuo archivio di valori chiave (ad esempio, certificati revocati).
5. (Facoltativo) Aggiungi una descrizione.
6. Scegli Crea archivio di valori chiave.

Per creare una KeyValueStore (AWS CLI)

L'esempio seguente mostra come creare un KeyValueStore:

```
aws cloudfront create-key-value-store \
```

```
  --name "revoked-certificates" \
  --comment "Store for revoked certificate serial numbers"
```

Importa i numeri di serie dei certificati revocati

Dopo aver creato un KeyValueStore, devi importare i numeri di serie dei certificati revocati:

Preparare i dati di revoca

Crea un file JSON con i numeri di serie del certificato revocato:

```
{
  "data": [
    {
      "key": "ABC123DEF456",
      "value": ""
    },
    {
      "key": "789XYZ012GHI",
      "value": ""
    }
  ]
}
```

Importazione da S3

1. Carica il file JSON in un bucket S3
2. Importa il file su: KeyValueStore

```
aws cloudfront create-key-value-store \
  --name "revoked-certificates" \
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::amzn-s3-demo-bucket1/revoked-serials.json"
  }'
```

Crea una funzione di connessione per il controllo delle revoce

Crea una funzione di connessione che confronti i numeri di serie dei certificati con i tuoi KeyValueStore:

Esempio di codice della funzione di connessione

L'esempio seguente mostra una funzione di connessione che esegue il controllo della revoca dei certificati:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get client certificate serial number
    const clientSerialNumber =
 connection.clientCertificate.certificates.leaf.serialNumber;

    // Check if the serial number exists in the KeyValueStore
    const isRevoked = await kvsHandle.exists(clientSerialNumber.replaceAll(':', ''));

    if (isRevoked) {
        console.log(`Certificate ${clientSerialNumber} is revoked. Denying
 connection.`);
        connection.logCustomData(`REVOKED:${clientSerialNumber}`);
        connection.deny();
    } else {
        console.log(`Certificate ${clientSerialNumber} is valid. Allowing
 connection.`);
        connection.allow();
    }

}
```

Per creare la funzione di connessione (AWS CLI)

L'esempio seguente mostra come creare una funzione di connessione con KeyValueStore associazione:

```
aws cloudfront create-connection-function \
  --name "revocation-checker" \
  --connection-function-config '{
      "Comment": "Certificate revocation checking function",
      "Runtime": "cloudfront-js-2.0",
```

```
      "KeyValueStoreAssociations": {
          "Quantity": 1,
          "Items": [
              {
                  "KeyValueStoreARN": "arn:aws:cloudfront::123456789012:key-value-
store/revoked-certificates"
              }
          ]
      }
  }' \
  --connection-function-code fileb://revocation-checker.js
```

Associate la funzione alla vostra distribuzione

Dopo aver creato e pubblicato la tua Connection Function, associala alla tua CloudFront distribuzione abilitata per MTLS come descritto nella sezione. Associare una funzione di CloudFront connessione

Osservabilità utilizzando i log di connessione

CloudFront i registri di connessione forniscono una visibilità dettagliata degli eventi di autenticazione TLS reciproca, consentendo di monitorare la convalida dei certificati, tenere traccia dei tentativi di connessione e risolvere i problemi di autenticazione.

Cosa sono i log di connessione?

I log di connessione raccolgono informazioni dettagliate sugli handshake TLS e sulla convalida dei certificati per le distribuzioni reciproche abilitate per TLS. A differenza dei log di accesso standard che registrano le informazioni sulle richieste HTTP, i log di connessione si concentrano specificamente sulla fase di creazione della connessione TLS, tra cui:

- Stato della connessione (successo/errore)
- Dettagli del certificato del cliente
- Informazioni sul protocollo TLS e sulla cifratura
- Metriche sulla tempistica della connessione
- Dati personalizzati da Connection Functions

Questi registri offrono una visibilità completa sugli eventi di autenticazione basati su certificati, aiutandovi a monitorare la sicurezza, risolvere i problemi e soddisfare i requisiti di conformità.

Abilita i registri di connessione

I log di connessione sono disponibili solo per le distribuzioni con l'autenticazione TLS reciproca abilitata. Puoi inviare i log di connessione a più destinazioni, tra cui CloudWatch Logs, Amazon Data Firehose e Amazon S3.

Prerequisiti

Prima di abilitare i log di connessione:

- Configura il TLS reciproco per la tua distribuzione CloudFront
- Abilita i log di connessione per la tua distribuzione CloudFront
- Assicurati di disporre delle autorizzazioni necessarie per la destinazione di registrazione scelta
- Per la distribuzione tra più account, configura le politiche IAM appropriate

Per abilitare i registri di connessione (Console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dalla lista di distribuzione, seleziona la tua distribuzione abilitata per MTLS.
3. Scegli la scheda Logging (Utilizzo log).
4. Scegliere Aggiungi.
5. Seleziona il servizio per ricevere i log:
   - CloudWatch Log
   - Firehose
   - Amazon S3
6. Per Destinazione, seleziona la risorsa per il servizio scelto:
   - Per CloudWatch Log, inserisci il nome del gruppo di log
   - Per Firehose, selezionare lo stream di distribuzione Firehose
   - Per Amazon S3, inserisci il nome del bucket (facoltativamente con un prefisso)
7. (Facoltativo) Configura le impostazioni aggiuntive:
   - Selezione dei campi: seleziona campi di registro specifici da includere.
   - Formato di output: scegli tra JSON, Plain, w3c, Raw o Parquet (solo S3).

- Delimitatore di campo: specifica come separare i campi del registro.

8. Scegliere Salva modifiche.

Per abilitare i log di connessione (AWS CLI)

L'esempio seguente mostra come abilitare i log di connessione utilizzando l'API: CloudWatch

```
# Step 1: Create a delivery source
aws logs put-delivery-source \
  --name "cf-mtls-connection-logs" \
  --resource-arn "arn:aws:cloudfront::123456789012:distribution/E1A2B3C4D5E6F7" \
  --log-type CONNECTION_LOGS

# Step 2: Create a delivery destination
aws logs put-delivery-destination \
  --name "s3-destination" \
  --delivery-destination-configuration \
  "destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket1"

# Step 3: Create the delivery
aws logs create-delivery \
  --delivery-source-name "cf-mtls-connection-logs" \
  --delivery-destination-arn "arn:aws:logs:us-east-1:123456789012:delivery-
destination:s3-destination"
```

> **Note**
>
> Quando si utilizza l' CloudWatch API, è necessario specificare la regione Stati Uniti orientali (Virginia settentrionale) (us-east-1) anche quando si consegnano i log in altre regioni.

Campi del registro delle connessioni

I registri di connessione includono informazioni dettagliate su ogni tentativo di connessione TLS:

Campo	Description	Esempio
`eventTimestamp`	Timestamp ISO 8601 quando la connessione è stata stabilita o non è riuscita	1731620046814
`connectionId`	Identificatore univoco per la connessione TLS	`oLHiEKbQSn8lkvJfA3D4gFowK3_iZ0g4i5nMUjE1Akod8TuAzn5nzg==`
`connectionStatus`	Lo stato del tentativo di connessione mTLS.	`Success` o `Failed`
`clientIp`	Indirizzo IP del client di connessione	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
`clientPort`	Porta utilizzata dal client	12137
`serverIp`	Indirizzo IP del server CloudFront perimetrale	`99.84.71.136`
`distributionId`	CloudFront ID di distribuzione	`E2DX1SLDPK0123`
`distributionTenantId`	CloudFront ID del tenant di distribuzione (se applicabile)	`dt_2te1Ura9X3R2iCGNjW123`
`tlsProtocol`	versione del protocollo TLS utilizzata	`TLSv1.3`
`tlsCipher`	Suite di crittografia TLS utilizzata per la connessione	`TLS_AES_128_GCM_SHA256`
`tlsHandshakeDuration`	Durata dell'handshake TLS in millisecondi	153
`tlsSni`	Valore di indicazione del nome del server ricavato dall'handshake TLS	`d111111abcdef8.cloudfront.net`

Campo	Description	Esempio
`clientLeafCertSerialNumber`	Numero di serie del certificato del client	`00:b1:43:ed:93:d2:d8:f3:9d`
`clientLeafCertSubject`	Campo relativo all'oggetto del certificato del cliente	`C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=client.test.mtls.net`
`clientLeafCertIssuer`	Campo dell'emittente del certificato del cliente	`C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=test.mtls.net`
`clientLeafCertValidity`	Periodo di validità del certificato del cliente	`NotBefore=2025-06-05T23:28:21Z;NotAfter=2125-05-12T23:28:21Z`
`connectionLogCustomData`	Dati personalizzati aggiunti tramite Connection Functions	`REVOKED:00:b1:43:ed:93:d2:d8:f3:9d`

Codici di errore di connessione

```
Failed:ClientCertMaxChainDepthExceeded
Failed:ClientCertMaxSizeExceeded
Failed:ClientCertUntrusted
Failed:ClientCertNotYetValid
Failed:ClientCertExpired
Failed:ClientCertTypeUnsupported
Failed:ClientCertInvalid
Failed:ClientCertIntentInvalid
Failed:ClientCertRejected
Failed:ClientCertMissing
Failed:TcpError
Failed:TcpTimeout
Failed:ConnectionFunctionError
Failed:ConnectionFunctionDenied
```

```
Failed:Internal
Failed:UnmappedConnectionError
```

Quando le connessioni falliscono, CloudFront registra codici di motivo specifici:

Codice	Description
ClientCertMaxChain DepthExceeded	È stata superata la profondità massima della catena di certificati
ClientCertMaxSizeExceeded	Dimensione massima del certificato superata
ClientCertUntrusted	Il certificato non è attendibile
ClientCertNotYetValid	Il certificato non è ancora valido
ClientCertExpired	Il certificato è scaduto
ClientCertTypeUnsupported	Il tipo di certificato non è supportato
ClientCertInvalid	Il certificato non è valido
ClientCertIntentInvalid	L'intento del certificato non è valido
ClientCertRejected	Certificato rifiutato mediante convalida personalizzata
ClientCertMissing	Manca il certificato
TcpError	Si è verificato un errore durante il tentativo di stabilire una connessione
TcpTimeout	Non è stato possibile stabilire la connessione entro il periodo di timeout
ConnectionFunctionError	È stata generata un'eccezione non rilevata durante l'esecuzione della funzione di connessione
Interno	Si è verificato un errore interno del servizio
UnmappedConnectionError	Si è verificato un errore che non rientra in nessuna delle altre categorie

Offri contenuti privati con cookie firmati URLs e firmati

Molte aziende che distribuiscono contenuto tramite Internet vogliono limitare l'accesso a documenti, dati aziendali, flussi multimediali o contenuto destinato a utenti selezionati, ad esempio, utenti paganti. Per servire in modo sicuro questi contenuti privati utilizzando CloudFront, puoi fare quanto segue:

- Richiedi che gli utenti accedano ai tuoi contenuti privati utilizzando speciali cookie CloudFront firmati URLs o firmati.
- Richiedi che i tuoi utenti accedano ai tuoi contenuti utilizzando CloudFront URLs, non URLs che accedano ai contenuti direttamente sul server di origine (ad esempio, Amazon S3 o un server HTTP privato). La richiesta CloudFront URLs non è necessaria, ma la consigliamo per impedire agli utenti di aggirare le restrizioni specificate nei cookie firmati URLs o firmati.

Per ulteriori informazioni, consulta Limitazione dell'accesso ai file.

Come gestire contenuti privati

CloudFront Per configurare la visualizzazione di contenuti privati, esegui le seguenti operazioni:

1. (Facoltativo ma consigliato) Richiedi agli utenti di accedere ai tuoi contenuti solo tramite CloudFront. Il metodo utilizzato varia a seconda se utilizzi origini Amazon S3 o origini personalizzate:

   - Amazon S3 - Vedere the section called "Limitazione dell'accesso a un'origine Amazon S3".
   - Origine personalizzata - Consulta Limitazione dell'accesso ai file su origini personalizzate.

   Le origini personalizzate includono Amazon EC2, i bucket Amazon S3 configurati come endpoint di siti Web, ELB e i tuoi server Web HTTP.
2. Specificate i gruppi di chiavi attendibili o i firmatari fidati che desiderate utilizzare per creare cookie firmati o firmati. URLs Ti consigliamo di utilizzare gruppi di chiavi attendibili. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .
3. Scrivi la tua applicazione per rispondere alle richieste degli utenti autorizzati con cookie firmati URLs o con `Set-Cookie` intestazioni che impostano cookie firmati. Segui le fasi in uno dei seguenti argomenti:

   - Usa firmato URLs

- Utilizzo di cookie firmati

Se non si è certi del metodo da utilizzare, consultare Decidi di utilizzare cookie firmati URLs o firmati.

Argomenti

Limitazione dell'accesso ai file

Puoi controllare l'accesso degli utenti ai tuoi contenuti privati in due modi:

- Limita l'accesso ai file nelle CloudFront cache.
- Limita l'accesso ai file nel server di origine in uno dei seguenti modi:
  - Imposta un controllo di accesso origine (OAC) per il bucket Amazon S3.
  - Configura intestazioni personalizzate per un server HTTP privato (un'origine personalizzata).

Limita l'accesso ai file nelle cache CloudFront

Puoi configurare in modo CloudFront da richiedere che gli utenti accedano ai tuoi file utilizzando cookie firmati URLs o firmati. Successivamente, sviluppate l'applicazione per creare e distribuire i cookie firmati URLs agli utenti autenticati o per inviare `Set-Cookie` intestazioni che impostano cookie firmati per gli utenti autenticati. (Per consentire ad alcuni utenti l'accesso a lungo termine a un numero limitato di file, puoi anche creare file firmati URLs manualmente.)

Quando crei cookie firmati URLs o firmati per controllare l'accesso ai tuoi file, puoi specificare le seguenti restrizioni:

- Una data e un'ora di fine, dopo le quali l'URL non è più valido.
- (Facoltativo) La data e l'ora in cui l'URL diventa valido.
- (Facoltativo) L'indirizzo IP o l'intervallo di indirizzi dei computer che possono essere utilizzati per accedere al tuo contenuto.

Una parte di un URL o di un cookie firmato viene sottoposta a hashing e firmata utilizzando la chiave privata di una coppia di chiavi pubblica/privata. Quando qualcuno utilizza un URL firmato o un cookie firmato per accedere a un file, CloudFront confronta le parti firmate e non firmate dell'URL o del cookie. Se non corrispondono, CloudFront non serve il file.

È necessario utilizzare le chiavi private RSA 2048 o ECDSA 256 per la firma o i cookie. URLs

Limitazione dell’accesso ai file nei bucket Amazon S3

Facoltativamente, puoi proteggere i contenuti nel tuo bucket Amazon S3 in modo che gli utenti possano accedervi tramite la distribuzione CloudFront specificata ma non possono accedervi direttamente utilizzando Amazon S3. URLs Ciò impedisce a qualcuno di aggirare CloudFront e utilizzare l'URL di Amazon S3 per ottenere contenuti a cui desideri limitare l'accesso. Questo passaggio non è necessario per utilizzare signedURLs, ma lo consigliamo.

Per richiedere agli utenti di accedere ai tuoi contenuti tramite CloudFront URLs, esegui le seguenti attività:

- Concedi a un'autorizzazione di controllo dell'accesso all' CloudFront origine per leggere i file nel bucket S3.
- Crea il controllo di accesso di origine e associalo alla tua CloudFront distribuzione.
- Rimuovi l'autorizzazione a chiunque altro a utilizzare Amazon S3 URLs per leggere i file.

Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

Limitazione dell’accesso ai file su origini personalizzate

Se utilizzi un'origine personalizzata, puoi facoltativamente configurare le intestazioni personalizzate per limitare l'accesso. CloudFront Per ottenere i file da un'origine personalizzata, è necessario che i file siano accessibili CloudFront tramite una richiesta HTTP (o HTTPS) standard. Tuttavia, utilizzando intestazioni personalizzate, puoi limitare ulteriormente l'accesso ai tuoi contenuti in modo che gli

utenti possano accedervi solo tramite CloudFront e non direttamente. Questo passaggio non è necessario per utilizzare signed URLs, ma lo consigliamo.

Per richiedere agli utenti di accedere ai contenuti tramite CloudFront, modifica le seguenti impostazioni nelle tue CloudFront distribuzioni:

Origin Custom Headers (Intestazioni personalizzate origine)

Configura CloudFront per inoltrare le intestazioni personalizzate alla tua origine. Per informazioni, consulta Configurazione di CloudFront per aggiungere intestazioni personalizzate alle richieste origine.

Viewer Protocol Policy (Policy protocollo visualizzatore)

Configura la distribuzione in modo che i visualizzatori utilizzino HTTPS per accedere a CloudFront. Per informazioni, consulta Viewer Protocol Policy (Policy protocollo visualizzatore).

Origin Protocol Policy (Policy protocollo origine)

Configura la tua distribuzione in modo CloudFront che richieda l'utilizzo dello stesso protocollo dei visualizzatori per inoltrare le richieste all'origine. Per informazioni, consulta Protocollo (solo origini personalizzate).

Dopo aver apportato queste modifiche, aggiorna l'applicazione sull'origine personalizzata per accettare solo le richieste che includono le intestazioni personalizzate che hai configurato CloudFront per l'invio.

La combinazione della Policy del protocollo del visualizzatore e della Policy del protocollo di origine garantisce che le intestazioni personalizzate siano crittografate durante il transito. Tuttavia, ti consigliamo di eseguire periodicamente le seguenti operazioni per ruotare le intestazioni personalizzate che vengono CloudFront inoltrate all'origine:

1. Aggiorna la CloudFront distribuzione per iniziare a inoltrare una nuova intestazione all'origine personalizzata.
2. Aggiorna l'applicazione per accettare la nuova intestazione come conferma dell'origine della richiesta. CloudFront
3. Quando le richieste non includono più l'intestazione che stai sostituendo, aggiorna l'applicazione in modo che non accetti più la vecchia intestazione come conferma dell'origine della richiesta. CloudFront

Specificate i firmatari che possono creare cookie firmati e firmati URLs

Argomenti

Per creare cookie firmati URLs o firmati, è necessario un firmatario. Un firmatario è un gruppo di chiavi attendibile in cui CloudFront crei o un AWS account che contiene una coppia di CloudFront chiavi. Ti consigliamo di utilizzare gruppi di chiavi affidabili con cookie firmati URLs e firmati. Per ulteriori informazioni, consulta Scegli tra gruppi di chiavi affidabili (consigliato) e Account AWS.

Il firmatario ha due scopi:

- Non appena aggiungi il firmatario alla tua distribuzione, CloudFront inizia a richiedere che gli spettatori utilizzino cookie firmati URLs o firmati per accedere ai tuoi file.
- Quando crei cookie firmati URLs o firmati, utilizzi la chiave privata della coppia di chiavi del firmatario per firmare una parte dell'URL o del cookie. Quando qualcuno richiede un file con restrizioni, CloudFront confronta la firma nell'URL o nel cookie con l'URL o il cookie non firmato, per verificare che non sia stata manomessa. CloudFront verifica inoltre che l'URL o il cookie siano validi, vale a dire, ad esempio, che la data e l'ora di scadenza non siano trascorse.

Quando specifichi un firmatario, specifichi anche indirettamente i file che richiedono cookie firmati URLs o firmati aggiungendo il firmatario a un comportamento di cache. Se la tua distribuzione ha un solo comportamento nella cache, gli utenti devono utilizzare cookie firmati URLs o firmati per accedere a qualsiasi file della distribuzione. Se crei più comportamenti di cache e aggiungi firmatari ad alcuni comportamenti di cache e non ad altri, puoi richiedere che gli utenti utilizzino i cookie firmati URLs o firmati per accedere ad alcuni file e non ad altri.

Per specificare i firmatari (le chiavi private) autorizzati a creare cookie firmati URLs o firmati e per aggiungere i firmatari alla tua CloudFront distribuzione, esegui le seguenti operazioni:

1. Decidi se utilizzare un gruppo di chiavi attendibile o un altro Account AWS come firmatario. Ti consigliamo di utilizzare un gruppo di chiavi attendibile. Per ulteriori informazioni, consulta Scegli tra gruppi di chiavi affidabili (consigliato) e Account AWS.
2. Per il firmatario scelto nel passaggio 1, crea una coppia di chiavi pubbliche-private. Per ulteriori informazioni, consulta Creazione di coppie di chiavi per i firmatari.
3. Se utilizzi .NET o Java per creare cookie firmati URLs o firmati, riformatta la chiave privata. Per ulteriori informazioni, consulta Riformattazione della chiave privata (solo .NET e Java).
4. Nella distribuzione per la quale stai creando cookie firmati URLs o firmati, specifica il firmatario. Per ulteriori informazioni, consulta Aggiunta di un firmatario a una distribuzione.

Scegli tra gruppi di chiavi affidabili (consigliato) e Account AWS

Per utilizzare i cookie firmati URLs o firmati, è necessario un firmatario. Un firmatario è un gruppo di chiavi attendibile in CloudFront cui crei o un gruppo Account AWS che contiene una coppia di CloudFront chiavi. Ti consigliamo di utilizzare i gruppi di chiavi attendibili per i seguenti motivi:

- Con i gruppi di CloudFront chiavi, non è necessario utilizzare l' AWS account utente root per gestire le chiavi pubbliche per i cookie CloudFront firmati URLs e firmati. AWS le migliori pratiche consigliano di non utilizzare l'utente root quando non è necessario.
- Con i gruppi di CloudFront chiavi, puoi gestire chiavi pubbliche, gruppi di chiavi e firmatari affidabili utilizzando l' CloudFront API. Puoi utilizzare l'API per automatizzare la creazione e la rotazione delle chiavi. Quando si utilizza l'utente AWS root, è necessario utilizzare il per Console di gestione AWS gestire le coppie di CloudFront chiavi, quindi non è possibile automatizzare il processo.
- Poiché puoi gestire i gruppi di chiavi con l' CloudFront API, puoi anche utilizzare le politiche di autorizzazione AWS Identity and Access Management (IAM) per limitare ciò che i diversi utenti sono autorizzati a fare. Ad esempio, puoi consentire agli utenti di caricare chiavi pubbliche, ma non eliminarle. In alternativa, puoi consentire agli utenti di eliminare le chiavi pubbliche, ma solo quando vengono soddisfatte determinate condizioni, ad esempio l'utilizzo dell'autenticazione a più fattori, l'invio della richiesta da una determinata rete o l'invio della richiesta entro un determinato intervallo di data e ora.
- Con i gruppi di CloudFront chiavi, puoi associare un numero maggiore di chiavi pubbliche alla tua CloudFront distribuzione, offrendoti una maggiore flessibilità nel modo in cui utilizzi e gestisci le chiavi pubbliche. Per impostazione predefinita, puoi associare fino a quattro gruppi di chiavi a una singola distribuzione e disporre di un massimo di cinque chiavi pubbliche in un gruppo di chiavi.

Quando si utilizza l'utente root dell' AWS account per gestire le coppie di CloudFront chiavi, è possibile avere solo fino a due coppie di CloudFront chiavi attive per AWS account.

Creazione di coppie di chiavi per i firmatari

Ogni firmatario utilizzato per creare cookie CloudFront firmati URLs o firmati deve disporre di una coppia di key pair pubblica-privata. Il firmatario utilizza la propria chiave privata per firmare l'URL o i cookie e CloudFront utilizza la chiave pubblica per verificare la firma.

Il modo in cui si crea una coppia di chiavi dipende dal fatto che si utilizzi un gruppo di chiavi attendibile come firmatario (consigliato) o una coppia di CloudFront chiavi. Per ulteriori informazioni, consultare le sezioni indicate di seguito. La coppia di chiavi creata deve soddisfare i seguenti requisiti:

- Deve essere una coppia di chiavi SSH-2 RSA 2048 o ECDSA 256.
- Deve essere in formato PEM codificato in base64.

Per proteggere le applicazioni, ti consigliamo di ruotare periodicamente le coppie di chiavi. Per ulteriori informazioni, consulta Rotazione di coppie di chiavi.

Crea una coppia di chiavi per un gruppo di chiavi attendibile (scelta consigliata)

Per creare una coppia di chiavi per un gruppo di chiavi attendibile, attieniti alla seguente procedura:

1. Creare la coppia di chiavi pubbliche-private.
2. Carica la chiave pubblica su CloudFront.
3. Aggiungi la chiave pubblica a un gruppo di CloudFront chiavi.

Per ulteriori informazioni, consulta le procedure seguenti.

Per creare una coppia di chiavi

> **Note**
>
> Le fasi seguenti utilizzano OpenSSL come esempio di un metodo per creare una coppia di chiavi. Esistono molti altri modi per creare una coppia di chiavi RSA o ECDSA.

1. Eseguire uno dei seguenti comandi di esempio:

   - Il comando di esempio seguente utilizza OpenSSL per generare una coppia di chiavi RSA con una lunghezza di 2048 bit e salvarla nel file denominato `private_key.pem`.

     ```
     openssl genrsa -out private_key.pem 2048
     ```

   - Il comando di esempio seguente utilizza OpenSSL per generare una coppia di chiavi ECDSA con una curva `prime256v1` e salvarla nel file denominato `private_key.pem`.

     ```
     openssl ecparam -name prime256v1 -genkey -noout -out privatekey.pem
     ```

2. Il file risultante contiene la chiave pubblica e quella privata. Il comando di esempio seguente estrae la chiave pubblica dal file denominato `private_key.pem`.

   ```
   openssl rsa -pubout -in private_key.pem -out public_key.pem
   ```

   Puoi caricare la chiave pubblica (nel file `public_key.pem`) in un secondo momento, nella procedura seguente.

Per caricare la chiave pubblica su CloudFront

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel menu di navigazione, scegli Public keys (Chiavi pubbliche).
3. Scegli Crea chiave pubblica.
4. Nella finestra Crea chiave pubblica, effettua le operazioni seguenti:

   a. In Key name (Nome chiave), digita un nome per identificare la chiave pubblica.

   b. In Key value (Valore chiave), incolla la chiave pubblica. Se hai seguito i passaggi descritti nella procedura precedente, la chiave pubblica si trova nel file denominato `public_key.pem`. Per copiare e incollare il contenuto della chiave pubblica, puoi procedere come segue:

      - Usa il comando cat sulla riga di comando macOS o Linux, in questo modo:

```
cat public_key.pem
```

Copia l'output di quel comando, quindi incollalo nel campo Key value (Valore chiave).

- Apri il `public_key.pem` file con un editor di testo semplice come Notepad (su Windows) o (su macOS). TextEdit Copia il contenuto del file, quindi incollalo nel campo Key value (Valore chiave).

c. (Facoltativo) Per Comment (Commento), aggiungi un commento per descrivere la chiave pubblica.

Al termine, scegli Add (Aggiungi).

5. Registra l'ID della chiave pubblica. Lo utilizzerai in seguito quando crei cookie firmati URLs o firmati, come valore del campo. `Key-Pair-Id`

Per aggiungere la chiave pubblica a un gruppo di chiavi

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel menu di navigazione, scegli Key groups (Gruppi di chiavi).
3. Scegli Add key group (Aggiungi gruppo di chiavi).
4. Nella pagina Create key group (Crea gruppo di chiavi) effettua le operazioni seguenti:

   a. In Key group name (Nome gruppo di chiavi), digita un nome per identificare il gruppo di chiavi.

   b. (Facoltativo) Per Comment (Commento), digita un commento per descrivere il gruppo di chiavi.

   c. Per Public keys (Chiavi pubbliche), seleziona la chiave pubblica da aggiungere al gruppo di chiavi, quindi scegli Add (Aggiungi). Ripeti questo passaggio per ogni chiave pubblica che desideri aggiungere al gruppo di chiavi.

5. Scegli Create key group (Crea gruppo di chiavi).
6. Registra il nome del gruppo di chiavi. La si usa in seguito per associare il gruppo di chiavi a un comportamento della cache in una CloudFront distribuzione. (Nell' CloudFront API, si utilizza l'ID del gruppo di chiavi per associare il gruppo di chiavi a un comportamento della cache.)

Creare una CloudFront key pair (scelta non consigliata, richiede l'utente Account AWS root)

> **Important**
>
> Ti consigliamo di creare una chiave pubblica per un gruppo di chiavi attendibili invece della seguente procedura. Per il metodo consigliato per creare chiavi pubbliche per i cookie firmati URLs e firmati, consultaCrea una coppia di chiavi per un gruppo di chiavi attendibile (scelta consigliata).

È possibile creare una CloudFront key pair nei seguenti modi:

- Crea una coppia di chiavi in Console di gestione AWS e scarica la chiave privata. Segui la procedura descritta di seguito.
- Crea un coppia di chiavi RSA utilizzando un'applicazione, ad esempio OpenSSL, e poi carica la chiave pubblica nella Console di gestione AWS. Per ulteriori informazioni sulla creazione di una coppia di chiavi RSA, consulta Crea una coppia di chiavi per un gruppo di chiavi attendibile (scelta consigliata).

Per creare coppie di CloudFront chiavi in Console di gestione AWS

1. Accedi Console di gestione AWS utilizzando le credenziali dell' AWS account utente root.

   > **Important**
   >
   > Gli utenti IAM non possono creare coppie di CloudFront chiavi. Devi accedere utilizzando le credenziali utente root per creare coppie di chiavi.

2. Scegli il nome dell'account, quindi scegli My Security Credentials (Le mie credenziali di sicurezza).
3. Scegli coppie di CloudFront chiavi.
4. Conferma di non avere più di una coppia di chiavi attiva. Non puoi creare una coppia di chiavi se hai già due coppie di chiavi attive.
5. Scegli Create New Key Pair (Crea nuova coppia di chiavi).

> **Note**
>
> Puoi anche scegliere di creare la tua coppia di chiavi e caricare la chiave pubblica. CloudFront le coppie di chiavi supportano chiavi a 1024, 2048 o 4096 bit.

6. Nella finestra di dialogo Create Key Pair (Crea coppia di chiavi) scegli Download Private Key File (Scarica il file della chiave privata), quindi salva il file nel computer.

> **Important**
>
> Salva la chiave privata per la tua coppia di CloudFront chiavi in una posizione sicura e imposta le autorizzazioni sul file in modo che solo gli amministratori desiderati possano leggerlo. Se qualcuno ottiene la tua chiave privata, può generare cookie firmati URLs e firmati validi e scaricare i tuoi contenuti. Non è possibile recuperare nuovamente la chiave privata, quindi se la si perde o la si elimina, è necessario creare una nuova coppia di CloudFront chiavi.

7. Registra l'ID per la tua coppia di chiavi. (Nel Console di gestione AWS, questo è chiamato Access Key ID.) Lo utilizzerai quando crei cookie firmati URLs o firmati.

Riformattazione della chiave privata (solo .NET e Java)

Se utilizzi .NET o Java per creare cookie firmati URLs o firmati, non puoi utilizzare la chiave privata della tua coppia di chiavi nel formato PEM predefinito per creare la firma. Effettua invece le seguenti operazioni:

- .NET Framework: converti la chiave privata nel formato XML utilizzato da .NET Framework. Sono disponibili vari strumenti per eseguire la conversione.
- Java: converti la chiave privata nel formato DER. Un modo per farlo è con il seguente comando OpenSSL. Nel comando seguente, `private_key.pem` è il nome del file che contiene la chiave privata con formattazione PEM e `private_key.der` è il nome del file che contiene la chiave privata con formattazione DER dopo l'esecuzione del comando.

```
openssl pkcs8 -topk8 -nocrypt -in private_key.pem -inform PEM -out private_key.der -
outform DER
```

Per assicurarti che l'encoder funzioni correttamente, aggiungi il JAR per la crittografia Java Bouncy Castle APIs al tuo progetto, quindi aggiungi il provider Bouncy Castle.

Aggiunta di un firmatario a una distribuzione

Un firmatario è il gruppo di chiavi attendibile (consigliato) o CloudFront la coppia di chiavi che può creare cookie firmati URLs e firmati per una distribuzione. Per utilizzare i cookie firmati URLs o firmati con una CloudFront distribuzione, devi specificare un firmatario.

I firmatari sono associati ai comportamenti cache. Ciò consente di richiedere cookie firmati URLs o firmati per alcuni file e non per altri della stessa distribuzione. Una distribuzione richiede cookie firmati URLs o cookie solo per i file associati ai comportamenti di cache corrispondenti.

Analogamente, un firmatario può firmare URLs o utilizzare cookie solo per i file associati ai comportamenti di cache corrispondenti. Ad esempio, se hai un firmatario per un comportamento di cache e un firmatario diverso per un diverso comportamento di cache, nessuno dei due firmatari può creare cookie firmati URLs o cookie per i file associati all'altro comportamento di cache.

Important

Prima di aggiungere un firmatario alla distribuzione, effettua le seguenti operazioni:

- Definisci con attenzione i pattern di percorso nei comportamenti cache e la sequenza dei comportamenti cache in modo da non concedere agli utenti l'accesso non intenzionale al contenuto o impedisca loro di accedere ai contenuti che desideri essere disponibili per tutti.

  Ad esempio, supponiamo che una richiesta corrisponda al modello di percorso per due comportamenti cache. Il primo comportamento di cache non richiede cookie firmati URLs o firmati, mentre il secondo lo richiede. Gli utenti saranno in grado di accedere ai file senza utilizzare cookie firmati URLs o firmati perché CloudFront elabora il comportamento della cache associato alla prima corrispondenza.

  Per ulteriori informazioni sui modelli di percorso, consulta Modello di percorso.
- Per una distribuzione che stai già utilizzando per distribuire contenuti, assicurati di essere pronto a iniziare a generare cookie firmati URLs e firmati prima di aggiungere un firmatario. Quando aggiungi un firmatario, CloudFront rifiuta le richieste che non includono un URL firmato o un cookie firmato valido.

Puoi aggiungere firmatari alla tua distribuzione utilizzando la CloudFront console o l'API. CloudFront

Console

La procedura seguente illustra come aggiungere un gruppo di chiavi attendibili come firmatario. Puoi anche aggiungerne uno Account AWS come firmatario attendibile, ma non è consigliato.

Per aggiungere un firmatario a una distribuzione utilizzando la console

1. Registra l'ID gruppo di chiavi del gruppo di chiavi che desideri utilizzare come firmatario attendibile. Per ulteriori informazioni, consulta Crea una coppia di chiavi per un gruppo di chiavi attendibile (scelta consigliata).
2. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
3. Scegli la distribuzione di cui desideri proteggere i file con cookie firmati URLs o firmati.

   > **Note**
   >
   > Per aggiungere un firmatario a una nuova distribuzione, specifica le stesse impostazioni descritte nel passaggio 6 per la creazione della distribuzione.

4. Scegli la scheda Behaviors (Comportamenti).
5. Seleziona il comportamento della cache il cui modello di percorso corrisponde ai file che desideri proteggere con cookie firmati URLs o firmati, quindi scegli Modifica.
6. Nella pagina Edit Behavior (Modifica comportamento) effettua le operazioni seguenti:
   a. Per Limita l'accesso degli spettatori (utilizza cookie firmati URLs o firmati), scegli Sì.
   b. Per Trusted Key Groups or Trusted Signer (Gruppi di chiavi attendibili o Firmatari attendibili), scegli Trusted Key Groups (Gruppi di chiavi attendibili)
   c. Per Trusted Key Groups (Gruppi di chiavi attendibili), scegli il gruppo di chiavi da aggiungere, quindi scegli Add (Aggiungi). Ripeti l'operazione se desideri aggiungere più di un gruppo di chiavi.
7. Scegli Yes, Edit (Sì, Modifica) per aggiornare il comportamento cache.

API

Puoi utilizzare l' CloudFront API per aggiungere un gruppo di chiavi attendibile come firmatario. Puoi aggiungere un firmatario a una distribuzione esistente o a una nuova distribuzione. In entrambi i casi, specifica i valori nell'elemento `TrustedKeyGroups`.

Puoi anche aggiungerne uno Account AWS come firmatario attendibile, ma non è consigliato.

Consulta i seguenti argomenti nell'Amazon CloudFront API Reference:

- Aggiorna una distribuzione esistente: UpdateDistribution
- Crea una nuova distribuzione — CreateDistribution

Rotazione di coppie di chiavi

Ti consigliamo di ruotare (modificare) periodicamente le coppie di chiavi per i cookie firmati URLs e firmati. Per ruotare le coppie di chiavi che utilizzi per creare cookie firmati URLs o firmati senza invalidarli URLs o cookie che non sono ancora scaduti, esegui le seguenti operazioni:

1. Crea una nuova coppia di chiavi e aggiungi la chiave pubblica a un gruppo di chiavi. Per ulteriori informazioni, consulta Crea una coppia di chiavi per un gruppo di chiavi attendibile (scelta consigliata).
2. Se nel passaggio precedente hai creato un nuovo gruppo di chiavi, aggiungi il gruppo di chiavi alla distribuzione come firmatario.

   > **Important**
   >
   > Non rimuovere le chiavi pubbliche esistenti dal gruppo di chiavi o i gruppi di chiavi dalla distribuzione. Aggiungi solo nuovi elementi.

3. Aggiorna la tua applicazione per creare firme utilizzando la chiave privata della nuova coppia di chiavi. Verifica che i cookie firmati URLs o quelli firmati con le nuove chiavi private funzionino.
4. Attendi che sia trascorsa la data di scadenza URLs o che i cookie siano stati firmati utilizzando la chiave privata precedente. Quindi rimuovi la vecchia chiave pubblica dal gruppo di chiavi. Se hai creato un nuovo gruppo di chiavi nel passaggio 2, rimuovi il vecchio gruppo di chiavi dalla distribuzione.

Decidi di utilizzare cookie firmati URLs o firmati

CloudFront i cookie firmati URLs e firmati offrono le stesse funzionalità di base: consentono di controllare chi può accedere ai contenuti. Se desideri pubblicare contenuti privati CloudFront e stai cercando di decidere se utilizzare cookie firmati URLs o firmati, prendi in considerazione quanto segue.

Utilizza i file firmati URLs nei seguenti casi:

- Intendi limitare l'accesso a singoli file, ad esempio, il download di un'installazione per l'applicazione.
- I tuoi utenti stanno utilizzando un client (ad esempio, un client HTTP personalizzato) che non supporta i cookie.

Utilizza cookie firmati nei seguenti casi:

- Intendi fornire accesso a più file con restrizioni, ad esempio, tutti i file per un video in formato HLS o tutti i file nell'area abbonati di un sito Web.
- Non vuoi cambiare la tua versione attuale URLs.

Se attualmente non utilizzi signed URLs e se il file (unsigned) URLs contiene uno dei seguenti parametri della stringa di query, non puoi utilizzare cookie firmati URLs o firmati:

- `Expires`
- `Policy`
- `Signature`
- `Key-Pair-Id`

CloudFront presuppone URLs che i parametri della stringa di query che contengono uno di questi parametri siano firmati URLs e quindi non esaminerà i cookie firmati.

Utilizza sia i cookie firmati che URLs quelli firmati

I cookie firmati URLs hanno la precedenza sui cookie firmati. Se utilizzi sia cookie firmati URLs che firmati per controllare l'accesso agli stessi file e un visualizzatore utilizza un URL firmato per richiedere un file, CloudFront determina se restituire il file al visualizzatore solo in base all'URL firmato.

Usa firmato URLs

Un URL firmato include ulteriori informazioni, ad esempio, una data e un'ora di scadenza, che offrono un maggiore controllo sull'accesso al tuo contenuto. Queste informazioni aggiuntive appaiono in una dichiarazione di policy, basata su una policy predefinita o personalizzata. Le differenze tra policy predefinite e personalizzate sono descritte nelle due sezioni successive.

> **Note**
>
> È possibile crearne alcuni firmati URLs utilizzando criteri predefiniti e crearne alcuni firmati URLs utilizzando criteri personalizzati per la stessa distribuzione.

Argomenti

Decidi di utilizzare politiche predefinite o personalizzate per la firma URLs

Quando crei un URL firmato, scrivi una dichiarazione di policy in formato JSON che specifica le restrizioni sull'URL firmato, ad esempio, il periodo di validità dell'URL. Puoi utilizzare una policy predefinita o una personalizzata. Di seguito sono riportate le differenze tra policy predefinite e personalizzate:

Descrizione	Policy predefinita	Policy personalizzata
Puoi riutilizzare la dichiarazione di policy per più file. Per riutilizzare la dichiarazione di policy, devi utilizzare caratteri jolly nell'oggetto `Resource`. Per	No	Sì

Descrizione	Policy predefinita	Policy personalizzata
ulteriori informazioni, consulta Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata.)		
Puoi specificare la data e l'ora in cui gli utenti possono iniziare ad accedere al tuo contenuto.	No	Sì (facoltativo)
Puoi specificare la data e l'ora in cui gli utenti non possono più accedere al tuo contenuto.	Sì	Sì
Puoi specificare l'indirizzo IP o l'intervallo di indirizzi IP degli utenti che possono accedere al tuo contenuto.	No	Sì (facoltativo)
L'URL firmato include una versione con codifica base64 della policy, che risulta in un URL più lungo.	No	Sì

Per informazioni sulla creazione di criteri URLs predefiniti firmati, consulta. Creazione di un URL firmato utilizzando una policy di accesso predefinita

Per informazioni sulla creazione di una politica firmata URLs utilizzando una politica personalizzata, vedereCreazione di un URL firmato utilizzando una policy personalizzata.

Come funzionano i URLs firmatari

Ecco una panoramica di come CloudFront configuri Amazon S3 for signed URLs e di come CloudFront risponde quando un utente utilizza un URL firmato per richiedere un file.

1. Nella tua CloudFront distribuzione, specifica uno o più gruppi di chiavi affidabili, che contengono le chiavi pubbliche da CloudFront utilizzare per verificare la firma dell'URL. Utilizzi le chiavi private corrispondenti per firmare il URLs.

   CloudFront supporta firme a URLs chiave firmate con RSA 2048 ed ECDSA 256.

   Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

2. Sviluppa la tua applicazione per determinare se un utente debba avere accesso ai tuoi contenuti e creane una versione firmata URLs per i file o le parti dell'applicazione a cui desideri limitare l'accesso. Per ulteriori informazioni, consulta i seguenti argomenti:

   - Creazione di un URL firmato utilizzando una policy di accesso predefinita
   - Creazione di un URL firmato utilizzando una policy personalizzata

3. Un utente richiede la firma di un file per il quale si desidera richiedere la firma URLs.
4. La tua applicazione verifica che l'utente è autorizzato ad accedere al file: ha eseguito l'accesso, ha pagato per accedere al contenuto o ha soddisfatto altri requisiti per l'accesso.
5. La tua applicazione crea e restituisce un URL firmato all'utente.
6. L'URL firmato consente all'utente di scaricare o riprodurre in streaming il contenuto.

   Questa fase è automatica; l'utente in genere non deve eseguire ulteriori operazioni per accedere al contenuto. Ad esempio, se un utente accede al tuo contenuto in un browser Web, l'applicazione restituisce l'URL firmato al browser. Il browser utilizza immediatamente l'URL firmato per accedere al file nella cache CloudFront edge senza alcun intervento da parte dell'utente.
7. CloudFront utilizza la chiave pubblica per convalidare la firma e confermare che l'URL non è stato manomesso. Se la firma non è valida, la richiesta viene respinta.

   Se la firma è valida, CloudFront esamina l'informativa nell'URL (o ne costruisce una se utilizzi una politica predefinita) per confermare che la richiesta è ancora valida. Ad esempio, se hai specificato una data e un'ora di inizio e di fine per l'URL, CloudFront conferma che l'utente sta tentando di accedere ai tuoi contenuti durante il periodo di tempo in cui desideri consentire l'accesso.

   Se la richiesta soddisfa i requisiti dell'informativa, CloudFront esegue le operazioni standard: determina se il file è già presente nella cache edge, inoltra la richiesta all'origine se necessario e restituisce il file all'utente.

> **Note**
>
> Se un URL non firmato contiene parametri di stringa di query, assicurati di includerli nella parte dell'URL che firmi. Se aggiungi una stringa di query a un URL firmato dopo la sua creazione, l'URL restituisce uno stato HTTP 403.

Decidi per quanto tempo i firmi URLs sono validi

Puoi distribuire contenuto privato utilizzando un URL firmato valido soltanto per un breve periodo di tempo, anche di pochi minuti. I URLs documenti firmati e validi per un periodo così breve sono utili per distribuire contenuti on-the-fly a un utente per uno scopo specifico, come la distribuzione di film a noleggio o download di musica ai clienti su richiesta. Se i file firmati URLs saranno validi solo per un breve periodo, probabilmente vorrai generarli automaticamente utilizzando un'applicazione sviluppata da te. Quando l'utente inizia a scaricare un file o inizia a riprodurre un file multimediale, CloudFront confronta l'ora di scadenza dell'URL con l'ora corrente per determinare se l'URL è ancora valido.

Puoi anche distribuire contenuto privato utilizzando un URL firmato valido per un periodo di tempo più lungo, anche di vari anni. I URLs documenti firmati validi per un periodo più lungo sono utili per distribuire contenuti privati a utenti noti, ad esempio per distribuire un piano aziendale agli investitori o distribuire materiali di formazione ai dipendenti. Puoi sviluppare un'applicazione per generare questi messaggi firmati a lungo termine per te. URLs

When CloudFront controlla la data e l'ora di scadenza in un URL firmato

CloudFront controlla la data e l'ora di scadenza in un URL firmato al momento della richiesta HTTP. Se un client inizia a scaricare un file di grandi dimensioni immediatamente prima della scadenza, il download viene completato anche se la scadenza avviene durante il download. Se la connessione TCP viene interrotta e il client tenta di riavviare il download dopo la scadenza, il download non riesce.

Se un client utilizza Range GETs per ottenere un file in parti più piccole, qualsiasi richiesta GET che si verifica dopo la scadenza avrà esito negativo. Per ulteriori informazioni su RangeGETs, vedereCome CloudFront elabora le richieste parziali per un oggetto (intervalloGETs).

Codice di esempio e strumenti di terza parte.

Per un esempio di codice che crea la parte con hash e firma di signed URLs, consulta i seguenti argomenti:

- Creazione di una firma per URL utilizzando Perl
- Creazione di una firma per URL utilizzando PHP
- Crea una firma per URL utilizzando C# e .NET Framework
- Creazione di una firma per URL utilizzando Java

Creazione di un URL firmato utilizzando una policy di accesso predefinita

Per creare un URL firmato utilizzando una policy predefinita, completa la procedura seguente.

Creazione di un URL firmato utilizzando una policy predefinita

1. Se stai usando .NET o Java per creare un file firmato URLs e se non hai riformattato la chiave privata per la tua coppia di chiavi dal formato.pem predefinito a un formato compatibile con.NET o con Java, fallo ora. Per ulteriori informazioni, consulta Riformattazione della chiave privata (solo .NET e Java).
2. Concatena i seguenti valori. Puoi utilizzare il formato in questo URL firmato di esempio.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Expires=1767290400&Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5Ew
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

   Rimuovi tutti gli spazi vuoti (compresi i caratteri di tabulazione e di nuova riga). È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione. Tutti i valori hanno un tipo `String`.

   1. ***Base URL for the file***

      L'URL di base è l' CloudFront URL che utilizzeresti per accedere al file se non utilizzassi signed URLs, inclusi i parametri della stringa di query, se presenti. Nell'esempio precedente, l'URL di base è `https://d111111abcdef8.cloudfront.net/image.jpg`. Per ulteriori informazioni sul formato delle URLs distribuzioni, vederePersonalizzazione del formato URL per i file in CloudFront.

      - L' CloudFront URL seguente riguarda un file di immagine in una distribuzione (utilizzando il nome di CloudFront dominio). Nota che `image.jpg` è una directory `images`. Il percorso al file nell'URL deve corrispondere al percorso al file nel server HTTP o nel bucket Amazon S3.

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

      - Il seguente CloudFront URL include una stringa di query:

        ```
        https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
        ```

- Di seguito CloudFront URLs sono riportati i file di immagine in una distribuzione. Entrambi utilizzano un nome di dominio alternativo. Il secondo include una stringa di query:

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

  ```
  https://www.example.com/images/image.jpg?color=red
  ```

- L' CloudFront URL seguente riguarda un file di immagine in una distribuzione che utilizza un nome di dominio alternativo e il protocollo HTTPS:

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

2. **?**

   Il carattere ? indica che i parametri di query seguono l'URL di base. Includi il carattere ? anche senza specificare alcun parametro di query.

   > **Note**
   >
   > Puoi specificare i seguenti parametri di query in qualsiasi ordine.

3. ***Your query string parameters, if any*&**

   (Facoltativo) Puoi immettere parametri della stringa di query personalizzati. A tale scopo, aggiungi una e commerciale (&) tra ciascuno di essi, ad esempio `color=red&size=medium`. Puoi specificare parametri della stringa di query in qualsiasi ordine all'interno dell'URL.

   > **Important**
   >
   > I parametri della stringa di query non possono essere denominati `Expires`, `Signature` o `Key-Pair-Id`.

4. **Expires=*date and time in Unix time format (in seconds) and Coordinated Universal Time (UTC)***

   La data e l'ora in cui desideri che l'URL blocchi l'accesso al file.

Specifica la data e l'ora di scadenza in formato Unix (in secondi) e UTC. Ad esempio, la data 1 gennaio 2026 10:00 UTC viene convertita in `1767290400` in un formato Unix, come illustrato nell'esempio all'inizio di questo argomento.

Per usare il tempo epoch, specifica un numero intero a 64 bit per una data non posteriore a `9223372036854775807` (venerdì 11 aprile 2262 alle 23:47:16.854 UTC).

Per informazioni sul formato UTC, consulta RFC 3339, Date and Time on the Internet: Timestamps.

5. **`&Signature=`*`hashed and signed version of the policy statement`***

   Una versione con hash, firma e codifica base64 della dichiarazione di policy JSON. Per ulteriori informazioni, consulta Creazione di una firma per un URL firmato che utilizza una policy di accesso predefinita.

6. **`&Key-Pair-Id=`*`public key ID for the CloudFront public key whose corresponding private key you're using to generate the signature`***

   L'ID di una chiave CloudFront pubblica, ad esempio`K2JCJMDEHXQW5F`. L'ID della chiave pubblica indica CloudFront quale chiave pubblica utilizzare per convalidare l'URL firmato. CloudFront confronta le informazioni contenute nella firma con quelle contenute nell'informativa per verificare che l'URL non sia stato manomesso.

   Questa chiave pubblica deve appartenere a un gruppo di chiavi che sia un firmatario attendibile nella distribuzione. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

Creazione di una firma per un URL firmato che utilizza una policy di accesso predefinita

Per creare la firma per un URL firmato che utilizza una policy di accesso predefinita, completa le seguenti procedure.

Argomenti

- Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy di accesso predefinita
- Creazione di una firma per un URL firmato che utilizza una policy di accesso predefinita

Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy di accesso predefinita

Quando crei un URL firmato utilizzando una policy predefinita, il parametro `Signature` è una versione con hash e firma di una dichiarazione di policy. Per i criteri firmati URLs che utilizzano una politica predefinita, non includi la dichiarazione di politica nell'URL, mentre per quelli firmati URLs che utilizzano una politica personalizzata. Per creare una dichiarazione di policy, esegui la procedura descritta di seguito.

Per creare la dichiarazione di policy per un URL firmato che utilizza una policy predefinita

1. Crea la dichiarazione di policy utilizzando il formato JSON seguente e la codifica caratteri UTF-8. Includi tutta le punteggiatura e altri valori letterali esattamente come specificato. Per informazioni sui parametri `Resource` e `DateLessThan`, consulta Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy predefinita.

   ```
   {
       "Statement": [
           {
               "Resource": "base URL or stream name",
               "Condition": {
                   "DateLessThan": {
                       "AWS:EpochTime": ending date and time in Unix time format and
    UTC
                   }
               }
           }
       ]
   }
   ```

2. Rimuovi tutti gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla dichiarazione di policy. È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione.

Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy predefinita

Quando crei una dichiarazione di policy per una policy predefinita, specifichi i valori seguenti.

Risorsa

> **Note**
>
> Puoi specificare un solo valore per `Resource`.

L'URL di base che include le stringhe di query, se presenti, ma escludendo CloudFront `Expires`, `Signature`, e `Key-Pair-Id` i parametri, ad esempio:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

Tenere presente quanto segue:

- Protocollo: il valore deve iniziare con `http://` o `https://`.
- Parametri di stringa di query: se non hai parametri di stringa di query, ometti il punto di domanda.
- Nomi di dominio alternativi: se specifichi un nome di dominio alternativo (CNAME) nell'URL, devi specificarlo quando fai riferimento al file nella pagina Web o nell'applicazione. Non specificare l'URL di Amazon S3 per l'oggetto.

DateLessThan

La data e l'ora di scadenza per l'URL in formato Unix (in secondi) e UTC. Ad esempio, le 10:00 UTC del 1° gennaio 2026 vengono convertite in 1767290400 nel formato orario Unix.

Questo valore deve corrispondere al valore del parametro di stringa di query `Expires` nell'URL firmato. Non racchiudere il valore tra virgolette.

Per ulteriori informazioni, consulta When CloudFront controlla la data e l'ora di scadenza in un URL firmato.

Esempio di dichiarazione di policy per un URL firmato che utilizza una policy predefinita

Quando si utilizza la seguente dichiarazione politica di esempio in un URL firmato, un utente può accedere al file `https://d111111abcdef8.cloudfront.net/horizon.jpg` fino alle 10:00 UTC del 1° gennaio 2026:

```
{
    "Statement": [
```

```
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Creazione di una firma per un URL firmato che utilizza una policy di accesso predefinita

Per creare il valore per il parametro `Signature` in un URL firmato, devi sottoporre a hashing e firmare la dichiarazione di policy creata in Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy di accesso predefinita.

Per ulteriori informazioni ed esempi su come sottoporre a hashing, firmare e codificare la dichiarazione di policy, consulta:

- Comandi Linux e OpenSSL per la crittografia e la codifica base64
- Codice di esempio per la creazione di una firma per un URL firmato

Opzione 1: per creare una firma utilizzando una policy predefinita

1. Utilizza la funzione hash SHA-1 e la chiave privata RSA o ECDSA generata per eseguire l'hashing e firmare la dichiarazione di policy creata nella procedura Per creare la dichiarazione di policy per un URL firmato che utilizza una policy predefinita. Utilizza la versione della dichiarazione di policy che non include più spazi vuoti.

   Per la chiave privata richiesta dalla funzione hash, utilizza una chiave privata la cui chiave pubblica si trova in un gruppo di chiavi attendibili attivo per la distribuzione.

   > **Note**
   >
   > Il metodo utilizzato per sottoporre a hashing e firmare la dichiarazione di policy dipende dalla piattaforma e dal linguaggio di programmazione. Per il codice di esempio, consulta Codice di esempio per la creazione di una firma per un URL firmato.

2. Rimuovi gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.
4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Aggiungi il valore risultante all'URL firmato dopo `&Signature=` e ritorna a Creazione di un URL firmato utilizzando una policy predefinita per completare il concatenamento delle parti dell'URL firmato.

Creazione di un URL firmato utilizzando una policy personalizzata

Per creare un URL firmato utilizzando una policy personalizzata, completa la procedura seguente.

Per creare un URL firmato utilizzando una policy personalizzata

1. Se stai usando .NET o Java per creare un file firmato URLs e se non hai riformattato la chiave privata per la tua coppia di chiavi dal formato.pem predefinito a un formato compatibile con.NET o con Java, fallo ora. Per ulteriori informazioni, consulta Riformattazione della chiave privata (solo .NET e Java).
2. Concatena i seguenti valori. Puoi utilizzare il formato in questo URL firmato di esempio.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Policy=eyANCiAgICEXAMPLEW1lbnQiOiBbeyANCiAgICAgICJSZXNvdXJj
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

Rimuovi tutti gli spazi vuoti (compresi i caratteri di tabulazione e di nuova riga). È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione. Tutti i valori hanno un tipo `String`.

1. ***`Base URL for the file`***

   L'URL di base è l' CloudFront URL che utilizzeresti per accedere al file se non utilizzassi signed URLs, inclusi i parametri della stringa di query, se presenti. Nell'esempio precedente, l'URL di base è `https://d111111abcdef8.cloudfront.net/image.jpg`. Per ulteriori informazioni sul formato delle URLs distribuzioni, vedere[Personalizzazione del formato URL per i file in CloudFront](#).

   I seguenti esempi mostrano i valori che specifichi per le distribuzioni.

   - L' CloudFront URL seguente riguarda un file di immagine in una distribuzione (utilizzando il nome di CloudFront dominio). Nota che `image.jpg` è una directory `images`. Il percorso al file nell'URL deve corrispondere al percorso al file nel server HTTP o nel bucket Amazon S3.

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

   - Il seguente CloudFront URL include una stringa di query:

     ```
     https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
     ```

   - Di seguito CloudFront URLs sono riportati i file di immagine in una distribuzione. Entrambi utilizzano un nome di dominio alternativo; il secondo include una stringa di query:

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

     ```
     https://www.example.com/images/image.jpg?color=red
     ```

   - L' CloudFront URL seguente riguarda un file di immagine in una distribuzione che utilizza un nome di dominio alternativo e il protocollo HTTPS:

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

2. **`?`**

   Il carattere ? indica che i parametri della stringa di query seguono l'URL di base. Includi il carattere ? anche senza specificare alcun parametro di query.

> **Note**
>
> Puoi specificare i seguenti parametri di query in qualsiasi ordine.

3. ***Your query string parameters, if any*&**

   (Facoltativo) Puoi immettere parametri della stringa di query personalizzati. A tale scopo, aggiungi una e commerciale (&) tra ciascuno di essi, ad esempio `color=red&size=medium`. Puoi specificare parametri della stringa di query in qualsiasi ordine all'interno dell'URL.

   > **Important**
   >
   > I parametri della stringa di query non possono essere denominati `Policy`, `Signature` o `Key-Pair-Id`.

   Se aggiungi parametri personalizzati, aggiungi un carattere & dopo ciascuno di essi, compreso l'ultimo.

4. **Policy=*base64 encoded version of policy statement***

   La dichiarazione di policy in formato JSON, con spazi vuoti rimossi e codifica base64. Per ulteriori informazioni, consulta Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata.

   La dichiarazione di policy controlla l'accesso che un URL firmato concede a un utente. Include l'URL del file, una data e un'ora di scadenza, una data e un'ora facoltative in cui l'URL diventa valido e un indirizzo IP facoltativo o un intervallo di indirizzi IP a cui è consentito accedere al file.

5. **&Signature=*hashed and signed version of the policy statement***

   Una versione con hash, firma e codifica base64 della dichiarazione di policy JSON. Per ulteriori informazioni, consulta Creazione di una firma per un URL firmato che utilizza una policy personalizzata.

6. **&Key-Pair-Id=*public key ID for the CloudFront public key whose corresponding private key you're using to generate the signature***

   L'ID di una chiave CloudFront pubblica, ad esempio`K2JCJMDEHXQW5F`. L'ID della chiave pubblica indica CloudFront quale chiave pubblica utilizzare per convalidare l'URL firmato. CloudFrontconfronta le informazioni contenute nella firma con quelle contenute nell'informativa per verificare che l'URL non sia stato manomesso.

   Questa chiave pubblica deve appartenere a un gruppo di chiavi che sia un firmatario attendibile nella distribuzione. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata

Completa i passaggi seguenti per creare un'istruzione di policy per un URL firmato che utilizza una policy personalizzata.

Per esempi di istruzioni di policy che controllano l'accesso a file in vari modi, consultare the section called "Esempi di dichiarazioni di policy per un URL firmato che utilizza una policy personalizzata".

Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata

1. Crea la dichiarazione di policy utilizzando il formato JSON seguente. Sostituisci i simboli minore di (<) e maggiore di (>) e le relative descrizioni con i tuoi valori. Per ulteriori informazioni, consulta the section called "Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata".

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

Tenere presente quanto segue:

- Puoi includere una sola istruzione nella policy.
- Utilizza la codifica caratteri UTF-8.
- Includi tutta le punteggiatura e nomi di parametro esattamente come specificato. Le abbreviazioni per i nomi di parametro non sono accettate.
- L'ordine dei parametri nella sezione `Condition` non è rilevante.
- Per informazioni sui valori per `Resource`, `DateLessThan`, `DateGreaterThan` e `IpAddress`, consulta the section called “Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata”.

2. Rimuovi tutti gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla dichiarazione di policy. È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione.
3. Codifica la dichiarazione di policy utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.
4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Aggiungi il valore risultante al tuo URL firmato dopo `Policy=`.

6. Crea una firma per l'URL firmato sottoponendo a hashing, firmando e codificando in base64 la dichiarazione di policy. Per ulteriori informazioni, consulta the section called “Creazione di una firma per un URL firmato che utilizza una policy personalizzata”.

Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata

Quando crei una dichiarazione di policy per una policy personalizzata, specifichi i valori seguenti.

Risorsa

L'URL, incluse tutte le stringhe di query, ma esclusi i parametri e. CloudFront `Policy` `Signature` `Key-Pair-Id` Esempio:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg\?
size=large&license=yes
```

Puoi specificare un solo valore URL per `Resource`.

> **Important**
>
> È possibile omettere il parametro `Resource` in una policy, ma in questo caso chiunque con l’URL firmato può accedere a tutti i file in qualsiasi distribuzione associata alla coppia di chiavi utilizzata per creare l’URL firmato.

Tenere presente quanto segue:

- Protocollo: il valore deve iniziare con `http://` `https://` o `*://`.
- Parametri della stringa di query: se l'URL contiene parametri della stringa di query, non utilizzate una barra rovesciata (\) per evitare il carattere del punto interrogativo (?) che inizia la stringa di query. Esempio:

  ```
  https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
  size=large&license=yes
  ```
- Caratteri jolly: puoi utilizzare caratteri jolly nell'URL della policy. Sono supportati i seguenti caratteri jolly:
  - asterisco (*), che corrisponde a zero o più caratteri
  - punto interrogativo (?), che corrisponde esattamente a un carattere

Quando l'URL nella policy CloudFront corrisponde all'URL nella richiesta HTTP, l'URL nella policy viene diviso in quattro sezioni: protocol, domain, path e query string, come segue:

```
[protocol]://[domain]/[path]\?[query string]
```

Quando si utilizza un carattere jolly nell'URL nella policy, la corrispondenza con i caratteri jolly si applica solo entro i limiti della sezione che contiene il carattere jolly. Ad esempio, considera questo URL in una policy:

```
https://www.example.com/hello*world
```

In questo esempio, l'asterisco wildcard (`*`) si applica solo all'interno della sezione path, quindi corrisponde a URLs `https://www.example.com/helloworld` and`https://www.example.com/hello-world`, ma non all'URL. `https://www.example.net/hello?world`

Le seguenti eccezioni si applicano ai limiti delle sezioni per la corrispondenza con i caratteri jolly:

- Un asterisco finale nella sezione del percorso implica un asterisco nella sezione della stringa di query. Ad esempio, `http://example.com/hello*` è uguale a `http://example.com/hello*\?*`.
- Un asterisco finale nella sezione del dominio implica un asterisco nelle sezioni del percorso e della stringa di query. Ad esempio, `http://example.com*` è uguale a `http://example.com*/*\?*`.
- Un URL nella policy può omettere la sezione del protocollo e iniziare con un asterisco nella sezione del dominio. In tal caso, la sezione del protocollo è impostata implicitamente su un asterisco. Ad esempio, l'URL `*example.com` in una policy è equivalente a `*://*example.com/`.
- Un asterisco da solo (`"Resource": "*"`) corrisponde a qualsiasi URL.

Ad esempio, il valore: `https://d111111abcdef8.cloudfront.net/*game_download.zip*` in una policy corrisponde a tutti i seguenti valori: URLs

- `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`
- Nomi di dominio alternativi: se specifichi un nome di dominio alternativo (CNAME) nell'URL nella policy, la richiesta HTTP deve utilizzare il nome di dominio alternativo nella pagina Web o nell'applicazione. Non specificare l'URL Amazon S3 per il file in una policy.

DateLessThan

La data e l'ora di scadenza per l'URL in formato Unix (in secondi) e UTC. Nella policy, non racchiudere il valore tra virgolette. Per informazioni sul formato UTC, consultare Date and Time on the Internet: Timestamps.

Ad esempio, la data 31 gennaio 2023 10:00 UTC viene convertita in 1675159200 nel formato Unix.

Questo è l'unico parametro obbligatorio nella `Condition` sezione. CloudFront richiede questo valore per impedire agli utenti di avere accesso permanente ai tuoi contenuti privati.

Per ulteriori informazioni, consulta the section called "When CloudFront controlla la data e l'ora di scadenza in un URL firmato"

DateGreaterThan (Facoltativo)

Una data e un'ora di inizio (facoltative) per l'URL in formato Unix (in secondi) e UTC. Agli utenti non è consentito accedere al file prima o in corrispondenza della data e ora specificate. Non racchiudere il valore tra virgolette.

IpAddress (Opzionale)

L'indirizzo IP del client che esegue la richiesta HTTP. Tenere presente quanto segue:

- Per consentire a qualsiasi indirizzo IP di accedere al file, ometti il parametro `IpAddress`.
- Puoi specificare un indirizzo IP o un intervallo di indirizzi IP. Non puoi utilizzare la policy per consentire l'accesso se l'indirizzo IP del client si trova in uno dei due intervalli distinti.
- Per consentire l'accesso da un singolo indirizzo IP, specifica:

  `"IPv4 IP address/32"`
- È necessario specificare gli intervalli di indirizzi IP nel formato IPv4 CIDR standard (ad esempio,`192.0.2.0/24`). Per ulteriori informazioni, consultare Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.

> **Important**
>
> Gli indirizzi IP in IPv6 formato, ad esempio 2001:0 db 8:85 a3: :8a2e: 0370:7334, non sono supportati.

Se utilizzi una politica personalizzata che include, non abilitarla per la distribuzione. `IpAddress` IPv6 Se desideri limitare l'accesso ad alcuni contenuti in base all'indirizzo IP e IPv6 alle richieste di supporto per altri contenuti, puoi creare due distribuzioni. Per ulteriori informazioni, consulta the section called “Abilita IPv6 (richieste del visualizzatore)” nell'argomento the section called “Tutte le impostazioni distribuzione”.

Esempi di dichiarazioni di policy per un URL firmato che utilizza una policy personalizzata

Gli esempi di dichiarazioni di policy seguenti mostrano il modo in cui controllare l'accesso a un determinato file, a tutti i file in una directory o a tutti i file associati a un ID di coppia di chiavi. Gli esempi mostrano inoltre come controllare l'accesso da un singolo indirizzo IP o da un intervallo di indirizzi IP e come impedire agli utenti di utilizzare l'URL firmato dopo una data e un'ora specificate.

Se copi e incolli uno di questi esempi, devi rimuovere gli eventuali spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni), sostituire i valori con i tuoi valori e includere un carattere di nuova riga dopo la parentesi graffa di chiusura (}).

Per ulteriori informazioni, consulta the section called “Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata”.

Argomenti

- Esempio di dichiarazione di policy: accesso a un file da un intervallo di indirizzi IP
- Esempio di dichiarazione di policy: accesso a tutti i file in una directory da un intervallo di indirizzi IP
- Esempio di dichiarazione di policy: accesso a tutti i file associati a un ID di coppia di chiavi da un indirizzo IP

Esempio di dichiarazione di policy: accesso a un file da un intervallo di indirizzi IP

L'esempio di policy personalizzata seguente in un URL firmato specifica che un utente può accedere al file `https://d111111abcdef8.cloudfront.net/game_download.zip` dagli indirizzi IP nell'intervallo `192.0.2.0/24` fino al 31 gennaio 2023 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Esempio di dichiarazione di policy: accesso a tutti i file in una directory da un intervallo di indirizzi IP

Il seguente esempio di politica personalizzata consente di creare un carattere firmato URLs per qualsiasi file nella `training` directory, come indicato dal carattere jolly asterisco (`*`) nel parametro. `Resource` Gli utenti possono accedere al file da un indirizzo IP incluso nell'intervallo `192.0.2.0/24` fino al 31 gennaio 2023 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
```

```
    ]
}
```

Ogni URL firmato con cui utilizzi questa policy, dispone di un URL che identifica un file specifico, ad esempio:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Esempio di dichiarazione di policy: accesso a tutti i file associati a un ID di coppia di chiavi da un indirizzo IP

La politica personalizzata di esempio seguente consente di creare un carattere firmato URLs per qualsiasi file associato a qualsiasi distribuzione, come indicato dal carattere jolly asterisco (*) nel parametro. `Resource` L'URL firmato deve utilizzare il protocollo `https://`, non `http://`. L'utente deve utilizzare l'indirizzo I `192.0.2.10/32`. (il valore `192.0.2.10/32` nella notazione CIDR fa riferimento a un singolo indirizzo IP, `192.0.2.10`). I file sono disponibili solo dal 31 gennaio 2023 10:00 UTC fino al 2 febbraio 2023 10:00 UTC:

```
{
    "Statement": [
       {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1675159200
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675332000
                }
            }
        }
    ]
}
```

Ogni URL firmato con cui utilizzate questa politica ha un URL che identifica un file specifico in una CloudFront distribuzione specifica, ad esempio:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

L'URL firmato include inoltre un ID di coppia di chiavi, che deve essere associato a un gruppo di chiavi attendibili nella distribuzione (d111111abcdef8.cloudfront.net) specificata nell'URL.

Creazione di una firma per un URL firmato che utilizza una policy personalizzata

La firma per un URL firmato che utilizza una policy personalizzata è una versione con firma, hash e codifica base64 della dichiarazione della policy. Per creare una firma per una policy personalizzata, procedi come indicato di seguito.

Per ulteriori informazioni ed esempi su come sottoporre a hashing, firmare e codificare la dichiarazione di policy, consulta:

- Comandi Linux e OpenSSL per la crittografia e la codifica base64
- Codice di esempio per la creazione di una firma per un URL firmato

Opzione 1: per creare una firma utilizzando una policy personalizzata

1. Utilizza la funzione hash SHA-1 e la chiave privata RSA o ECDSA generata per eseguire l'hashing e firmare la dichiarazione di policy JSON creata nella procedura Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata. Utilizza la versione della dichiarazione di policy che non include più spazi vuoti, ma che non è ancora stata codificata in base64.

   Per la chiave privata richiesta dalla funzione hash, utilizza una chiave privata la cui chiave pubblica si trova in un gruppo di chiavi attendibili attivo per la distribuzione.

   > **Note**
   >
   > Il metodo utilizzato per sottoporre a hashing e firmare la dichiarazione di policy dipende dalla piattaforma e dal linguaggio di programmazione. Per il codice di esempio, consulta Codice di esempio per la creazione di una firma per un URL firmato.

2. Rimuovi gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.

4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Aggiungi il valore risultante all'URL firmato dopo `&Signature=` e ritorna a Per creare un URL firmato utilizzando una policy personalizzata per completare il concatenamento delle parti dell'URL firmato.

Utilizzo di cookie firmati

CloudFront i cookie firmati consentono di controllare chi può accedere ai contenuti quando non si desidera modificare quelli correnti URLs o quando si desidera consentire l'accesso a più file con restrizioni, ad esempio tutti i file presenti nell'area riservata agli abbonati di un sito Web. Questo argomento descrive le considerazioni relative all'utilizzo di cookie firmati e come definire cookie firmati utilizzando policy predefinite e personalizzate.

Argomenti

- Scelta se utilizzare policy di accesso predefinite o personalizzate per cookie firmati
- Funzionamento di cookie firmati
- Prevenzione contro l'uso improprio di cookie firmati
- When CloudFront controlla la data e l'ora di scadenza in un cookie firmato
- Codice di esempio e strumenti di terza parte.
- Impostazione di cookie firmati mediante una policy di accesso predefinita
- Impostazione di cookie firmati che utilizzano una policy personalizzata
- Creazione di cookie firmati utilizzando PHP

Scelta se utilizzare policy di accesso predefinite o personalizzate per cookie firmati

Quando crei un cookie firmato, scrivi una dichiarazione di policy in formato JSON che specifica le restrizioni sul cookie firmato, ad esempio, il periodo di validità del cookie. Puoi utilizzare policy predefinite o policy personalizzate. La seguente tabella confronta questi due tipi di policy:

Descrizione	Policy predefinita	Policy personalizzata
Puoi riutilizzare la dichiarazione di policy per più file. Per riutilizzare la dichiarazione di policy, devi utilizzare caratteri jolly nell'oggetto `Resource`. Per ulteriori informazioni, consulta Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy personalizzata.)	No	Sì
Puoi specificare la data e l'ora in cui gli utenti possono iniziare ad accedere al tuo contenuto.	No	Sì (facoltativo)
Puoi specificare la data e l'ora in cui gli utenti non possono più accedere al tuo contenuto.	Sì	Sì
Puoi specificare l'indirizzo IP o l'intervallo di indirizzi IP degli utenti che possono accedere al tuo contenuto	No	Sì (facoltativo)

Per informazioni sulla creazione di cookie firmati utilizzando una policy predefinita, consulta Impostazione di cookie firmati mediante una policy di accesso predefinita.

Per informazioni sulla creazione di cookie firmati utilizzando una policy personalizzata, consulta Impostazione di cookie firmati che utilizzano una policy personalizzata.

Funzionamento di cookie firmati

Ecco una panoramica di come CloudFront configuri i cookie firmati e di come CloudFront reagisce quando un utente invia una richiesta che contiene un cookie firmato.

1. Nella tua CloudFront distribuzione, specifica uno o più gruppi di chiavi affidabili, che contengono le chiavi pubbliche che CloudFront possono essere utilizzate per verificare la firma dell'URL. Utilizzi le chiavi private corrispondenti per firmare il URLs.

   Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .
2. Sviluppa la tua applicazione per determinare se un utente deve avere accesso al tuo contenuto e, in caso affermativo, per inviare tre intestazioni `Set-Cookie` al visualizzatore (Ogni `Set-Cookie` intestazione può contenere solo una coppia nome-valore e un cookie CloudFront firmato richiede tre coppie nome-valore.) Devi inviare le intestazioni `Set-Cookie` al visualizzatore prima che il visualizzatore richieda il tuo contenuto privato. Se hai impostato un breve periodo di scadenza sul cookie, è possibile che tu intenda inviare tre ulteriori intestazioni `Set-Cookie` in risposta a richieste successive, in modo che l'utente continui ad avere accesso.

   In genere, la CloudFront distribuzione avrà almeno due comportamenti di cache, uno che non richiede l'autenticazione e uno che richiede l'autenticazione. La pagina di errore della parte protetta del sito include un redirector o un collegamento a una pagina di login.

   Se configuri la distribuzione per memorizzare nella cache i file basati sui cookie, CloudFront non memorizza nella cache file separati in base agli attributi dei cookie firmati.
3. Un utente accede al tuo sito Web e paga per il contenuto o soddisfa alcuni altri requisiti per l'accesso.
4. La tua applicazione restituisce le intestazioni `Set-Cookie` nella risposta e il visualizzatore archivia la coppia nome-valore.
5. L'utente richiede un file.

   Il browser dell'utente o un altro visualizzatore ottiene le coppie nome-valore della fase 4 e le aggiunge alla richiesta in un'intestazione `Cookie`. Questo è il cookie firmato.
6. CloudFront utilizza la chiave pubblica per convalidare la firma nel cookie firmato e per confermare che il cookie non è stato manomesso. Se la firma non è valida, la richiesta viene respinta.

   Se la firma nel cookie è valida, CloudFront esamina l'informativa contenuta nel cookie (o ne crea una se utilizzi una politica predefinita) per confermare che la richiesta è ancora valida. Ad esempio, se hai specificato una data e un'ora di inizio e fine per il cookie, CloudFront conferma che l'utente sta tentando di accedere ai tuoi contenuti durante il periodo di tempo in cui desideri consentire l'accesso.

Se la richiesta soddisfa i requisiti dell'informativa, CloudFront serve i contenuti come per i contenuti non soggetti a restrizioni: determina se il file è già presente nella cache edge, inoltra la richiesta all'origine se necessario e restituisce il file all'utente.

Prevenzione contro l'uso improprio di cookie firmati

Se specifichi il parametro `Domain` in un'intestazione `Set-Cookie`, specifica il valore più preciso possibile per ridurre l'accesso potenziale da parte di un utente con lo stesso nome di dominio radice. Ad esempio, ape.example.com è preferibile a example.com, soprattutto quando non controlli example.com. In questo modo, impedisci agli utenti di accedere al tuo contenuto a partire da www.example.com.

Per impedire questo tipo di attacco, procedi come segue:

- Escludi gli attributi di cookie `Expires` e `Max-Age`, in modo che l'intestazione `Set-Cookie` crei un cookie di sessione. I cookie di sessione vengono eliminati automaticamente quando l'utente chiude il browser, cosa che riduce la possibilità che qualcuno ottenga accesso non autorizzato al tuo contenuto.
- Includi l'attributo `Secure`, in modo che il cookie sia crittografato quando un visualizzatore lo include in una richiesta.
- Quando possibile, utilizza una policy personalizzata e includi l'indirizzo IP del visualizzatore.
- Nell'attributo `CloudFront-Expires`, specifica la scadenza ragionevole più corta basata sul periodo di tempo durante il quale intendi autorizzare gli utenti ad accedere al tuo contenuto.

When CloudFront controlla la data e l'ora di scadenza in un cookie firmato

Per determinare se un cookie firmato è ancora valido, CloudFront controlla la data e l'ora di scadenza nel cookie al momento della richiesta HTTP. Se un client inizia a scaricare un file di grandi dimensioni immediatamente prima della scadenza, il download viene completato anche se la scadenza avviene durante il download. Se la connessione TCP viene interrotta e il client tenta di riavviare il download dopo la scadenza, il download non riesce.

Se un client utilizza Range GETs per ottenere un file in parti più piccole, qualsiasi richiesta GET che si verifica dopo la scadenza avrà esito negativo. Per ulteriori informazioni su Range GETs, vedereCome CloudFront elabora le richieste parziali per un oggetto (intervalloGETs).

Codice di esempio e strumenti di terza parte.

Il codice di esempio per i contenuti privati mostra solo come creare la firma per signed URLs. Tuttavia, il processo per la creazione di una firma per un cookie firmato è molto simile, di conseguenza una gran parte del codice di esempio è ancora rilevante. Per ulteriori informazioni, consultare i seguenti argomenti:

- Creazione di una firma per URL utilizzando Perl
- Creazione di una firma per URL utilizzando PHP
- Crea una firma per URL utilizzando C# e .NET Framework
- Creazione di una firma per URL utilizzando Java

Impostazione di cookie firmati mediante una policy di accesso predefinita

Per definire un cookie firmato utilizzando una policy predefinita, completa la procedura descritta di seguito. Per creare la firma, consulta Creazione di una firma per un cookie firmato che utilizza una policy di accesso predefinita.

Definizione di un cookie firmato utilizzando una policy predefinita

1. Se utilizzi .NET o Java per creare cookie firmati e non hai riformattato la chiave privata per la coppia di chiavi dal formato default .pem a un formato compatibile con .NET o Java, fallo adesso. Per ulteriori informazioni, consulta Riformattazione della chiave privata (solo .NET e Java).
2. Programma la tua applicazione affinché invii tre intestazioni `Set-Cookie` a visualizzatori approvati. Sono necessarie tre intestazioni `Set-Cookie` in quanto ogni intestazione `Set-Cookie` può contenere una sola coppia nome-valore e un cookie firmato di CloudFront richiede tre coppie nome-valore. Le coppie nome-valore sono: `CloudFront-Expires`, `CloudFront-Signature` e `CloudFront-Key-Pair-Id`. I valori devono essere presenti sul visualizzatore prima che un utente effettui la prima richiesta per un file di cui intendi controllare l'accesso.

   > **Note**
   >
   > Come regola generale, ti consigliamo di escludere attributi `Expires` e `Max-Age`. In seguito all'esclusione degli attributi, il browser elimina il cookie quando l'utente chiude il browser e ciò riduce la possibilità che qualcuno ottenga accesso non autorizzato al tuo contenuto. Per ulteriori informazioni, consulta Prevenzione contro l'uso improprio di cookie firmati.

I nomi degli attributi di cookie fanno distinzione tra maiuscole e minuscole.

Le interruzioni di riga sono incluse solo per rendere gli attributi più leggibili.

```
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
```

(Facoltativo) **`Domain`**

Il nome di dominio per il file richiesto. Se non specifichi un attributo `Domain`, il valore di default è il nome di dominio nell'URL e viene applicato solo al nome di dominio specificato, non ai sottodomini. Se specifichi un attributo `Domain`, è applicabile anche ai sottodomini. Un punto all'inizio del nome di dominio (ad esempio `Domain=.example.com`) è facoltativo. Inoltre, se specifichi un attributo `Domain`, il nome di dominio nell'URL e il valore dell'attributo `Domain` devono corrispondere.

Puoi specificare il nome di dominio CloudFront assegnato alla tua distribuzione, ad esempio d111111abcdef8.cloudfront.net, ma non puoi specificare *.cloudfront.net per il nome di dominio.

Se desideri utilizzare un nome di dominio alternativo come example.com in, devi aggiungere il nome di dominio alternativo alla tua distribuzione indipendentemente dal fatto che tu specifichi l'attributo. URLs `Domain` Per ulteriori informazioni, consulta Nomi di dominio alternativi () CNAMEs nell'argomento Riferimento a tutte le impostazioni di distribuzione.

(Facoltativo) **`Path`**

Il percorso per il file richiesto. Se non si specifichi un attributo `Path`, il valore di default è il percorso nell'URL.

`Secure`

Richiede al visualizzatore di crittografare i cookie prima dell'invio di una richiesta. Ti consigliamo di inviare l'`Set-Cookie`intestazione tramite una connessione HTTPS per assicurarti che gli attributi del cookie siano protetti dagli attacchi. man-in-the-middle

`HttpOnly`

Definisce in che modo il browser (ove supportato) interagisce con il valore del cookie. Con`HttpOnly`, i valori dei cookie sono inaccessibili a. JavaScript Questa precauzione può aiutare a mitigare gli attacchi di cross-site scripting (XSS). Per ulteriori informazioni, consulta Utilizzo di cookie HTTP.

`CloudFront-Expires`

Specifica la data e l'ora di scadenza in formato Unix (in secondi) e UTC. Ad esempio, le 10:00 UTC del 1° gennaio 2026 vengono convertite in 1767290400 nel formato orario Unix.

Per usare il tempo epoch, specifica un numero intero a 64 bit per una data non posteriore a `9223372036854775807` (venerdì 11 aprile 2262 alle 23:47:16.854 UTC).

Per informazioni sul formato UTC, consulta RFC 3339, Date and Time on the Internet: Timestamps, https://tools.ietf.org/html/rfc3339.

`CloudFront-Signature`

Una versione con hash, firma e codifica base64 di una dichiarazione di policy JSON. Per ulteriori informazioni, consulta Creazione di una firma per un cookie firmato che utilizza una policy di accesso predefinita.

`CloudFront-Key-Pair-Id`

L'ID di una chiave pubblica, ad esempio,. CloudFront `K2JCJMDEHXQW5F` L'ID della chiave pubblica indica CloudFront quale chiave pubblica utilizzare per convalidare l'URL firmato. CloudFront confronta le informazioni contenute nella firma con quelle contenute nell'informativa per verificare che l'URL non sia stato manomesso.

Questa chiave pubblica deve appartenere a un gruppo di chiavi che sia un firmatario attendibile nella distribuzione. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

L'esempio seguente mostra le `Set-Cookie` intestazioni di un cookie firmato quando si utilizza il nome di dominio associato alla distribuzione in for your files: URLs

```
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'esempio seguente mostra le `Set-Cookie` intestazioni per un cookie firmato quando utilizzi il nome di dominio alternativo example.org nella cartella per i tuoi file: URLs

```
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
```

Se desideri utilizzare un nome di dominio alternativo come example.com in URLs, devi aggiungere il nome di dominio alternativo alla tua distribuzione indipendentemente dal fatto che tu specifichi l'attributo `Domain` Per ulteriori informazioni, consulta Nomi di dominio alternativi () CNAMEs nell'argomento Riferimento a tutte le impostazioni di distribuzione.

Creazione di una firma per un cookie firmato che utilizza una policy di accesso predefinita

Per creare la firma per un cookie firmato che utilizza una policy di accesso predefinita, completa le seguenti procedure.

Argomenti

Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy di accesso predefinita

Quando definisci un cookie firmato che utilizza una policy predefinita, l'attributo `CloudFront-Signature` è una versione con hash e firma di una dichiarazione di policy. Per i cookie firmati che utilizzano una policy predefinita, non includi la dichiarazione di policy nell'intestazione `Set-Cookie`, come avviene per i cookie firmati che utilizzano una policy personalizzata. Per creare una dichiarazione di policy, esegui la procedura descritta di seguito.

Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy predefinita

1. Crea la dichiarazione di policy utilizzando il formato JSON seguente e la codifica caratteri UTF-8. Includi tutta le punteggiatura e altri valori letterali esattamente come specificato. Per informazioni sui parametri `Resource` e `DateLessThan`, consulta Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy predefinita.

   ```
   {
       "Statement": [
           {
               "Resource": "base URL or stream name",
               "Condition": {
                   "DateLessThan": {
                       "AWS:EpochTime": ending date and time in Unix time format and
    UTC
                   }
               }
           }
       ]
   }
   ```

2. Rimuovi tutti gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla dichiarazione di policy. È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione.

Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy predefinita

Quando crei una dichiarazione di policy per una policy predefinita, specifichi i valori seguenti:

Risorsa

L'URL di base che include le eventuali stringhe di query, ad esempio:

`https://d111111abcdef8.cloudfront.net/images/horizon.jpg?size=large&license=yes`

Puoi specificare un solo valore per `Resource`.

Tieni presente quanto segue:

- Protocollo: il valore deve iniziare con `http://` o `https://`.
- Parametri di stringa di query: se non hai parametri di stringa di query, ometti il punto di domanda.
- Nomi di dominio alternativi: se specifichi un nome di dominio alternativo (CNAME) nell'URL, devi specificarlo quando fai riferimento al file nella pagina Web o nell'applicazione. Non specificare l'URL Amazon S3 per il file.

DateLessThan

La data e l'ora di scadenza per l'URL in formato Unix (in secondi) e UTC. Non racchiudere il valore tra virgolette.

Ad esempio, 16 marzo 2015 10:00 UTC viene convertito in 1426500000 nel formato Unix.

Questo valore deve corrispondere al valore dell'attributo `CloudFront-Expires` nell'intestazione `Set-Cookie`. Non racchiudere il valore tra virgolette.

Per ulteriori informazioni, consulta When CloudFront controlla la data e l'ora di scadenza in un cookie firmato.

Esempio di dichiarazione di policy per una policy predefinita

Quando utilizzi l'esempio di dichiarazione di policy seguente in un cookie firmato, un utente può accedere al file `https://d111111abcdef8.cloudfront.net/horizon.jpg` fino al 16 marzo 2015 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1426500000
                }
            }
        }
    ]
}
```

Firma di una dichiarazione di policy per creare una firma per un cookie firmato che utilizza una policy di accesso predefinita

Per creare il valore per l'attributo `CloudFront-Signature` in un'intestazione `Set-Cookie`, sottoponi a hashing e firmi la dichiarazione di policy che hai creato in Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy predefinita.

Per ulteriori informazioni ed esempi su come sottoporre a hashing, firmare e codificare la dichiarazione di policy, consulta i seguenti argomenti:

- Comandi Linux e OpenSSL per la crittografia e la codifica base64
- Codice di esempio per la creazione di una firma per un URL firmato

Creazione di una firma per un cookie firmato che utilizza una policy predefinita

1. Utilizza la funzione hash SHA-1 e RSA per sottoporre a hashing e firmare la dichiarazione di policy che hai creato nella procedura Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy predefinita. Utilizza la versione della dichiarazione di policy che non include più spazi vuoti.

   Per la chiave privata richiesta dalla funzione hash, utilizza una chiave privata la cui chiave pubblica si trova in un gruppo di chiavi attendibili attivo per la distribuzione.

> **Note**
>
> Il metodo utilizzato per sottoporre a hashing e firmare la dichiarazione di policy dipende dalla piattaforma e dal linguaggio di programmazione. Per il codice di esempio, consulta Codice di esempio per la creazione di una firma per un URL firmato.

2. Rimuovi gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.
4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Includi il valore risultante nell'intestazione `Set-Cookie` per la coppia nome-valore `CloudFront-Signature`. Quindi ritorna a Definizione di un cookie firmato utilizzando una policy predefinita e aggiungi l'intestazione `Set-Cookie` per `CloudFront-Key-Pair-Id`.

Impostazione di cookie firmati che utilizzano una policy personalizzata

Per definire un cookie firmato che utilizza una policy personalizzata, procedi come indicato di seguito.

Impostazione di un cookie firmato che utilizza una policy personalizzata

1. Se stai usando .NET o Java per creare un file firmato URLs e se non hai riformattato la chiave privata per la tua coppia di chiavi dal formato.pem predefinito a un formato compatibile con.NET o con Java, fallo ora. Per ulteriori informazioni, consulta Riformattazione della chiave privata (solo .NET e Java).

2. Programma la tua applicazione affinché invii tre intestazioni `Set-Cookie` a visualizzatori approvati. Sono necessarie tre `Set-Cookie` intestazioni perché ogni `Set-Cookie` intestazione può contenere solo una coppia nome-valore e un cookie firmato richiede tre coppie nome-valore. CloudFront Le coppie nome-valore sono: `CloudFront-Policy`, `CloudFront-Signature` e `CloudFront-Key-Pair-Id`. I valori devono essere presenti sul visualizzatore prima che un utente effettui la prima richiesta per un file di cui intendi controllare l'accesso.

   > **Note**
   >
   > Come regola generale, ti consigliamo di escludere attributi `Expires` e `Max-Age`. Ciò comporta l'eliminazione del cookie da parte del browser quando l'utente chiude il browser, cosa che riduce la possibilità che qualcuno ottenga accesso non autorizzato al tuo contenuto. Per ulteriori informazioni, consulta Prevenzione contro l'uso improprio di cookie firmati.

   I nomi degli attributi di cookie fanno distinzione tra maiuscole e minuscole.

   Le interruzioni di riga sono incluse solo per rendere gli attributi più leggibili.

```
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
```

(Facoltativo) **`Domain`**

Il nome di dominio per il file richiesto. Se non specifichi un attributo `Domain`, il valore di default è il nome di dominio nell'URL e viene applicato solo al nome di dominio specificato, non ai sottodomini. Se specifichi un attributo `Domain`, è applicabile anche ai sottodomini. Un punto all'inizio del nome di dominio (ad esempio `Domain=.example.com`) è facoltativo. Inoltre, se specifichi un attributo `Domain`, il nome di dominio nell'URL e il valore dell'attributo `Domain` devono corrispondere.

Puoi specificare il nome di dominio CloudFront assegnato alla tua distribuzione, ad esempio d111111abcdef8.cloudfront.net, ma non puoi specificare *.cloudfront.net per il nome di dominio.

Se desideri utilizzare un nome di dominio alternativo come example.com in, devi aggiungere il nome di dominio alternativo alla tua distribuzione indipendentemente dal fatto che tu specifichi l'attributo. URLs `Domain` Per ulteriori informazioni, consulta Nomi di dominio alternativi () CNAMEs nell'argomento Riferimento a tutte le impostazioni di distribuzione.

(Facoltativo) **`Path`**

Il percorso per il file richiesto. Se non si specifichi un attributo `Path`, il valore di default è il percorso nell'URL.

`Secure`

Richiede al visualizzatore di crittografare i cookie prima dell'invio di una richiesta. Ti consigliamo di inviare l'`Set-Cookie`intestazione tramite una connessione HTTPS per assicurarti che gli attributi del cookie siano protetti dagli attacchi. man-in-the-middle

`HttpOnly`

Richiede al visualizzatore di inviare il cookie solo nelle richieste HTTP o HTTPS.

`CloudFront-Policy`

La dichiarazione di policy in formato JSON, con spazi vuoti rimossi e codifica base64. Per ulteriori informazioni, consulta Creazione di una firma per un cookie firmato che utilizza una policy personalizzata.

La dichiarazione di policy controlla l'accesso che un cookie firmato concede a un utente. Include i file a cui l'utente può accedere, una data e un'ora di scadenza, una data e un'ora facoltative in cui l'URL diventa valido e un indirizzo IP facoltativo o un intervallo di indirizzi IP a cui è consentito accedere al file.

`CloudFront-Signature`

Una versione con hash, firma e codifica base64 della dichiarazione di policy JSON. Per ulteriori informazioni, consulta Creazione di una firma per un cookie firmato che utilizza una policy personalizzata.

`CloudFront-Key-Pair-Id`

L'ID di una chiave CloudFront pubblica, ad esempio,`K2JCJMDEHXQW5F`. L'ID della chiave pubblica indica CloudFront quale chiave pubblica utilizzare per convalidare l'URL firmato. CloudFrontconfronta le informazioni contenute nella firma con quelle contenute nell'informativa per verificare che l'URL non sia stato manomesso.

Questa chiave pubblica deve appartenere a un gruppo di chiavi che sia un firmatario attendibile nella distribuzione. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare cookie firmati e firmati URLs .

Intestazioni **`Set-Cookie`** di esempio per policy personalizzate

Vedi i seguenti esempi di coppie di intestazioni `Set-Cookie`.

Se desideri utilizzare un nome di dominio alternativo come example.org in URLs, devi aggiungere il nome di dominio alternativo alla tua distribuzione indipendentemente dal fatto che tu specifichi l'attributo. `Domain` Per ulteriori informazioni, consulta Nomi di dominio alternativi () CNAMEs nell'argomento Riferimento a tutte le impostazioni di distribuzione.

Example Esempio 1

Puoi utilizzare le `Set-Cookie` intestazioni per un cookie firmato quando utilizzi il nome di dominio associato alla tua distribuzione in for your files. URLs

```
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 Esempio 2

Puoi utilizzare le `Set-Cookie` intestazioni per un cookie firmato quando utilizzi un nome di dominio alternativo (example.org) nella cartella per i tuoi file. URLs

```
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 Esempio 3

Puoi utilizzare le coppie di `Set-Cookie` intestazioni per una richiesta firmata quando utilizzi il nome di dominio associato alla tua distribuzione in for your files. URLs

```
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 Esempio 4

Puoi utilizzare le coppie di `Set-Cookie` intestazioni per una richiesta firmata quando utilizzi un nome di dominio alternativo (example.org) associato alla tua distribuzione nella sezione per i tuoi file. URLs

```
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
```

Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy personalizzata

Per creare una dichiarazione di policy per una policy personalizzata, completa i seguenti passaggi. Per vari esempi di dichiarazioni di policy che controllano l'accesso a file in vari modi, consulta Esempi di dichiarazioni di policy per un cookie firmato che utilizza una policy personalizzata.

Creazione di una dichiarazione di policy per un cookie firmato che utilizza una policy personalizzata

1. Crea la dichiarazione di policy utilizzando il formato JSON seguente.

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

Tieni presente quanto segue:

- Puoi includere solo una dichiarazione.
- Utilizza la codifica caratteri UTF-8.
- Includi tutta le punteggiatura e nomi di parametro esattamente come specificato. Le abbreviazioni per i nomi di parametro non sono accettate.
- L'ordine dei parametri nella sezione `Condition` non è rilevante.

- Per informazioni sui valori per `Resource`, `DateLessThan`, `DateGreaterThan` e `IpAddress`, consulta Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy personalizzata.

2. Rimuovi tutti gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla dichiarazione di policy. È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione.
3. Codifica la dichiarazione di policy utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.
4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Includi il valore risultante nella tua intestazione `Set-Cookie` dopo `CloudFront-Policy=`.
6. Crea una firma per l'intestazione `Set-Cookie` per `CloudFront-Signature` sottoponendo a hashing, firmando e codificando in base64 la dichiarazione di policy. Per ulteriori informazioni, consulta Creazione di una firma per un cookie firmato che utilizza una policy personalizzata.

Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy personalizzata

Quando crei una dichiarazione di policy per una policy personalizzata, specifichi i valori seguenti.

Risorsa

L'URL di base che include le eventuali stringhe di query:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

> **Important**
>
> Se ometti il parametro `Resource`, gli utenti possono accedere a tutti i file associati a qualsiasi distribuzione associata alla coppia di chiavi che utilizzi per creare l'URL firmato.

Puoi specificare un solo valore per `Resource`.

Tieni presente quanto segue:

- Protocollo: il valore deve iniziare con `http://` o `https://`.
- Parametri di stringa di query: se non hai parametri di stringa di query, ometti il punto di domanda.
- Caratteri jolly: puoi utilizzare il carattere jolly che corrisponde a zero o più caratteri (*) o il carattere jolly che corrisponde esattamente a un carattere (?) in qualsiasi punto della stringa. Ad esempio, il valore:

  ```
  https://d111111abcdef8.cloudfront.net/*game_download.zip*
  ```

  includerebbe (ad esempio) i seguenti file:

  - `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`
- Nomi di dominio alternativi: se specifichi un nome di dominio alternativo (CNAME) nell'URL, devi specificarlo quando fai riferimento al file nella pagina Web o nell'applicazione. Non specificare l'URL Amazon S3 per il file.

DateLessThan

La data e l'ora di scadenza per l'URL in formato Unix (in secondi) e UTC. Non racchiudere il valore tra virgolette.

Ad esempio, 16 marzo 2015 10:00 UTC viene convertito in 1426500000 nel formato Unix.

Per ulteriori informazioni, consulta When CloudFront controlla la data e l'ora di scadenza in un cookie firmato.

DateGreaterThan (Facoltativo)

Una data e un'ora di inizio (facoltative) per l'URL in formato Unix (in secondi) e UTC. Agli utenti non è consentito accedere al file prima o in corrispondenza della data e ora specificate. Non racchiudere il valore tra virgolette.

IpAddress (Opzionale)

L'indirizzo IP del client che esegue la richiesta GET. Tieni presente quanto segue:

- Per consentire a qualsiasi indirizzo IP di accedere al file, ometti il parametro `IpAddress`.
- Puoi specificare un indirizzo IP o un intervallo di indirizzi IP. Ad esempio, non puoi definire la policy per consentire l'accesso se l'indirizzo IP del client è in uno dei due intervalli distinti.
- Per consentire l'accesso da un singolo indirizzo IP, specifica:

  `"`*`IPv4 IP address`*`/32"`
- È necessario specificare gli intervalli di indirizzi IP nel formato IPv4 CIDR standard (ad esempio,`192.0.2.0/24`). Per ulteriori informazioni, consulta RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, https://tools.ietf.org/html/rfc4632.

  > **Important**
  >
  > Gli indirizzi IP in IPv6 formato, ad esempio 2001:0 db 8:85 a3: :8a2e: 0370:7334, non sono supportati.

  Se utilizzi una politica personalizzata che include, non abilitarla per la distribuzione. `IpAddress` IPv6 Se desideri limitare l'accesso ad alcuni contenuti in base all'indirizzo IP e IPv6 alle richieste di supporto per altri contenuti, puoi creare due distribuzioni. Per ulteriori informazioni, consulta Abilita IPv6 (richieste del visualizzatore) nell'argomento Riferimento a tutte le impostazioni di distribuzione.

Esempi di dichiarazioni di policy per un cookie firmato che utilizza una policy personalizzata

Gli esempi di dichiarazioni di policy seguenti mostrano il modo in cui controllare l'accesso a un determinato file, a tutti i file in una directory o a tutti i file associati a un ID di coppia di chiavi. Gli esempi mostrano inoltre come controllare l'accesso da un singolo indirizzo IP o da un intervallo

di indirizzi IP e come impedire agli utenti di utilizzare il cookie firmato dopo una data e un'ora specificate.

Se copi e incolli uno di questi esempi, devi rimuovere gli eventuali spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni), sostituire i valori con i tuoi valori e includere un carattere di nuova riga dopo la parentesi graffa di chiusura (}).

Per ulteriori informazioni, consulta Valori da specificare in una dichiarazione di policy per cookie firmati che utilizzano una policy personalizzata.

Argomenti

- Esempio di dichiarazione di policy: accesso a un file da un intervallo di indirizzi IP
- Esempio di dichiarazione di policy: accesso a tutti i file in una directory da un intervallo di indirizzi IP
- Esempio di dichiarazione di policy: accesso a tutti i file associati a un ID di coppia di chiavi da un indirizzo IP

Esempio di dichiarazione di policy: accesso a un file da un intervallo di indirizzi IP

L'esempio seguente di policy personalizzata in un cookie firmato specifica che un utente può accedere al file `https://d111111abcdef8.cloudfront.net/game_download.zip` dagli indirizzi IP nell'intervallo `192.0.2.0/24` fino al 1° gennaio 2013 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Esempio di dichiarazione di policy: accesso a tutti i file in una directory da un intervallo di indirizzi IP

L'esempio di policy personalizzata seguente consente di creare cookie firmati per qualsiasi file nella directory `training`, come indicato dal carattere jolly * nel parametro `Resource`. Gli utenti possono accedere al file da un indirizzo IP incluso nell'intervallo `192.0.2.0/24` fino al 1° gennaio 2013 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Ogni cookie firmato in cui utilizzi questa policy include un URL di base che identifica un file specifico, ad esempio:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Esempio di dichiarazione di policy: accesso a tutti i file associati a un ID di coppia di chiavi da un indirizzo IP

L'esempio di policy personalizzata seguente ti consente di definire cookie firmati per qualsiasi file associato a qualsiasi distribuzione, come indicato dal carattere jolly * nel parametro `Resource`. L'utente deve utilizzare l'indirizzo I `192.0.2.10/32`. (il valore `192.0.2.10/32` nella notazione CIDR fa riferimento a un singolo indirizzo IP, `192.0.2.10`). I file sono disponibili solo dal 1° gennaio 2013 10:00 UTC fino al 2 gennaio 2013 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://*",
```

```
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1767290400
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767376800
                }
            }
        }
    ]
}
```

Ogni cookie firmato in cui si utilizza questa politica include un URL di base che identifica un file specifico in una CloudFront distribuzione specifica, ad esempio:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Il cookie firmato include inoltre un ID di coppia di chiavi, che deve essere associato a un firmatario attendibile nella distribuzione (d111111abcdef8.cloudfront.net) specificato nell'URL di base.

Creazione di una firma per un cookie firmato che utilizza una policy personalizzata

La firma di un cookie firmato che utilizza una policy personalizzata è una versione con hash, firma e codifica base64 della dichiarazione di policy.

Per ulteriori informazioni ed esempi su come sottoporre a hashing, firmare e codificare la dichiarazione di policy, consulta:

- Comandi Linux e OpenSSL per la crittografia e la codifica base64
- Codice di esempio per la creazione di una firma per un URL firmato

Creazione di una firma per un cookie firmato utilizzando una policy personalizzata

1. Utilizza la funzione hash SHA-1 e RSA per sottoporre a hashing e firmare la dichiarazione di policy JSON che hai creato nella procedura Creazione di una dichiarazione di policy per un URL firmato che utilizza una policy personalizzata. Utilizza la versione della dichiarazione di policy che non include più spazi vuoti, ma che non è ancora stata codificata in base64.

Per la chiave privata richiesta dalla funzione hash, utilizza una chiave privata la cui chiave pubblica si trova in un gruppo di chiavi attendibili attivo per la distribuzione.

> **Note**
>
> Il metodo utilizzato per sottoporre a hashing e firmare la dichiarazione di policy dipende dalla piattaforma e dal linguaggio di programmazione. Per il codice di esempio, consulta Codice di esempio per la creazione di una firma per un URL firmato.

2. Rimuovi gli spazi vuoti (inclusi i caratteri di nuova riga e le tabulazioni) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, vedere Sezione 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions), parte prima: Formato dei corpi dei messaggi Internet.
4. Sostituisci i caratteri non validi nella stringa di query dell'URL con caratteri validi. La tabella seguente elenca i caratteri validi e non validi.

Sostituisci questi caratteri non validi	Con questi caratteri validi
+	- (trattino)
=	_ (carattere di sottolineatura)
/	~ (tilde)

5. Includi il valore risultante nell'intestazione `Set-Cookie` per la coppia nome-valore `CloudFront-Signature=` e ritorna a Impostazione di un cookie firmato che utilizza una policy personalizzata per aggiungere l'intestazione `Set-Cookie` per `CloudFront-Key-Pair-Id`.

Creazione di cookie firmati utilizzando PHP

Il seguente esempio di codice è simile all'esempio in Creazione di una firma per URL utilizzando PHP in quanto crea un collegamento a un video. Tuttavia, invece di firmare l'URL nel codice, questo esempio firma i cookie con la funzione `create_signed_cookies()`. Il player lato client utilizza i cookie per autenticare ogni richiesta alla distribuzione. CloudFront

Questo approccio è utile per lo streaming di contenuti, come HTTP Live Streaming (HLS) o Dynamic Adaptive Streaming over HTTP (DASH), in cui il client deve effettuare più richieste per recuperare il manifesto, i segmenti e gli asset di riproduzione correlati. Utilizzando i cookie firmati, il client può autenticare ogni richiesta senza dover generare un nuovo URL firmato per ogni segmento.

> **Note**
>
> - La creazione di una firma URL è solo una parte del processo di gestione di contenuti privati tramite cookie firmati. Per ulteriori informazioni, consulta Utilizzo di cookie firmati.

Argomenti

- Creazione della firma RSA SHA-1
- Creazione di cookie firmati
- Codice completo

Nelle sezioni seguenti, l'esempio di codice viene suddiviso in singole parti. Di seguito è riportato l'esempio di codice completo.

Creazione della firma RSA SHA-1

In questo codice di esempio vengono eseguite le seguenti operazioni:

1. La funzione `rsa_sha1_sign` esegue l'hashing e firma la dichiarazione di policy. Gli argomenti richiesti sono una dichiarazione di policy e la chiave privata che corrisponde a una chiave pubblica appartenente a un gruppo di chiavi attendibili per la distribuzione.
2. Successivamente, la funzione `url_safe_base64_encode` crea una versione URL-safe della firma.

```
function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
```

```
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

Creazione di cookie firmati

I costrutti di codice seguenti creano i cookie firmati, utilizzando i seguenti attributi dei cookie: `CloudFront-Expires`, `CloudFront-Signature` e `CloudFront-Key-Pair-Id`. Il codice utilizza una policy personalizzata.

```
function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null) {
   $policy = array(
       'Statement' => array(
           array(
               'Resource' => $resource,
               'Condition' => array(
                   'DateLessThan' => array('AWS:EpochTime' => $expires)
               )
           )
       )
   );

   if ($client_ip) {
       $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
   }

   $policy = json_encode($policy);
   $encoded_policy = url_safe_base64_encode($policy);
   $signature = rsa_sha1_sign($policy, $private_key_filename);
   $encoded_signature = url_safe_base64_encode($signature);

   return array(
       'CloudFront-Policy' => $encoded_policy,
```

```
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );
}
```

Per ulteriori informazioni, consulta Impostazione di cookie firmati che utilizzano una policy personalizzata.

Codice completo

Il codice di esempio seguente fornisce una dimostrazione completa della creazione di cookie CloudFront firmati con PHP. Puoi scaricare l'esempio completo dal file demo-php.zip.

Nell'esempio seguente, è possibile modificare l'`$policy Condition`elemento per consentire sia gli intervalli di indirizzi che gli intervalli IPv4 di IPv6 indirizzi. Per un esempio, IPv6 consulta Using address in IAM policies nella Amazon Simple Storage Service User Guide.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}

function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null) {
    $policy = array(
        'Statement' => array(
            array(
```

```
                'Resource' => $resource,
                'Condition' => array(
                    'DateLessThan' => array('AWS:EpochTime' => $expires)
                )
            )
        )
    );

    if ($client_ip) {
        $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
    }

    $policy = json_encode($policy);
    $encoded_policy = url_safe_base64_encode($policy);
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    $encoded_signature = url_safe_base64_encode($signature);

    return array(
        'CloudFront-Policy' => $encoded_policy,
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );
}



$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';
$base_url = 'https://d1234.cloudfront.net';

$expires = time() + 3600; // 1 hour from now

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];


// For HLS manifest and segments (using wildcard)
$hls_resource = $base_url . '/sign/*';
$signed_cookies = create_signed_cookies($hls_resource, $private_key_filename,
 $key_pair_id, $expires, $client_ip);
```

```
// Set the cookies
$cookie_domain = parse_url($base_url, PHP_URL_HOST);
foreach ($signed_cookies as $name => $value) {
    setcookie($name, $value, $expires, '/', $cookie_domain, true, true);
}

?>

<!DOCTYPE html>
<html>
<head>
    <title>CloudFront Signed HLS Stream with Cookies</title>
</head>
<body>
    <h1>Amazon CloudFront Signed HLS Stream with Cookies</h1>
    <h2>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h2>

    <div id='hls-video'>
        <video id="video" width="640" height="360" controls></video>
    </div>

    <script src="https://cdn.jsdelivr.net/npm/hls.js@latest"></script>
    <script>
        var video = document.getElementById('video');
        var manifestUrl = '<?php echo $base_url; ?>/sign/manifest.m3u8';

        if (Hls.isSupported()) {
            var hls = new Hls();
            hls.loadSource(manifestUrl);
            hls.attachMedia(video);
        }
        else if (video.canPlayType('application/vnd.apple.mpegurl')) {
            video.src = manifestUrl;
        }
    </script>
</body>
</html>
```

Invece di utilizzare cookie firmati, puoi utilizzare cookie firmati URLs. Per ulteriori informazioni, consulta Creazione di una firma per URL utilizzando PHP.

Comandi Linux e OpenSSL per la crittografia e la codifica base64

Puoi utilizzare il seguente comando della riga di comando Linux e OpenSSL per sottoporre a hashing e firmare la dichiarazione di policy, codificare in base64 la firma e sostituire i caratteri non validi nei parametri di stringa di query degli URL con caratteri validi.

Per informazioni su OpenSSL, consulta https://www.openssl.org.

```
cat policy | tr -d "\n" | tr -d " \t\n\r" | openssl sha1 -sign private_key.pem |
 openssl base64 -A | tr -- '+=/' '-_~'
```

Nel precedente comando:

- `cat` legge il file `policy`.
- `tr -d "\n" | tr -d " \t\n\r"` rimuove gli spazi e il carattere di nuova riga aggiunti da `cat`.
- OpenSSL esegue l'hashing del file utilizzando SHA-1 e lo firma utilizzando il file di chiave privata `private_key.pem`. La firma chiave privata può essere RSA 2048 o ECDSA 256.
- OpenSSL codifica in base64 la dichiarazione di policy con hash e firmata.
- `tr` sostituisce i caratteri non validi nei parametri di stringa di query dell'URL con caratteri validi.

Per ulteriori codici di esempio che illustrano la creazione di una firma, consulta Codice di esempio per la creazione di una firma per un URL firmato.

Codice di esempio per la creazione di una firma per un URL firmato

Questa sezione include esempi di applicazioni scaricabili che dimostrano come creare firme per signed. URLs Vengono forniti esempi in Perl, PHP, C# e Java. È possibile utilizzare uno qualsiasi degli esempi per creare firme firmate. URLs Lo script Perl viene eseguito su piattaforme Linux e macOS. L'esempio PHP funzionerà su qualsiasi server che esegue PHP. L'esempio C# utilizza .NET Framework.

Ad esempio, codice in JavaScript (Node.js), consulta Creazione di Amazon CloudFront Signed URLs in Node.js sul blog AWS degli sviluppatori.

Per un esempio di codice in Python, consulta Generare un URL firmato per Amazon CloudFront nell'API di riferimento dell'AWS SDK for Python (Boto3) e questo codice di esempio nel repository Boto3. GitHub

Argomenti

Creazione di una firma per URL utilizzando Perl

Questa sezione include uno script Perl per Linux/Mac piattaforme che è possibile utilizzare per creare la firma per contenuti privati. Per creare la firma, esegui lo script con argomenti della riga di comando che specificano l' CloudFront URL, il percorso della chiave privata del firmatario, l'ID della chiave e una data di scadenza dell'URL. Lo strumento può anche decodificare i segni firmati. URLs

> **Note**
>
> La creazione di una firma per URL è solo una parte del processo di distribuzione di contenuto privato mediante un URL firmato. Per ulteriori informazioni sul end-to-end processo, vedereUsa firmato URLs.

Argomenti

Origine dello script Perl per la creazione di un URL firmato

Il seguente codice sorgente Perl può essere usato per creare un URL firmato per CloudFront. I commenti del codice includono informazioni sulle opzioni della riga di comando e le caratteristiche dello strumento.

```
#!/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;
```

Creazione di una firma per URL utilizzando PHP

Qualsiasi server Web che esegue PHP può utilizzare questo codice di esempio PHP per creare dichiarazioni politiche e firme per distribuzioni private. CloudFront L'esempio completo crea una pagina Web funzionante con collegamenti URL firmati che riproducono uno streaming video utilizzando lo streaming. CloudFront Puoi scaricare l’esempio completo dal file demo-php.zip.

> **Note**
>
> - La creazione di una firma per URL è solo una parte del processo di distribuzione di contenuto privato mediante un URL firmato. Per ulteriori informazioni sull'intero processo, consulta Usa firmato URLs.
> - È inoltre possibile creare un URLs file firmato utilizzando la `UrlSigner` classe in. AWS SDK per PHP Per ulteriori informazioni, vedete Class UrlSigner nel AWS SDK per PHP API Reference.

Argomenti

- Creazione della firma RSA SHA-1
- Creazione di una policy di accesso predefinita
- Creare una policy personalizzata
- Esempio di codice completo

Nelle sezioni seguenti, l'esempio di codice viene suddiviso in singole parti. Di seguito è riportato il Esempio di codice completo completo.

Creazione della firma RSA SHA-1

In questo codice di esempio vengono eseguite le seguenti operazioni:

- La funzione `rsa_sha1_sign` esegue l'hashing e firma la dichiarazione di policy. Gli argomenti richiesti sono una dichiarazione di policy e la chiave privata che corrisponde a una chiave pubblica appartenente a un gruppo di chiavi attendibili per la distribuzione.
- Successivamente, la funzione `url_safe_base64_encode` crea una versione URL-safe della firma.

```
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);
}
```

Il seguente frammento di codice utilizza le funzioni `get_canned_policy_stream_name()` e `get_custom_policy_stream_name()` crea una politica predefinita e personalizzata. CloudFront utilizza le politiche per creare l'URL per lo streaming del video, inclusa la specifica dell'ora di scadenza.

Puoi quindi utilizzare una policy di accesso predefinita o una policy personalizzata per determinare come gestire l'accesso ai contenuti. Per ulteriori informazioni su quale scegliere, consulta la sezione Decidi di utilizzare politiche predefinite o personalizzate per la firma URLs.

Creazione di una policy di accesso predefinita

Il codice di esempio seguente crea una dichiarazione di policy predefinita per la firma.

> **Note**
>
> La `$expires` variabile è un date/time timbro che deve essere un numero intero, non una stringa.

```
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
    return $stream_name;
}
```

Per ulteriori informazioni sulle policy predefinite, consulta Creazione di un URL firmato utilizzando una policy di accesso predefinita.

Creare una policy personalizzata

Il codice di esempio seguente crea una dichiarazione di policy personalizzata per la firma.

```
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
    return $stream_name;
}
```

Per ulteriori informazioni sulle policy personalizzate, consulta Creazione di un URL firmato utilizzando una policy personalizzata.

Esempio di codice completo

Il codice di esempio seguente fornisce una dimostrazione completa della creazione di CloudFront signed URLs with PHP. Puoi scaricare l'esempio completo dal file demo-php.zip.

Nell'esempio seguente, è possibile modificare l'`$policyCondition`elemento per consentire sia gli intervalli di indirizzi che gli intervalli IPv4 di IPv6 indirizzi. Per un esempio, IPv6consulta Using address in IAM policies nella Amazon Simple Storage Service User Guide.

```
<?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 .= $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 .= $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 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
    return $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
    return $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';

// Make sure you have "Restrict viewer access" enabled on this path behaviour and using
 the above Trusted key groups (recommended).
$video_path = 'https://example.com/secure/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);

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
$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>
</head>

<body>
    <h1>Amazon CloudFront</h1>
    <h2>Canned Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?></h3>
    <br />

    <div id='canned'>The canned policy video will be here: <br>

        <video width="640" height="360" autoplay muted controls>
        <source src="<?php echo $canned_policy_stream_name; ?>" type="video/mp4">
        Your browser does not support the video tag.
        </video>
    </div>

    <h2>Custom Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h3>
    <div id='custom'>The custom policy video will be here: <br>

         <video width="640" height="360" autoplay muted controls>
         <source src="<?php echo $custom_policy_stream_name; ?>" type="video/mp4">
         Your browser does not support the video tag.
        </video>
    </div>

</body>

</html>
```

Per ulteriori esempi di firme URL, consulta i seguenti argomenti:

- Creazione di una firma per URL utilizzando Perl
- Crea una firma per URL utilizzando C# e .NET Framework
- Creazione di una firma per URL utilizzando Java

Invece di utilizzare signed URLs per creare la firma, puoi utilizzare cookie firmati. Per ulteriori informazioni, consulta Creazione di cookie firmati utilizzando PHP.

Crea una firma per URL utilizzando C# e .NET Framework

Gli esempi in C# in questa sezione implementano un'applicazione di esempio che dimostra come creare le firme per le distribuzioni CloudFront private utilizzando istruzioni di policy predefinite e personalizzate. Gli esempi includono funzioni utility basate sul AWS SDK per .NET che può rivelarsi utile nelle applicazioni .NET.

È inoltre possibile creare cookie firmati URLs e firmati utilizzando. SDK per .NET Nella Documentazione di riferimento delle API di SDK per .NET , consulta i seguenti argomenti:

- Firmato URLs: AmazonCloudFrontUrlSigner
- Cookie firmati — AmazonCloudFrontCookieSigner

Per scaricare il codice, consulta Signature Code in C#.

> **Note**
>
> - Le classi `AmazonCloudFrontUrlSigner` e `AmazonCloudFrontCookieSigner` sono state spostate in un pacchetto separato. Per ulteriori informazioni sul loro utilizzo, consulta CookieSigner e UrlSigner nella AWS SDK per .NET (V4) Developer Guide.
> - La creazione di una firma per URL è solo una parte del processo di distribuzione di contenuto privato mediante un URL firmato. Per ulteriori informazioni, consulta Usa firmato URLs. Per ulteriori informazioni sull'utilizzo di cookie firmati, consulta Utilizzo di cookie firmati.

Utilizzo di una chiave RSA in .NET Framework

Per utilizzare una chiave RSA in.NET Framework, è necessario convertire il file.pem AWS fornito nel formato XML utilizzato da .NET Framework.

Dopo la conversione, il file di chiave privata RSA è nel seguente formato:

Example : chiave privata RSA nel formato .NET Framework XML

```
<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>
```

Metodo di firma di policy predefinita in C#

Il codice C# esposto di seguito crea un URL firmato che utilizza una policy predefinita eseguendo la procedura seguente:

- Crea una dichiarazione di policy.
- Esegue l'hash della dichiarazione politica utilizzando SHA1 e firma il risultato utilizzando RSA e la chiave privata la cui chiave pubblica corrispondente si trova in un gruppo di chiavi attendibili.
- Codifica in base64 la dichiarazione di policy con firma e hash e sostituisce i caratteri speciali per rendere sicura la stringa da utilizzare come parametro di richiesta URL.
- Concatena i valori.

Per l'implementazione completa, vedi l'esempio in Signature Code in C#.

> **Note**
>
> `keyId`Viene restituito quando si carica una chiave pubblica su. CloudFront Per ulteriori informazioni, consulta
>
> 6
>
> &Key-Pair-Id.

Example : metodo di firma di policy di accesso predefinita in 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;
    }
}
```

Metodo di firma di policy personalizzata in C#

Il codice C# esposto di seguito crea un URL firmato che utilizza una policy personalizzata mediante le seguenti operazioni:

1. Crea una dichiarazione di policy.
2. Codifica in base64 la dichiarazione di policy e sostituisce caratteri speciali per rendere sicura la stringa da utilizzare come parametro di richiesta URL.
3. Esegue l'hash della dichiarazione politica utilizzando SHA1 e crittografa il risultato utilizzando RSA e la chiave privata la cui chiave pubblica corrispondente si trova in un gruppo di chiavi attendibile.
4. Codifica in base64 la dichiarazione di policy con hash e sostituisce i caratteri speciali per rendere sicura la stringa da utilizzare come parametro di richiesta URL.
5. Concatena i valori.

Per l'implementazione completa, vedi l'esempio in Signature Code in C#.

> **Note**
>
> `keyId`Viene restituito quando si carica una chiave pubblica su. CloudFront Per ulteriori informazioni, consulta
>
> 6
>
> &Key-Pair-Id.

Example : metodo di firma di policy personalizzato in 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;
    }
}
```

Metodi utility per generazione di firme

I seguenti metodi ottengono la dichiarazione di policy da un file e analizzano gli intervalli di tempo per la generazione di firme.

Example : metodi di utilità per generazione di firme

```
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();
}
```

Consulta anche

- Creazione di una firma per URL utilizzando Perl
- Creazione di una firma per URL utilizzando PHP
- Creazione di una firma per URL utilizzando Java

Creazione di una firma per URL utilizzando Java

Oltre al seguente esempio di codice, è possibile utilizzare la classe di `CloudFrontUrlSigner` utilità nella AWS SDK per Java (versione 1) per creare CloudFront signed URLs.

Per altri esempi, consulta Creare cookie firmati URLs e cookie utilizzando un AWS SDK nella libreria di codici AWS SDK Code Examples.

> **Note**
>
> La creazione di un URL firmato è solo una parte del processo di pubblicazione di contenuti privati. CloudFront Per ulteriori informazioni sull'intero processo, consulta Usa firmato URLs.

L'esempio seguente mostra come creare un URL CloudFront firmato.

Example Metodi di policy e di crittografia di firme 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);

    }
}
```

Consulta anche:

- Creazione di una firma per URL utilizzando Perl
- Creazione di una firma per URL utilizzando PHP
- Crea una firma per URL utilizzando C# e .NET Framework

Limitazione dell’accesso a un’origine AWS

Puoi configurare CloudFront alcune AWS origini in modo da offrire i seguenti vantaggi:

- Limita l'accesso all' AWS origine in modo che non sia accessibile pubblicamente.
- Garantisce che gli spettatori (utenti) possano accedere al contenuto dell' AWS origine solo tramite la distribuzione specificata CloudFront . Ciò impedisce agli spettatori di accedere al contenuto direttamente dall'origine o tramite una distribuzione CloudFront involontaria.

A tale scopo, configura CloudFront l'invio di richieste autenticate all' AWS origine e configura l' AWS origine per consentire l'accesso solo alle richieste autenticate da. CloudFront Per ulteriori informazioni, consulta gli argomenti seguenti per i tipi di AWS origini compatibili.

Argomenti

- Limita l’accesso a un’origine AWS Elemental MediaPackage v2

- Limitazione dell’accesso a un’origine AWS Elemental MediaStore
- Limitazione dell’accesso all’origine dell’URL di una funzione AWS Lambda
- Limitazione dell’accesso a un’origine Amazon S3
- Limitazione dell’accesso con VPC Origins

Limita l’accesso a un’origine AWS Elemental MediaPackage v2

CloudFront fornisce il controllo dell'accesso all'origine (OAC) per limitare l'accesso a un'origine v2. MediaPackage

> **Note**
>
> CloudFront OAC supporta solo la versione 2. MediaPackage MediaPackage la v1 non è supportata.

Argomenti

- Creazione di un nuovo OAC
- Impostazioni avanzate per il controllo dell'accesso all'origine

Creazione di un nuovo OAC

Completa i passaggi descritti nei seguenti argomenti per configurare un nuovo OAC in. CloudFront

Argomenti

- Prerequisiti
- Concedi CloudFront l'autorizzazione per accedere all'origine v2 MediaPackage
- Creazione dell’OAC

Prerequisiti

Prima di creare e configurare OAC, è necessario disporre di una CloudFront distribuzione con origine MediaPackage v2. Per ulteriori informazioni, consulta Usa un MediaStore contenitore o un canale MediaPackage .

Concedi CloudFront l'autorizzazione per accedere all'origine v2 MediaPackage

Prima di creare un OAC o configurarlo in una CloudFront distribuzione, assicurati che CloudFront disponga dell'autorizzazione per accedere all'origine MediaPackage v2. Esegui questa operazione dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all'origine MediaPackage v2 nella configurazione di distribuzione.

Utilizza una policy IAM per consentire al CloudFront service principal (`cloudfront.amazonaws.com`) di accedere all'origine. L'`Condition`elemento della policy consente di accedere CloudFront all'origine MediaPackage v2 solo quando la richiesta è per conto della CloudFront distribuzione che contiene l'origine MediaPackage v2. Questa è la distribuzione con l'origine MediaPackage v2 a cui desideri aggiungere OAC.

Example : policy IAM che consente l'accesso in sola lettura per una CloudFront distribuzione con OAC abilitato

La seguente politica consente alla CloudFront distribuzione (*E1PDK09ESKHJWT*) l'accesso all'origine v2. MediaPackage L'origine è l'ARN specificato per l'elemento `Resource`.

JSON

```
{
    "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**
>
> - Se hai abilitato la funzionalità MQAR e il controllo di accesso origine (OAC), aggiungi l'azione `mediapackagev2:GetHeadObject` alla policy IAM. MQAR richiede questa autorizzazione per inviare `HEAD` richieste all'origine MediaPackage v2. Per ulteriori informazioni su MQAR, consulta MQAR (Media Quality-Aware Resiliency).
> - Se crei una distribuzione che non dispone dell'autorizzazione per la tua origine MediaPackage v2, puoi scegliere Copy policy dalla CloudFront console e quindi scegliere Update endpoint permissions. Puoi quindi collegare l'autorizzazione copiata all'endpoint. Per ulteriori informazioni, consulta Campi della policy dell'endpoint nella Guida per l'utente di AWS Elemental MediaPackage .

Creazione dell'OAC

Per creare un OAC, puoi utilizzare l' Console di gestione AWS, CloudFormation, o l'API AWS CLI. CloudFront

Console

Come creare un OAC

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione a sinistra, scegli Accesso origine.
3. Scegli Crea un'impostazione di controllo.
4. Nel modulo Crea nuovo OAC, procedi come indicato di seguito:
   a. Immetti un Nome e (facoltativamente) una Descrizione per l'OAC.
   b. Per Comportamento di firma, si consiglia di lasciare l'impostazione predefinita (Richieste di firma (consigliato)). Per ulteriori informazioni, consulta the section called "Impostazioni avanzate per il controllo dell'accesso all'origine".
5. Per il tipo Origin, scegli MediaPackage V2.
6. Scegli Create (Crea).

> **Tip**
>
> Dopo aver creato l'OAC, prendi nota del Nome. In questa procedura, eseguire le seguenti operazioni:

Per aggiungere un OAC a un'origine MediaPackage v2 in una distribuzione

1. Apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Scegli una distribuzione con un'origine MediaPackage V2 a cui desideri aggiungere l'OAC, quindi scegli la scheda Origins.
3. Seleziona l'origine MediaPackage v2 a cui desideri aggiungere l'OAC, quindi scegli Modifica.
4. Seleziona HTTPS solo per il protocollo di origine.
5. Nel menu a discesa Controllo di accesso origine, scegli il nome OAC che desideri utilizzare.
6. Scegli Save changes (Salva modifiche).

La distribuzione inizia a essere distribuita in tutte le edge location. CloudFront Quando una edge location riceve la nuova configurazione, firma tutte le richieste che invia all'origine MediaPackage v2.

CloudFormation

Per creare un OAC con CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del CloudFormation modello, in formato YAML, per la creazione di 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
```

Per ulteriori informazioni, vedere AWS::CloudFront::OriginAccessControl nella Guida per l'utente.AWS CloudFormation

CLI

Per creare un controllo di accesso all'origine con AWS Command Line Interface (AWS CLI), utilizzate il aws cloudfront create-origin-access-control comando. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare un controllo di accesso all'origine (CLI con file di input)

1. Per creare un file denominato `origin-access-control.yaml`, utilizza il comando seguente. Tale file contiene tutti i parametri di input per il comando create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Aprire il file `origin-access-control.yaml` appena creato. Modifica il file per aggiungere un nome per l'OAC, una descrizione (opzionale) e modificare `SigningBehavior` in `always`. Quindi salvare il file.

   Per ulteriori informazioni sulle impostazioni OAC, consultare the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.

3. Utilizzare il comando seguente per creare il controllo di accesso origine utilizzando i parametri di input dal file `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Prendere nota del valore `Id` nell'output del comando. È necessario per aggiungere l'OAC a un'origine MediaPackage v2 in una CloudFront distribuzione.

Per collegare un OAC a un'origine MediaPackage v2 in una distribuzione esistente (CLI con file di input)

1. Usa il comando seguente per salvare la configurazione di distribuzione per la CloudFront distribuzione a cui desideri aggiungere l'OAC. La distribuzione deve avere un'origine MediaPackage v2.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Aprire il file denominato `dist-config.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

   - Nell'oggetto `Origins`, aggiungi l'ID dell'OAC al campo a cui è stato assegnato il nome `OriginAccessControlId`.
   - Rimuovi il valore dal campo denominato `OriginAccessIdentity`, se esiste.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare il controllo di accesso origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una edge location riceve la nuova configurazione, firma tutte le richieste che invia all'origine MediaPackage v2.

API

Per creare un OAC con l' CloudFront API, usa. CreateOriginAccessControl Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato un OAC, puoi collegarlo a un'origine MediaPackage v2 in una distribuzione, utilizzando una delle seguenti chiamate API:

- Per collegarlo a una distribuzione esistente, usa. UpdateDistribution
- Per collegarlo a una nuova distribuzione, usa CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID di OAC nel campo `OriginAccessControlId`, all'interno di un'origine. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Impostazioni avanzate per il controllo dell'accesso all'origine

La funzionalità CloudFront OAC include impostazioni avanzate destinate solo a casi d'uso specifici. Usa le impostazioni consigliate a meno che tu non abbia una necessità specifica per le impostazioni avanzate.

OAC contiene un'impostazione denominata Signing behavior (nella console) o `SigningBehavior` (nell'API, nella CLI e). CloudFormation Questa impostazione offre le seguenti opzioni:

Firma sempre le richieste di origine (impostazione consigliata)

Si consiglia di utilizzare questa impostazione, denominata Richieste di firma (consigliata) nella console, oppure `always` nell'API, nell'interfaccia a riga di comando e CloudFormation. Con questa impostazione, firma CloudFront sempre tutte le richieste che invia all'origine MediaPackage v2.

Non firmare le richieste di origine

Questa impostazione è denominata Non firmare le richieste nella console, oppure `never`nell'API, nell'interfaccia a riga di comando e CloudFormation. Usa questa impostazione per disattivare OAC per tutte le origini in tutte le distribuzioni che utilizzano questo OAC. Ciò consente di risparmiare tempo e fatica rispetto alla rimozione di un OAC da tutte le origini e le distribuzioni che lo utilizzano, uno per uno. Con questa impostazione, CloudFront non firma alcuna richiesta inviata all'origine MediaPackage v2.

> **Warning**
>
> Per utilizzare questa impostazione, l'origine MediaPackage v2 deve essere accessibile pubblicamente. Se utilizzi questa impostazione con un'origine MediaPackage v2 che non è accessibile pubblicamente, non CloudFront puoi accedere all'origine. L'origine MediaPackage v2 restituisce gli errori CloudFront e li CloudFront trasmette agli spettatori. Per ulteriori informazioni, consulta l'esempio della politica MediaPackage v2 per le politiche e le autorizzazioni MediaPackage nella Guida per l'utente.AWS Elemental MediaPackage

Non ignorare l'intestazione del visualizzatore (client) **`Authorization`**

Questa impostazione è denominata Non sovrascrivere l'intestazione di autorizzazionenella console, oppure `no-override` nell'API, nell'interfaccia a riga di comando e CloudFormation. Utilizzate questa impostazione quando desiderate firmare CloudFront le richieste di origine solo quando la richiesta del visualizzatore corrispondente non include un'`Authorization`intestazione. Con questa impostazione, CloudFront trasmette l'`Authorization`intestazione della richiesta del visualizzatore quando ne è presente una, ma firma la richiesta di origine (aggiungendo la propria `Authorization` intestazione) quando la richiesta del visualizzatore non include un'intestazione. `Authorization`

> **Warning**
>
> Per trasmettere l'`Authorization`intestazione dalla richiesta del visualizzatore, è necessario aggiungere l'`Authorization`intestazione a una politica di cache per tutti i comportamenti della cache che utilizzano le origini MediaPackage v2 associate a questo controllo di accesso all'origine.

Limitazione dell'accesso a un'origine AWS Elemental MediaStore

CloudFront fornisce il controllo dell'accesso all'origine (OAC) per limitare l'accesso a un'origine. AWS Elemental MediaStore

Argomenti

- Creazione di un nuovo controllo di accesso origine
- Impostazioni avanzate per il controllo dell'accesso all'origine

Creazione di un nuovo controllo di accesso origine

Completa i passaggi descritti nei seguenti argomenti per configurare un nuovo controllo di accesso all'origine in. CloudFront

Argomenti

- Prerequisiti
- Concedi CloudFront l'autorizzazione per accedere all' MediaStore origine
- Creazione del controllo di accesso origine

Prerequisiti

Prima di creare e configurare il controllo di accesso all'origine, è necessario disporre di una CloudFront distribuzione con un' MediaStore origine.

Concedi CloudFront l'autorizzazione per accedere all' MediaStore origine

Prima di creare un controllo di accesso all'origine o di configurarlo in una CloudFront distribuzione, assicurati che CloudFront disponga dell'autorizzazione per accedere all' MediaStore origine. Fatelo dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all' MediaStoreorigine nella configurazione di distribuzione.

Utilizza una politica del MediaStore contenitore per consentire al CloudFront service principal (`cloudfront.amazonaws.com`) di accedere all'origine. Utilizzate un `Condition` elemento della policy per consentire l'accesso CloudFront al MediaStore contenitore solo quando la richiesta è per conto della CloudFront distribuzione che contiene l' MediaStore origine. Questa è la distribuzione con l' MediaStore origine a cui vuoi aggiungere OAC.

Di seguito sono riportati alcuni esempi di politiche relative ai MediaStore contenitori che consentono a una CloudFront distribuzione di accedere a un' MediaStore origine.

Example MediaStore politica dei contenitori che consente l'accesso in sola lettura per una CloudFront distribuzione con OAC abilitato

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadOnly",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject"
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/<container name>/*",
                "Condition": {
```

```
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

Example MediaStore politica del contenitore che consente l'accesso in lettura e scrittura per una CloudFront distribuzione con OAC abilitato

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadWrite",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject",
                  "mediastore:PutObject"
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/container-name/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
```

```
            }
        ]
}
```

> **Note**
>
> Per consentire l'accesso in scrittura, è necessario configurare i metodi HTTP consentiti da includere PUT nelle impostazioni di comportamento della CloudFront distribuzione.

Creazione del controllo di accesso origine

Per creare un OAC, puoi utilizzare Console di gestione AWS, CloudFormation AWS CLI, the o l' CloudFrontAPI.

Console

Per creare un controllo di accesso all'origine

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione a sinistra, scegli Accesso origine.
3. Scegli Crea un'impostazione di controllo.
4. Nel modulo Crea un'impostazione di controllo, effettua le seguenti operazioni:
   a. Nel riquadro Dettagli, inserisci un Nome e (facoltativamente) una Descrizione per il controllo degli accessi all'origine.
   b. Nel riquadro Impostazioni, si consiglia di mantenere l'impostazione predefinita (Richieste di firma (consigliato)). Per ulteriori informazioni, consulta the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.
5. Scegli MediaStore dal menu a discesa del tipo di origine.
6. Scegli Create (Crea).

   Dopo aver creato l'OAC, prendere nota del Nome. In questa procedura, eseguire le seguenti operazioni:

Per aggiungere un controllo di accesso all'origine a un' MediaStore origine in una distribuzione

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli una distribuzione con un' MediaStore origine a cui desideri aggiungere l'OAC, quindi scegli la scheda Origins.
3. Seleziona l' MediaStore origine a cui vuoi aggiungere l'OAC, quindi scegli Modifica.
4. Seleziona HTTPS solo per il protocollo di origine.
5. Nel menu a discesa Controllo degli accessi origine, scegliere l'OAC che desideri utilizzare.
6. Scegli Save changes (Salva modifiche).

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando un'edge location riceve la nuova configurazione, firma tutte le richieste che invia all'origine del MediaStore bucket.

CloudFormation

Per creare un controllo di accesso all'origine (OAC) con CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del CloudFormation modello, in formato YAML, per creare un controllo di accesso all'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: mediastore
      SigningBehavior: always
      SigningProtocol: sigv4
```

Per ulteriori informazioni, consulta AWS::CloudFront::OriginAccessControl nella Guida per l'AWS CloudFormation utente.

CLI

Per creare un controllo di accesso all'origine con AWS Command Line Interface (AWS CLI), utilizzate il aws cloudfront create-origin-access-control comando. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare un controllo di accesso all'origine (CLI con file di input)

1. Per creare un file denominato `origin-access-control.yaml`, utilizza il comando seguente. Tale file contiene tutti i parametri di input per il comando create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Aprire il file `origin-access-control.yaml` appena creato. Modifica il file per aggiungere un nome per l'OAC, una descrizione (opzionale) e modificare `SigningBehavior` in `always`. Quindi salvare il file.

   Per ulteriori informazioni sulle impostazioni OAC, consultare the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.

3. Utilizzare il comando seguente per creare il controllo di accesso origine utilizzando i parametri di input dal file `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Prendere nota del valore `Id` nell'output del comando. È necessario per aggiungere l'OAC a un' MediaStore origine in una CloudFront distribuzione.

Per collegare un OAC a un' MediaStore origine in una distribuzione esistente (CLI con file di input)

1. Utilizzate il comando seguente per salvare la configurazione di distribuzione per la CloudFront distribuzione a cui desiderate aggiungere l'OAC. La distribuzione deve avere un' MediaStoreorigine.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Aprire il file denominato `dist-config.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

- Nell'oggetto `Origins`, aggiungi l'ID dell'OAC al campo a cui è stato assegnato il nome `OriginAccessControlId`.
- Rimuovi il valore dal campo denominato `OriginAccessIdentity`, se esiste.
- Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare il controllo di accesso origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una edge location riceve la nuova configurazione, firma tutte le richieste inviate all' MediaStore origine.

API

Per creare un controllo di accesso all'origine con l' CloudFront API, usa CreateOriginAccessControl. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato un controllo di accesso di origine, puoi collegarlo a un' MediaStore origine in una distribuzione, utilizzando una delle seguenti chiamate API:

- Per collegarlo a una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a una nuova distribuzione, usa CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID di controllo dell'accesso origine nel campo `OriginAccessControlId`, all'interno di un'origine. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Impostazioni avanzate per il controllo dell'accesso all'origine

La funzionalità di controllo dell'accesso all' CloudFront origine include impostazioni avanzate destinate solo a casi d'uso specifici. Usa le impostazioni consigliate a meno che tu non abbia una necessità specifica per le impostazioni avanzate.

Origin Access Control contiene un'impostazione denominata Signing behavior (nella console) o `SigningBehavior` (nell'API, CLI e CloudFormation). Questa impostazione offre le seguenti opzioni:

Firma sempre le richieste di origine (impostazione consigliata)

Si consiglia di utilizzare questa impostazione, denominata Richieste di firma (consigliata) nella console, oppure `always` nell'API, nell'interfaccia a riga di comando e CloudFormation. Con questa impostazione, firma CloudFront sempre tutte le richieste che invia all' MediaStore origine.

Non firmare le richieste di origine

Questa impostazione è denominata Non firmare le richieste nella console, oppure `never`nell'API, nell'interfaccia a riga di comando e CloudFormation. Usa questa impostazione per disattivare il controllo dell'accesso all'origine per tutte le origini in tutte le distribuzioni che utilizzano questo controllo di accesso all'origine. Ciò consente di risparmiare tempo e fatica rispetto alla rimozione di un controllo di accesso all'origine da tutte le origini e le distribuzioni che lo utilizzano, uno per uno. Con questa impostazione, CloudFront non firma alcuna richiesta inviata all' MediaStoreorigine.

> **Warning**
>
> Per utilizzare questa impostazione, l' MediaStore origine deve essere accessibile pubblicamente. Se utilizzi questa impostazione con un' MediaStore origine non accessibile pubblicamente, CloudFront non puoi accedere all'origine. L' MediaStore origine restituisce gli errori CloudFront e li CloudFront trasmette agli spettatori. Per ulteriori informazioni, consulta l'esempio di politica del MediaStore contenitore per l'accesso pubblico in lettura tramite HTTPS.

Non ignorare l'intestazione del visualizzatore (client) **`Authorization`**

Questa impostazione è denominata Non sovrascrivere l'intestazione di autorizzazionenella console, oppure `no-override` nell'API, nell'interfaccia a riga di comando e CloudFormation. Utilizza questa impostazione quando desideri firmare CloudFront le

richieste di origine solo quando la richiesta del visualizzatore corrispondente non include un'`Authorization`intestazione. Con questa impostazione, CloudFront trasmette l'`Authorization`intestazione della richiesta del visualizzatore quando ne è presente una, ma firma la richiesta di origine (aggiungendo la propria `Authorization` intestazione) quando la richiesta del visualizzatore non include un'intestazione. `Authorization`

> **Warning**
>
> Per trasmettere l'`Authorization`intestazione dalla richiesta del visualizzatore, è necessario aggiungere l'`Authorization`intestazione a una politica di cache per tutti i comportamenti della cache che utilizzano le MediaStore origini associate a questo controllo di accesso all'origine.

Limitazione dell'accesso all'origine dell'URL di una funzione AWS Lambda

CloudFront fornisce il controllo dell'accesso all'origine (OAC) per limitare l'accesso all'origine dell'URL di una funzione Lambda.

Argomenti

- Creazione di un nuovo OAC
- Impostazioni avanzate per il controllo dell'accesso all'origine
- Esempio di codice modello

Creazione di un nuovo OAC

Completa i passaggi descritti nei seguenti argomenti per configurare un nuovo OAC in. CloudFront

> **Important**
>
> Se utilizzi `PUT` o `POST` metodi con l'URL della funzione Lambda, gli utenti devono calcolare il corpo SHA256 del corpo e includere il valore hash del payload del corpo della richiesta nell'`x-amz-content-sha256`intestazione quando inviano la richiesta a. CloudFront Lambda non supporta i payload non firmati.

Argomenti

- Prerequisiti
- Concedi CloudFront l'autorizzazione per accedere all'URL della funzione Lambda
- Creazione dell'OAC

Prerequisiti

Prima di creare e configurare OAC, è necessario disporre di una CloudFront distribuzione con un URL della funzione Lambda come origine. Per utilizzare OAC, deve specificare `AWS_IAM` come il valore per il parametro `AuthType`. Per ulteriori informazioni, consulta Utilizzo dell'URL di una funzione Lambda.

Concedi CloudFront l'autorizzazione per accedere all'URL della funzione Lambda

Prima di creare un OAC o configurarlo in una CloudFront distribuzione, assicurati che CloudFront disponga dell'autorizzazione per accedere all'URL della funzione Lambda. Esegui questa operazione dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all'URL della funzione Lambda nella configurazione di distribuzione.

> **Note**
>
> Per aggiornare la policy IAM per l'URL della funzione Lambda, devi usare AWS Command Line Interface (AWS CLI). La modifica della policy IAM nella console Lambda non è attualmente supportata.

Il AWS CLI comando seguente concede al CloudFront service principal (`cloudfront.amazonaws.com`) l'accesso all'URL della funzione Lambda. L'`Condition`elemento della policy consente di accedere CloudFront a Lambda solo quando la richiesta è per conto della CloudFront distribuzione che contiene l'URL della funzione Lambda. Questa è la distribuzione con l'origine dell'URL della funzione Lambda a cui desideri aggiungere l'OAC.

Example : AWS CLI comando per aggiornare una policy per consentire l'accesso in sola lettura a una CloudFront distribuzione con OAC abilitato

I seguenti AWS CLI comandi consentono alla CloudFront distribuzione (*`E1PDK09ESKHJWT`*) di accedere alla tua *`FUNCTION_URL_NAME`* Lambda.

```
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
```

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipalInvokeFunction" \
--action "lambda:InvokeFunction" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
--function-name FUNCTION_URL_NAME
```

> **Note**
>
> Se crei una distribuzione e questa non dispone dell'autorizzazione per l'URL della funzione Lambda, puoi scegliere Copia il comando CLI dalla CloudFront console e quindi immettere questo comando dal tuo terminale a riga di comando. Per ulteriori informazioni, consulta Concedere alla funzione l'accesso a Servizi AWS nella Guida per gli sviluppatori di AWS Lambda .

Creazione dell'OAC

Per creare un OAC, puoi usare l' Console di gestione AWS, CloudFormation AWS CLI, o l'API. CloudFront

Console

Come creare un OAC

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione a sinistra, scegli Accesso origine.
3. Scegli Crea un'impostazione di controllo.
4. Nel modulo Crea nuovo OAC, procedi come indicato di seguito:
   a. Immetti un Nome e (facoltativamente) una Descrizione per l'OAC.

b. Per Comportamento di firma, si consiglia di lasciare l'impostazione predefinita (Richieste di firma (consigliato)). Per ulteriori informazioni, consulta the section called "Impostazioni avanzate per il controllo dell'accesso all'origine".

5. Per Tipo di origine, scegli Lambda.
6. Scegli Create (Crea).

> **Tip**
>
> Dopo aver creato l'OAC, prendi nota del Nome. In questa procedura, eseguire le seguenti operazioni:

Come aggiungere un controllo di accesso origine all'URL di una funzione Lambda in una distribuzione

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli una distribuzione con un'URL della funzione Lambda a cui desideri aggiungere l'OAC, quindi scegli la scheda Origini.
3. Seleziona l'URL della funzione Lambda a cui desideri aggiungere l'OAC, quindi scegli Modifica.
4. Seleziona HTTPS solo per il protocollo di origine.
5. Nel menu a discesa Controllo di accesso origine, scegli il nome OAC che desideri utilizzare.
6. Scegli Save changes (Salva modifiche).

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una posizione edge riceve la nuova configurazione, firma tutte le richieste che invia all'URL della funzione Lambda.

CloudFormation

Per creare un OAC con CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del CloudFormation modello, in formato YAML, per la creazione di 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
```

Per ulteriori informazioni, vedere AWS::CloudFront::OriginAccessControl nella Guida per l'utente.AWS CloudFormation

CLI

Per creare un controllo di accesso all'origine con AWS Command Line Interface (AWS CLI), utilizzate il aws cloudfront create-origin-access-control comando. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare un controllo di accesso all'origine (CLI con file di input)

1. Per creare un file denominato `origin-access-control.yaml`, utilizza il comando seguente. Tale file contiene tutti i parametri di input per il comando create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Aprire il file `origin-access-control.yaml` appena creato. Modifica il file per aggiungere un nome per l'OAC, una descrizione (opzionale) e modificare `SigningBehavior` in `always`. Quindi salvare il file.

   Per ulteriori informazioni sulle impostazioni OAC, consultare the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.

3. Utilizzare il comando seguente per creare il controllo di accesso origine utilizzando i parametri di input dal file `origin-access-control.yaml`.

   ```
   aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
   access-control.yaml
   ```

   Prendere nota del valore `Id` nell'output del comando. Ne hai bisogno per aggiungere l'OAC all'URL di una funzione Lambda in CloudFront una distribuzione.

Come collegare un OAC all'URL di una funzione Lambda in una distribuzione esistente (CLI con file di input)

1. Usa il comando seguente per salvare la configurazione di distribuzione per la CloudFront distribuzione a cui desideri aggiungere l'OAC. La distribuzione deve avere come origine l'URL di una funzione Lambda.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Aprire il file denominato `dist-config.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

   - Nell'oggetto `Origins`, aggiungi l'ID dell'OAC al campo a cui è stato assegnato il nome `OriginAccessControlId`.
   - Rimuovi il valore dal campo denominato `OriginAccessIdentity`, se esiste.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare il controllo di accesso origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una posizione edge riceve la nuova configurazione, firma tutte le richieste che invia all'URL della funzione Lambda.

API

Per creare un OAC con l' CloudFront API, usa. CreateOriginAccessControl Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato un OAC, puoi collegarlo all'URL di una funzione Lambda in una distribuzione, utilizzando una delle seguenti chiamate API:

- Per collegarlo a una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a una nuova distribuzione, usa CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID di OAC nel campo `OriginAccessControlId`, all'interno di un'origine. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Impostazioni avanzate per il controllo dell'accesso all'origine

La funzionalità CloudFront OAC include impostazioni avanzate destinate solo a casi d'uso specifici. Usa le impostazioni consigliate a meno che tu non abbia una necessità specifica per le impostazioni avanzate.

OAC contiene un'impostazione denominata Signing behavior (nella console) o `SigningBehavior` (nell'API, nella CLI e). CloudFormation Questa impostazione offre le seguenti opzioni:

Firma sempre le richieste di origine (impostazione consigliata)

Si consiglia di utilizzare questa impostazione, denominata Richieste di firma (consigliata) nella console, oppure `always` nell'API, nell'interfaccia a riga di comando e CloudFormation. Con questa impostazione, firma CloudFront sempre tutte le richieste inviate all'URL della funzione Lambda.

Non firmare le richieste di origine

Questa impostazione è denominata Non firmare le richieste nella console, oppure `never`nell'API, nell'interfaccia a riga di comando e CloudFormation. Usa questa impostazione per disattivare OAC per tutte le origini in tutte le distribuzioni che utilizzano questo OAC. Ciò consente di risparmiare tempo e fatica rispetto alla rimozione di un OAC da tutte le origini e le distribuzioni che lo utilizzano, uno per uno. Con questa impostazione, CloudFront non firma alcuna richiesta inviata all'URL della funzione Lambda.

> **Warning**
>
> Per utilizzare questa impostazione, l'URL della funzione Lambda deve essere accessibile pubblicamente. Se usi questa impostazione con un URL della funzione Lambda non

accessibile pubblicamente, non CloudFront puoi accedere all'origine. L'URL della funzione Lambda restituisce gli errori CloudFront e li CloudFront trasmette ai visualizzatori. Per ulteriori informazioni, consulta il modello di sicurezza e autenticazione per la URLs funzione Lambda nella Guida per AWS Lambda l'utente.

Non ignorare l'intestazione del visualizzatore (client) **`Authorization`**

Questa impostazione è denominata Non sovrascrivere l'intestazione di autorizzazionenella console, oppure `no-override` nell'API, nell'interfaccia a riga di comando e CloudFormation. Utilizzate questa impostazione quando desiderate firmare CloudFront le richieste di origine solo quando la richiesta del visualizzatore corrispondente non include un'`Authorization`intestazione. Con questa impostazione, CloudFront trasmette l'`Authorization`intestazione della richiesta del visualizzatore quando ne è presente una, ma firma la richiesta di origine (aggiungendo la propria `Authorization` intestazione) quando la richiesta del visualizzatore non include un'intestazione. `Authorization`

⚠ Warning

- Se utilizzi questa impostazione, devi specificare la firma Signature Version 4 per l'URL della funzione Lambda anziché il nome o il CNAME della CloudFront distribuzione. Quando CloudFront inoltra l'`Authorization`intestazione dalla richiesta del visualizzatore all'URL della funzione Lambda, Lambda convalida la firma rispetto all'host del dominio URL Lambda. Se la firma non è basata sul dominio URL Lambda, l'host nella firma non corrisponderà all'host utilizzato dall'origine dell'URL Lambda. Ciò significa che la richiesta non andrà a buon fine, causando un errore di convalida della firma.
- Per trasmettere l'`Authorization`intestazione dalla richiesta del visualizzatore, è necessario aggiungere l'`Authorization`intestazione a una politica di cache per tutti i comportamenti della cache che utilizzano la funzione Lambda URLs associata a questo controllo di accesso all'origine.

Esempio di codice modello

Se la tua CloudFront origine è l'URL di una funzione Lambda associata a un OAC, puoi usare il seguente script Python per caricare file nella funzione Lambda con il metodo. `POST`

Questo codice presuppone che l'OAC sia stato configurato con il comportamento di firma predefinito impostato su Firma sempre le richieste di origine e che non sia stata selezionata l'impostazione Non sovrascrivere l'intestazione di autorizzazione.

Questa configurazione consente all'OAC di gestire correttamente l'autorizzazione SigV4 con Lambda utilizzando il nome host Lambda. Il payload viene firmato utilizzando SigV4 dall'identità IAM autorizzata per l'URL della funzione Lambda, che è designato come tipo `IAM_AUTH`.

Il modello mostra come gestire i valori hash del payload firmato nell'intestazione x-amz-content-sha256 per le richieste `POST` dal lato client. Nello specifico, questo modello è progettato per gestire i payload dei dati dei moduli. Il modello consente il caricamento sicuro dei file su un URL CloudFront della funzione Lambda e AWS utilizza meccanismi di autenticazione per garantire che solo le richieste autorizzate possano accedere alla funzione Lambda.

Il codice include la seguente funzionalità:

- Soddisfa il requisito di includere l'hash del payload nell'intestazione x-amz-content-sha256
- Utilizza l'autenticazione SigV4 per un accesso sicuro Servizio AWS
- Supporta caricamenti di file utilizzando dati di moduli multiparte
- Include la gestione degli errori per le eccezioni richiesta

```
import boto3
from botocore.auth import SigV4Auth
from botocore.awsrequest import AWSRequest
import requests
import hashlib
import os


def calculate_body_hash(body):
    return hashlib.sha256(body).hexdigest()


def sign_request(request, credentials, region, service):
    sigv4 = SigV4Auth(credentials, service, region)
    sigv4.add_auth(request)
```

```
def upload_file_to_lambda(cloudfront_url, file_path, region):
    # AWS credentials
    session = boto3.Session()
    credentials = session.get_credentials()

    # Prepare the multipart form-data
    boundary = "------------------------boundary"

    # Read file content
    with open(file_path, 'rb') as file:
        file_content = file.read()

    # Get the filename from the path
    filename = os.path.basename(file_path)

    # Prepare the multipart body
    body = (
        f'--{boundary}\r\n'
        f'Content-Disposition: form-data; name="file"; filename="{filename}"\r\n'
        f'Content-Type: application/octet-stream\r\n\r\n'
    ).encode('utf-8')
    body += file_content
    body += f'\r\n--{boundary}--\r\n'.encode('utf-8')

    # Calculate SHA256 hash of the entire body
    body_hash = calculate_body_hash(body)

    # Prepare headers
    headers = {
        'Content-Type': f'multipart/form-data; boundary={boundary}',
        'x-amz-content-sha256': body_hash
    }

    # Create the request
    request = AWSRequest(
        method='POST',
        url=cloudfront_url,
        data=body,
        headers=headers
    )

    # Sign the request
    sign_request(request, credentials, region, 'lambda')
```

```
    # Get the signed headers
    signed_headers = dict(request.headers)

    # Print request headers before sending
    print("Request Headers:")
    for header, value in signed_headers.items():
        print(f"{header}: {value}")

    try:
        # Send POST request with signed headers
        response = requests.post(
            cloudfront_url,
            data=body,
            headers=signed_headers
        )

        # Print response status and content
        print(f"\nStatus code: {response.status_code}")
        print("Response:", response.text)

        # Print response headers
        print("\nResponse Headers:")
        for header, value in response.headers.items():
            print(f"{header}: {value}")

    except requests.exceptions.RequestException as e:
        print(f"An error occurred: {e}")


# Usage
cloudfront_url = "https://d111111abcdef8.cloudfront.net"
file_path = r"filepath"
region = "us-east-1"  # example: "us-west-2"

upload_file_to_lambda(cloudfront_url, file_path, region)
```

Limitazione dell’accesso a un’origine Amazon S3

CloudFront offre due modi per inviare richieste autenticate a un'origine Amazon S3: Origin Access Control (OAC) e Origin Access Identity (OAI). OAC consente di proteggere le origini, come Amazon S3.

Ti consigliamo di utilizzare OAC perché supporta le seguenti funzionalità:

- Tutti i bucket Amazon S3 in totale Regioni AWS, comprese le regioni opt-in lanciate dopo dicembre 2022
- Crittografia lato server con chiavi AWS KMS (SSE-KMS) Amazon S3
- Richieste dinamiche (`PUT` e `DELETE`) su Amazon S3

OAI non supporta queste funzionalità o richiede soluzioni alternative aggiuntive in tali scenari. Se stai già utilizzando OAI e desideri migrare, consulta the section called “Migrazione dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC)”.

> **Note**
>
> - Quando usi CloudFront OAC con le origini dei bucket Amazon S3, devi impostare Amazon S3 Object Ownership su Bucket owner enforced, l'impostazione predefinita per i nuovi bucket Amazon S3. Se necessario ACLs, utilizza l'impostazione preferita del proprietario di Bucket per mantenere il controllo sugli oggetti caricati tramite. CloudFront
> - Se la tua origine è un bucket Amazon S3 configurato come endpoint di un sito Web, devi configurarlo CloudFront come origine personalizzata. Ciò significa che non è possibile utilizzare OAC (o OAI). OAC non supporta il reindirizzamento dell’origine tramite Lambda@Edge.

I seguenti argomenti descrivono come utilizzare OAC con origine Amazon S3.

Argomenti

- the section called “Creazione di un nuovo controllo di accesso origine”
- the section called “Eliminazione di una distribuzione con un OAC collegato a un bucket S3”
- the section called “Migrazione dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC)”
- the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”

Creazione di un nuovo controllo di accesso origine

Completa i passaggi descritti nei seguenti argomenti per configurare un nuovo controllo di accesso di origine in. CloudFront

Argomenti

Prerequisiti

Prima di creare e configurare Origin Access Control (OAC), devi disporre di una CloudFront distribuzione con un'origine di bucket Amazon S3. Questa origine deve essere un normale bucket S3, non un bucket configurato come endpoint del sito Web. Per ulteriori informazioni sulla configurazione di una CloudFront distribuzione con un'origine del bucket S3, consulta. the section called “Nozioni di base su una distribuzione standard”

Important

Quando usi OAC per proteggere la tua origine Amazon S3, la comunicazione CloudFront tra Amazon S3 e Amazon S3 avviene sempre tramite HTTPS, ma solo quando scegli di firmare sempre le richieste. Devi scegliere Sign request (consigliato) nella console o specificarlo `always` nell' CloudFront API, AWS CLI oppure. CloudFormation
Se scegli invece l'opzione Do not sign requests o Do not override authorization header, CloudFront utilizza il protocollo di connessione specificato nelle seguenti politiche:

- Politica del protocollo Viewer
- Policy del protocollo di origine (solo origini personalizzate)

Ad esempio, se scegli Non sovrascrivere l'intestazione di autorizzazione e desideri utilizzare HTTPS tra CloudFront e la tua origine Amazon S3, utilizza Redirect HTTP to HTTPS o HTTPS solo per la policy del protocollo del visualizzatore.

Concedi l' CloudFront autorizzazione per accedere al bucket S3

Prima di creare un controllo di accesso all'origine (OAC) o configurarlo in una CloudFront distribuzione, assicurati che CloudFront disponga dell'autorizzazione per accedere all'origine del bucket S3. Esegui questa operazione dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all'origine S3 nella configurazione di distribuzione.

Utilizza una policy del bucket S3 per consentire al CloudFront service principal (`cloudfront.amazonaws.com`) di accedere al bucket. Utilizza un `Condition` elemento della policy per consentire l'accesso CloudFront al bucket solo quando la richiesta è per conto della CloudFront distribuzione che contiene l'origine S3. Questa è la distribuzione con l'origine S3 a cui desideri aggiungere l'OAC.

Per informazioni sull'aggiunta o la modifica di una politica del bucket, consulta Aggiunta di una policy di bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon S3.

Di seguito sono riportati alcuni esempi di policy relative ai bucket S3 che consentono una CloudFront distribuzione con accesso abilitato all'OAC a un'origine S3.

Example Policy sui bucket S3 che consente l'accesso in sola lettura per una distribuzione con OAC abilitato CloudFront

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadOnly",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
        }
      }
    }
  ]
}
```

Example Policy S3 bucket che consente l'accesso in lettura e scrittura per una distribuzione con OAC abilitato CloudFront

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID>"
        }
      }
    }
  ]
}
```

SSE-KMS

Se gli oggetti nell'origine del bucket S3 sono crittografati utilizzando la crittografia lato server con AWS Key Management Service (SSE-KMS), devi assicurarti che la distribuzione disponga dell'autorizzazione per utilizzare la chiave. CloudFront AWS KMS Per concedere alla CloudFront distribuzione l'autorizzazione all'uso della chiave KMS, aggiungi una dichiarazione alla politica della chiave KMS. Per informazioni su come modificare un criterio delle chiavi, consulta Modifica di una policy delle chiavinella Guida per gli sviluppatori AWS Key Management Service .

Example Dichiarazione della policy della chiave KMS

L'esempio seguente mostra una dichiarazione AWS KMS politica che consente alla CloudFront distribuzione con OAC di accedere a una chiave KMS per 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>"
            }
        }
}
```

Creazione del controllo di accesso origine

Per creare un controllo di accesso all'origine (OAC), puoi utilizzare l', Console di gestione AWS CloudFormation, o l'API. AWS CLI CloudFront

Console

Per creare un controllo di accesso all'origine

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione a sinistra, scegli Accesso origine.
3. Scegli Crea un'impostazione di controllo.
4. Nel modulo Crea un'impostazione di controllo, effettua le seguenti operazioni:

a. Nel riquadro Dettagli, inserisci un Nome e (facoltativamente) una Descrizione per il controllo degli accessi all'origine.

b. Nel riquadro Impostazioni, si consiglia di mantenere l'impostazione predefinita (Richieste di firma (consigliato)). Per ulteriori informazioni, consulta the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.

5. Scegli S3 dal menu a discesa tipo di origine.
6. Scegli Create (Crea).

   Dopo aver creato l'OAC, prendere nota del Nome. In questa procedura, eseguire le seguenti operazioni:

Per aggiungere un controllo di accesso di origine a un'origine S3 in una distribuzione

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli una distribuzione con un'origine S3 a cui desideri aggiungere l'OAC, quindi scegli lascheda Origini.
3. Selezionare l'origine S3 alla quale si desidera aggiungere l'OAC, quindi scegliere Modifica.
4. Per Accesso origine, scegli Impostazioni di controllo di accesso origine (consigliato).
5. Nel menu a discesa Controllo degli accessi origine, scegliere l'OAC che desideri utilizzare.
6. Scegli Save changes (Salva modifiche).

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una edge location riceve la nuova configurazione, firma tutte le richieste che invia all'origine del bucket S3.

CloudFormation

Per creare un controllo di accesso all'origine (OAC) con CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del CloudFormation modello, in formato YAML, per creare un controllo di accesso all'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: s3
```

```
      SigningBehavior: always
      SigningProtocol: sigv4
```

Per ulteriori informazioni, consulta AWS::CloudFront::OriginAccessControl nella Guida per l'AWS CloudFormation utente.

CLI

Per creare un controllo di accesso all'origine con AWS Command Line Interface (AWS CLI), utilizzate il aws cloudfront create-origin-access-control comando. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare un controllo di accesso all'origine (CLI con file di input)

1. Per creare un file denominato `origin-access-control.yaml`, utilizza il comando seguente. Tale file contiene tutti i parametri di input per il comando create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Aprire il file `origin-access-control.yaml` appena creato. Modifica il file per aggiungere un nome per l'OAC, una descrizione (opzionale) e modificare `SigningBehavior` in `always`. Quindi salvare il file.

   Per ulteriori informazioni sulle impostazioni OAC, consultare the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.

3. Utilizzare il comando seguente per creare il controllo di accesso origine utilizzando i parametri di input dal file `origin-access-control.yaml`.

   ```
   aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
   access-control.yaml
   ```

   Prendere nota del valore `Id` nell'output del comando. È necessario per aggiungere l'OAC a un'origine del bucket S3 in una distribuzione. CloudFront

Per allegare un OAC a un'origine bucket S3 in una distribuzione esistente (CLI con file di input)

1. Usa il comando seguente per salvare la configurazione di distribuzione per la CloudFront distribuzione a cui desideri aggiungere l'OAC. La distribuzione deve avere un'origine del bucket S3.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Aprire il file denominato `dist-config.yaml` appena creato. Modifica il file apportando le seguenti modifiche:

   - Nell'oggetto `Origins`, aggiungi l'ID dell'OAC al campo a cui è stato assegnato il nome `OriginAccessControlId`.
   - Rimuovi il valore dal campo denominato `OriginAccessIdentity`, se esiste.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Utilizzare il comando seguente per aggiornare la distribuzione e utilizzare il controllo di accesso origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribuzione inizia a essere distribuita in tutte le CloudFront edge location. Quando una edge location riceve la nuova configurazione, firma tutte le richieste che invia all'origine del bucket S3.

API

Per creare un controllo di accesso all'origine con l' CloudFront API, usa CreateOriginAccessControl. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato un controllo di accesso origine, è possibile collegarlo all'origine del bucket S3 in una distribuzione, utilizzando una delle seguenti chiamate API:

- Per collegarlo a una distribuzione esistente, usa UpdateDistribution.

- Per collegarlo a una nuova distribuzione, usa CreateDistribution.

Per entrambe queste chiamate API, fornire l'ID di controllo dell'accesso origine nel campo `OriginAccessControlId`, all'interno di un'origine. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento a tutte le impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Eliminazione di una distribuzione con un OAC collegato a un bucket S3

Se è necessario eliminare una distribuzione con un OAC collegato a un bucket S3, occorre eliminare la distribuzione prima di eliminare l'origine del bucket S3. In alternativa, includi la regione nel nome di dominio di origine. Se ciò non è possibile, puoi rimuovere l'OAC dalla distribuzione passando a pubblico prima dell'eliminazione. Per ulteriori informazioni, consulta Eliminazione di una distribuzione .

Migrazione dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC)

Per migrare da un'identità di accesso origine (OAI) legacy a un controllo di accesso origine (OAC), aggiorna innanzitutto l'origine del bucket S3 per consentire sia all'OAI che all'OAC di accedere al contenuto del bucket. Questo assicura che CloudFront non perda mai l'accesso al bucket durante la transizione. Per consentire sia a OAI che alla distribuzione con OAC abilitato di accedere a un bucket S3, aggiorna la policy di bucket per includere due dichiarazioni, una per ogni tipo di principale.

Il seguente esempio di policy di bucket S3 consente sia a un OAI che a una distribuzione con OAC abilitato di accedere a un'origine S3.

Example Policy del bucket S3 che consente l'accesso in sola lettura per un OAI e una distribuzione con OAC abilitato CloudFront

JSON

```
{
    "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>/*"
        }
    ]
}
```

Dopo aver aggiornato la politica dei bucket di S3 Origin per consentire l'accesso sia all'OAI che all'OAC, puoi aggiornare la configurazione di distribuzione per utilizzare OAC anziché OAI. Per ulteriori informazioni, consulta the section called “Creazione di un nuovo controllo di accesso origine”.

Dopo che la distribuzione è stata completamente distribuita, puoi rimuovere l'istruzione nella politica del bucket che consente l'accesso all'OAI. Per ulteriori informazioni, consulta the section called “Concedi l' CloudFront autorizzazione per accedere al bucket S3”.

Impostazioni avanzate per il controllo dell'accesso all'origine

La funzionalità di controllo dell'accesso all' CloudFront origine include impostazioni avanzate destinate solo a casi d'uso specifici. Usa le impostazioni consigliate a meno che tu non abbia una necessità specifica per le impostazioni avanzate.

Origin Access Control contiene un'impostazione denominata Signing behavior (nella console) o `SigningBehavior` (nell'API, CLI e CloudFormation). Questa impostazione offre le seguenti opzioni:

Firma sempre le richieste di origine (impostazione consigliata)

Si consiglia di utilizzare questa impostazione, denominata Richieste di firma (consigliata) nella console, oppure `always` nell'API, nell'interfaccia a riga di comando e CloudFormation. Con questa impostazione, firma CloudFront sempre tutte le richieste che invia all'origine del bucket S3.

Non firmare le richieste di origine

Questa impostazione è denominata Non firmare le richieste nella console, oppure `never`nell'API, nell'interfaccia a riga di comando e CloudFormation. Usa questa impostazione per disattivare il controllo dell'accesso all'origine per tutte le origini in tutte le distribuzioni che utilizzano questo controllo di accesso all'origine. Ciò consente di risparmiare tempo e fatica rispetto alla rimozione di un controllo di accesso all'origine da tutte le origini e le distribuzioni che lo utilizzano, uno per uno. Con questa impostazione, CloudFront non firma alcuna richiesta inviata all'origine del bucket S3.

> **Warning**
>
> Per utilizzare questa impostazione, l'origine del bucket S3 deve essere accessibile al pubblico. Se utilizzi questa impostazione con un'origine del bucket S3 che non è accessibile pubblicamente, CloudFront non puoi accedere all'origine. L'origine del bucket S3 restituisce gli errori CloudFront e li CloudFront trasmette agli spettatori.

Non ignorare l'intestazione del visualizzatore (client) **`Authorization`**

Questa impostazione è denominata Non sovrascrivere l'intestazione di autorizzazionenella console, oppure `no-override` nell'API, nell'interfaccia a riga di comando e CloudFormation. Utilizza questa impostazione quando desideri firmare le richieste CloudFront di origine solo quando la richiesta del visualizzatore corrispondente non include un'intestazione. `Authorization` Con questa impostazione, CloudFront trasmette l'`Authorization`intestazione della richiesta del visualizzatore quando ne è presente una, ma firma la richiesta di origine (aggiungendo la propria `Authorization` intestazione) quando la richiesta del visualizzatore non include un'intestazione. `Authorization`

> **Warning**
>
> Per passare lungo l'intestazione `Authorization` della richiesta del visualizzatore, devi aggiungere l'intestazione `Authorization` a una policy della cache per tutti i

comportamenti della cache che utilizzano le origini del bucket S3 associate a questo controllo di accesso all'origine.

Utilizzo di un'identità di accesso origine (legacy, non consigliata)

Panoramica dell'identità di accesso origine

CloudFront origin access identity (OAI) offre funzionalità simili a quelle di Origin Access Control (OAC), ma non funziona per tutti gli scenari. Nello specifico, l'OAI non supporta:

- Bucket Amazon S3 in tutto Regioni AWS, comprese le regioni con attivazione
- Crittografia lato server con chiavi AWS KMS (SSE-KMS) Amazon S3
- Richieste dinamiche (`PUT`, `POST` o `DELETE`) su Amazon S3
- Nuovo Regioni AWS lanciato dopo gennaio 2023

> **Tip**
>
> Ti consigliamo di utilizzare invece OAC. Per configurare OAC, consulta Creazione di un nuovo controllo di accesso origine. Per informazioni su come eseguire la migrazione da OAI a OAC, consulta the section called "Migrazione dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC)".

Concedere a un'identità di accesso origine l'autorizzazione per leggere i file nel bucket Amazon S3

Quando crei un OAI o ne aggiungi uno a una distribuzione con la CloudFront console, puoi aggiornare automaticamente la policy del bucket Amazon S3 per concedere all'OAI l'autorizzazione ad accedere al tuo bucket. In alternativa, è possibile scegliere di creare o aggiornare manualmente la policy di bucket. Qualunque sia il metodo utilizzato, è comunque necessario esaminare le autorizzazioni per assicurarsi che:

- Il tuo CloudFront OAI può accedere ai file nel bucket per conto degli utenti che li richiedono. CloudFront
- Gli utenti non possono utilizzare Amazon URLs S3 per accedere ai tuoi file al di fuori di. CloudFront

> **Important**
>
> Se configuri CloudFront per accettare e inoltrare tutti i metodi HTTP CloudFront supportati, assicurati di concedere all' CloudFront OAI le autorizzazioni desiderate. Ad esempio, se CloudFront configuri l'accettazione e l'inoltro delle richieste che utilizzano questo `DELETE` metodo, configura la tua bucket policy per gestire `DELETE` le richieste in modo appropriato in modo che gli utenti possano eliminare solo i file che desideri.

Utilizzo di policy di bucket di Amazon S3

Puoi consentire a un CloudFront OAI di accedere ai file in un bucket Amazon S3 creando o aggiornando la policy del bucket nei seguenti modi:

- Utilizzo della scheda Permissions (Autorizzazioni) del bucket Amazon S3 nella console Amazon S3.
- Utilizzo PutBucketPolicynell'API Amazon S3.
- Utilizzo della console CloudFront. Quando aggiungi un OAI alle impostazioni di origine nella CloudFront console, puoi scegliere Sì, aggiorna la policy del bucket per dire di aggiornare la policy del bucket CloudFront per tuo conto.

Se si aggiorna manualmente la policy del bucket, assicurarsi di:

- Specificare l'OAI corretto come `Principal` nella policy.
- Dare all'OAI le autorizzazioni necessarie per accedere agli oggetti per conto dei visualizzatori.

Per ulteriori informazioni, consultare le sezioni indicate di seguito.

Specificare un OAI come **`Principal`** in una policy di bucket

Per specificare un OAI come `Principal` in una policy del bucket Amazon S3, usa l'Amazon Resource Name (ARN) della OAI, che include il relativo ID. Esempio:

```
"Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <origin
 access identity ID>"
}
```

Trova l'ID OAI nella CloudFront console in Security, Origin access, Identities (legacy). In alternativa, utilizzalo ListCloudFrontOriginAccessIdentitiesnell'API. CloudFront

Concessione di autorizzazioni a una OAI

Per concedere alla OAI le autorizzazioni per accedere agli oggetti nel bucket Amazon S3, utilizzare le azioni nella policy relative a operazioni API Amazon S3 specifiche. Ad esempio, l'azione `s3:GetObject` consente all'OAI di leggere gli oggetti nel bucket. Per ulteriori informazioni, consulta gli esempi riportati nella sezione seguente oppure consulta la sezione Operazioni Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Esempi di policy del bucket Amazon S3

Gli esempi seguenti mostrano le policy dei bucket Amazon S3 che consentono a CloudFront OAI di accedere a un bucket S3.

Trova l'ID OAI nella CloudFront console in Security, Origin access, Identities (legacy). In alternativa, utilizzalo ListCloudFrontOriginAccessIdentitiesnell'API. CloudFront

Example Policy bucket Amazon S3 che fornisce l'accesso in lettura dell'OAI

L'esempio seguente consente all'OAI di leggere gli oggetti nel bucket (`s3:GetObject`) specificato.

JSON

```
{
    "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 Policy bucket Amazon S3 che fornisce all'OAI l'accesso in lettura e scrittura

L'esempio seguente consente all'OAI di leggere e scrivere oggetti nel bucket specificato (`s3:GetObject` e `s3:PutObject`). Ciò consente agli utenti di caricare file nel tuo bucket Amazon S3 tramite. CloudFront

JSON

```
{
    "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>/*"
        }
    ]
}
```

Usa oggetto Amazon S3 ACLs (non consigliato)

> **Important**
>
> Consigliamo l'utilizzo delle policy di bucket Amazon S3 per consentire a un OAI l'accesso a un bucket S3. Puoi usare le liste di controllo degli accessi (ACLs) come descritto in questa sezione, ma non è consigliabile.
> Amazon S3 consiglia di impostare S3 Object Ownership su bucket owner enforced, il che significa che ACLs sono disabilitati per il bucket e gli oggetti in esso contenuti. Quando si applica questa impostazione per la proprietà degli oggetti, è necessario utilizzare le policy del bucket per consentire l'accesso all'OAI (vedere la sezione precedente).
> La sezione seguente riguarda solo i casi d'uso precedenti che lo richiedono. ACLs

Puoi consentire a un CloudFront OAI di accedere ai file in un bucket Amazon S3 creando o aggiornando l'ACL del file nei seguenti modi:

- Utilizzo della scheda Permissions (Autorizzazioni) dell'oggetto Amazon S3 nella Console Amazon S3.
- Utilizzo PutObjectAclnell'API Amazon S3.

Quando si concede l'accesso a una OAI utilizzando un ACL, è necessario specificare l'OAI utilizzando il relativo ID utente Amazon S3 canonico. Nella CloudFront console, puoi trovare questo ID in Security, Origin access, Identities (legacy). Se utilizzi l' CloudFront API, utilizza il valore dell'`S3CanonicalUserId`elemento che è stato restituito quando hai creato l'OAI o richiama ListCloudFrontOriginAccessIdentitiesl' CloudFrontAPI.

Utilizzo di un'identità di accesso origine nelle regioni Amazon S3 che supportano solo l'autenticazione Signature Version 4

Le regioni Amazon S3 più recenti richiedono l'utilizzo di Signature Version 4 per le richieste autenticate. (Per le versioni di firma supportate in ogni regione Amazon S3, consultare Endpoint e quote Amazon Simple Storage Service nei Riferimenti generali di AWS.) Se utilizzi un'identità di accesso origine e se il bucket si trova in una delle regioni che richiedono Signature Version 4, nota quanto segue:

- Le richieste `DELETE`, `GET`, `HEAD`, `OPTIONS` e `PATCH` sono supportate senza qualifiche.
- Le richieste `POST` non sono supportate.

Limitazione dell'accesso con VPC Origins

È possibile CloudFront utilizzarlo per distribuire contenuti da applicazioni ospitate nelle sottoreti private del cloud privato virtuale (VPC). Puoi utilizzare Application Load Balancers (ALBs), Network Load Balancers (NLBs) e EC2 istanze in sottoreti private come origini VPC.

Di seguito sono riportati alcuni motivi per cui è possibile utilizzare VPC Origins:

- Sicurezza: VPC Origins è progettato per migliorare il livello di sicurezza dell'applicazione posizionando i sistemi di bilanciamento del carico e EC2 le istanze in sottoreti private, creando un unico punto di accesso. CloudFront Le richieste degli utenti passano dalle CloudFront origini del VPC tramite una connessione privata e sicura, che fornisce una sicurezza aggiuntiva per le tue applicazioni.

- Gestione: le origini VPC riducono il sovraccarico operativo richiesto per una connettività sicura tra e CloudFront origini. È possibile spostare le origini in sottoreti private senza accesso pubblico e non è necessario implementare liste di controllo degli accessi (ACLs) o altri meccanismi per limitare l'accesso alle origini. In questo modo, non è necessario investire in attività di sviluppo indifferenziate con cui proteggere le applicazioni web. CloudFront
- Scalabilità e prestazioni: VPC Origins ti aiuta a proteggere le tue applicazioni web, liberando tempo per concentrarti sulla crescita delle tue applicazioni aziendali critiche, migliorando al contempo la sicurezza e mantenendo alte prestazioni e scalabilità globale con. CloudFront VPC Origins semplifica la gestione della sicurezza e riduce la complessità operativa in modo da poterlo utilizzare CloudFront come unico punto di accesso per le applicazioni.

> **Tip**
>
> CloudFront supporta la condivisione delle origini VPC all'interno Account AWS dell'organizzazione o meno. Puoi condividere le origini del VPC dalla CloudFront console o utilizzare AWS Resource Access Manager ()AWS RAM. Per ulteriori informazioni, consulta Utilizzo di risorse condivise in CloudFront.

Prerequisiti

Prima di creare un'origine VPC per la tua CloudFront distribuzione, devi completare quanto segue:

- Crea un cloud privato virtuale (VPC) su Amazon VPC.
  - Il tuo VPC deve trovarsi in uno dei formati Regioni AWS supportati per le origini VPC. Per ulteriori informazioni, consulta Supportato Regioni AWS per le origini VPC.
  - La rete ACLs associata alle sottoreti VPC si applica al traffico in uscita (in uscita) quando la conservazione dell'indirizzo IP del client è abilitata sull'origine del VPC. Tuttavia, affinché il traffico possa uscire attraverso l'origine VPC, è necessario configurare l'ACL come regola sia in entrata che in uscita.

    Ad esempio, per consentire ai client TCP e UDP che utilizzano una porta di origine temporanea di connettersi all'endpoint tramite l'origine VPC, associa la sottorete dell'endpoint a una lista di controllo degli accessi alla rete (ACL) che consenta il traffico in uscita destinato a una porta TCP o UDP temporanea (intervallo di porte 1024-65535, destinazione 0.0.0.0/0). Inoltre, crea una regola in entrata corrispondente (intervallo di porte 1024-65535, origine 0.0.0.0/0).

Per informazioni sulla creazione di un VPC, consulta Creazione di un VPC e altre risorse VPC nella Guida per l'utente di Amazon VPC.

- Includi quanto segue nel VPC:
  - Gateway Internet: devi aggiungere un gateway Internet al VPC che contiene le risorse di origine VPC. Il gateway Internet è necessario per indicare che il VPC può ricevere traffico da Internet. Il gateway Internet non viene utilizzato per instradare il traffico verso le origini all'interno della sottorete e non è necessario aggiornare le policy di instradamento.
  - Sottorete privata con almeno un IPv4 indirizzo disponibile: effettua il CloudFront routing verso la sottorete utilizzando un'interfaccia di rete elastica (ENI) gestita dai servizi che CloudFront viene creata dopo aver definito la risorsa di origine VPC con. CloudFront È necessario disporre di almeno un IPv4 indirizzo disponibile nella sottorete privata in modo che il processo di creazione dell'ENI possa avere successo. L' IPv4 indirizzo può essere privato e non prevede costi aggiuntivi.

    > **Note**
    >
    > IPv6-solo le sottoreti non sono supportate.

- Nella sottorete privata, avvia un Application Load Balancer, un Network Load Balancer EC2 o un'istanza da usare come origine.
  - La risorsa avviata deve essere completamente distribuita e in stato Attivo prima di poterla utilizzare per un'origine VPC.
  - I Gateway Load Balancer, i Network Load Balancer dual-stack e i Network Load Balancer con listener TLS non possono essere aggiunti come origini.
  - Per essere utilizzato come un'origine VPC, un Network Load Balancer deve disporre di un gruppo di sicurezza collegato.
  - Aggiorna i tuoi gruppi di sicurezza per le origini private del VPC per consentire esplicitamente l'elenco dei prefissi CloudFront gestiti. Per ulteriori informazioni, consulta Utilizza l'elenco di prefissi gestiti CloudFront.

    > **Note**
    >
    > CloudFront-VPCOrigins-Service-SGè un nome AWS riservato per i gruppi di sicurezza utilizzati per le origini VPC. È necessario specificare un nome diverso per il gruppo di sicurezza. Per ulteriori informazioni, consulta Creazione di un gruppo di sicurezza.

- Dopo aver creato l'origine VPC, puoi limitare ulteriormente il gruppo di sicurezza per consentire solo il traffico da VPC Origins. A tale scopo, aggiorna la fonte di traffico consentita dall'elenco dei prefissi gestiti al gruppo di CloudFront sicurezza.

> **Note**
>
> WebSockets, il traffico gRPC, la richiesta di origine e i trigger di risposta all'origine con Lambda @Edge in CloudFront non sono supportati per le origini VPC. Per ulteriori informazioni, consulta Utilizzo di richieste e risposte nella documentazione di Lambda@Edge.

Creazione di un'origine VPC (nuova distribuzione)

La procedura seguente mostra come creare un'origine VPC per la nuova CloudFront distribuzione nella CloudFront console. In alternativa, puoi utilizzare le operazioni CreateVpcOrigine CreateDistributionAPI con AWS CLI o un AWS SDK.

Per creare un'origine VPC per una nuova distribuzione CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli VPC Origins, Crea origine VPC.
3. Compila i campi obbligatori. Per Origin ARN, seleziona l'ARN dell'Application Load Balancer, Network Load Balancer o dell'istanza. EC2 Se non vedi l'ARN, puoi copiare l'ARN specifico della risorsa e incollarlo qui.
4. Scegli Crea origine VPC.
5. Attendi che lo stato dell'origine VPC cambi in Implementato. Questa operazione può richiedere fino a 15 minuti.
6. Scegli Distribuzioni, Crea distribuzione.
7. Per Dominio origine, seleziona la risorsa VPC Origins dall'elenco a discesa.

   Se l'origine del VPC è un' EC2 istanza, copia e incolla il nome DNS IP privato dell'istanza nel campo Dominio di origine.
8. Completa la creazione della distribuzione. Per ulteriori informazioni, consulta Crea una CloudFront distribuzione nella console.

Creazione di un’origine VPC (distribuzione esistente)

La procedura seguente mostra come creare un'origine VPC per la CloudFront distribuzione esistente nella CloudFront console, che aiuta a garantire la disponibilità continua delle applicazioni. In alternativa, puoi utilizzare le operazioni CreateVpcOrigine UpdateDistributionWithStagingConfigAPI con AWS CLI o un AWS SDK.

Facoltativamente, puoi scegliere di aggiungere l’origine VPC alla distribuzione esistente senza creare una distribuzione temporanea.

Per creare un'origine VPC per la distribuzione esistente CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli VPC Origins, Crea origine VPC.
3. Compila i campi obbligatori. Per Origin ARN, seleziona l'ARN dell'Application Load Balancer, Network Load Balancer o dell'istanza. EC2 Se non vedi l’ARN, puoi copiare l’ARN specifico della risorsa e incollarlo qui.
4. Scegli Crea origine VPC.
5. Attendi che lo stato dell’origine VPC cambi in Implementato. Questa operazione può richiedere fino a 15 minuti.
6. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
7. Scegli l’ID della distribuzione.
8. Nella scheda Generale, in Implementazione continua, scegli Crea distribuzione di gestione temporanea. Per ulteriori informazioni, consulta Utilizza la distribuzione CloudFront continua per testare in sicurezza le modifiche alla configurazione CDN.
9. Segui le fasi della procedura guidata Creazione distribuzione di gestione temporanea per creare una distribuzione temporanea. Includi le fasi seguenti:

   - Per Origini, scegli Crea origine.
   - Per Dominio origine, seleziona la risorsa VPC Origins dal menu a discesa.

     Se l'origine del VPC è un' EC2 istanza, copia e incolla il nome DNS IP privato dell'istanza nel campo Dominio di origine.
   - Scegli Create Origin (Crea origine).
10. Nella distribuzione temporanea, verifica l’origine VPC.

11. Promuovi la configurazione della distribuzione temporanea nella distribuzione primaria. Per ulteriori informazioni, consulta Promozione di una configurazione di distribuzione temporanea.
12. Rimuovi l'accesso pubblico all'origine VPC rendendo privata la sottorete. Dopo aver eseguito questa operazione, l'origine del VPC non sarà più individuabile su Internet, ma CloudFront avrà comunque accesso privato ad essa. Per ulteriori informazioni, consulta Associare o dissociare una sottorete con una tabella di routing nella Guida per l'utente di Amazon VPC.

Aggiornamento di un'origine VPC

La procedura seguente mostra come aggiornare un'origine VPC per la CloudFront distribuzione nella CloudFront console. In alternativa, puoi utilizzare le operazioni UpdateDistributione UpdateVpcOriginAPI con AWS CLI o un AWS SDK.

Per aggiornare un'origine VPC esistente per la tua distribuzione CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
3. Scegli l'ID della distribuzione.
4. Scegli la scheda Behaviors (Comportamenti).
5. Assicurati che l'origine VPC non sia l'origine predefinita per il comportamento cache.
6. Seleziona la scheda Origins (Origini).
7. Seleziona l'origine VPC che intendi aggiornare e scegli Elimina. L'origine VPC viene dissociata dalla distribuzione. Ripeti i passaggi da 2 a 7 per dissociare l'origine VPC da qualsiasi altra distribuzione.
8. Scegli VPC Origins.
9. Seleziona l'origine VPC e scegli Modifica.
10. Effettua gli aggiornamenti e scegli Aggiorna origine VPC.
11. Attendi che lo stato dell'origine VPC cambi in Implementato. Questa operazione può richiedere fino a 15 minuti.
12. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
13. Scegli l'ID della distribuzione.
14. Seleziona la scheda Origins (Origini).
15. Scegli Create Origin (Crea origine).

16. Per Dominio origine, seleziona la risorsa VPC Origins dal menu a discesa.

    Se l'origine del VPC è un' EC2 istanza, copia e incolla il nome DNS IP privato dell'istanza nel campo Dominio di origine.

17. Scegli Create Origin (Crea origine). L’origine VPC viene nuovamente associata alla distribuzione. Ripeti i passaggi da 12 a 17 per associare l’origine VPC aggiornata a qualsiasi altra distribuzione.

Supportato Regioni AWS per le origini VPC

Le origini VPC sono attualmente supportate nelle seguenti pubblicità. Regioni AWS Sono indicate le eccezioni relative alla zona di disponibilità (AZ).

Nome della regione	Regione
Stati Uniti orientali (Ohio)	`us-east-2`
Stati Uniti orientali (Virginia settentrionale)	`us-east-1 (except AZ use1-az3)`
Stati Uniti occidentali (California settentrionale)	`us-west-1 (except AZ usw1-az2)`
Stati Uniti occidentali (Oregon)	`us-west-2`
Africa (Città del Capo)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`
Asia Pacifico (Mumbai)	`ap-south-1`
Asia Pacifico (Hyderabad)	`ap-south-2`
Asia Pacifico (Giacarta)	`ap-southeast-3`
Asia Pacifico (Melbourne)	`ap-southeast-4`
Asia Pacifico (Osaka)	`ap-northeast-3`
Asia Pacifico (Singapore)	`ap-southeast-1`
Asia Pacifico (Sydney)	`ap-southeast-2`

Nome della regione	Regione
Asia Pacifico (Tokyo)	`ap-northeast-1 (except AZ apne1-az3)`
Asia Pacifico (Seoul)	`ap-northeast-2 (except AZ apne2-az1)`
Canada (Centrale)	`ca-central-1 (except AZ cac1-az3)`
Canada occidentale (Calgary)	`ca-west-1`
Europa (Francoforte)	`eu-central-1`
Europa (Irlanda)	`eu-west-1`
Europe (Londra)	`eu-west-2`
Europa (Milano)	`eu-south-1`
Europa (Parigi)	`eu-west-3`
Europa (Spagna)	`eu-south-2`
Europa (Stoccolma)	`eu-north-1`
Europa (Zurigo)	`eu-central-2`
Israele (Tel Aviv)	`il-central-1`
Medio Oriente (Bahrein)	`me-south-1`
Medio Oriente (Emirati Arabi Uniti)	`me-central-1`
Sud America (San Paolo)	`sa-east-1`

Limitazione dell’accesso ad Application Load Balancer

Puoi utilizzare Application Load Balancer interni e con accesso a Internet con Amazon. CloudFront È possibile utilizzare Application Load Balancer interni all'interno di sottoreti private CloudFront

utilizzando origini VPC. CloudFront Le origini VPC consentono di servire contenuti da applicazioni ospitate in sottoreti VPC private senza esporli alla rete Internet pubblica. Per ulteriori informazioni, consulta Limitazione dell'accesso con VPC Origins.

Se si utilizza un Application Load Balancer CloudFront con accesso a Internet con, è possibile utilizzare le seguenti mitigazioni di sicurezza per impedire agli utenti di accedere direttamente a un Application Load Balancer e consentire l'accesso solo tramite. CloudFront

1. Configura CloudFront per aggiungere un'intestazione HTTP personalizzata alle richieste inviate all'Application Load Balancer.
2. Configura Application Load Balancer per inoltrare solo le richieste che contengono l'intestazione HTTP personalizzata.
3. Richiedi HTTPS per migliorare la sicurezza di questa soluzione.

CloudFront può anche contribuire a ridurre la latenza e persino ad assorbire alcuni attacchi Distributed Denial of Service (S)DDo.

Se il tuo caso d'uso richiede un doppio accesso alle applicazioni Web da entrambi CloudFront e da Application Load Balancer direttamente su Internet, valuta la possibilità di suddividere l'applicazione APIs Web come segue:

- APIs che deve passare. CloudFront In questo caso, valuta la possibilità di utilizzare un Application Load Balancer privato separato come origine.
- APIs che richiedono l'accesso tramite Application Load Balancer. In questo caso, si CloudFront ignora.

In alternativa, per un'applicazione Web o altri contenuti forniti da un Application Load Balancer con accesso a Internet in ELB CloudFront , puoi memorizzare nella cache gli oggetti e servirli direttamente agli utenti (visualizzatori), riducendo il carico sull'Application Load Balancer. Un bilanciatore del carico connesso a Internet ha un nome DNS risolvibile pubblicamente e instrada le richieste dei client verso le destinazioni su Internet.

Per ulteriori informazioni, consulta i seguenti argomenti. Dopo aver completato questi passaggi, gli utenti possono accedere all'Application Load Balancer solo tramite. CloudFront

Argomenti

- Configura CloudFront per aggiungere un'intestazione HTTP personalizzata alle richieste

- Configurazione di un Application Load Balancer per inoltrare solo le richieste che contengono un'intestazione specifica
- (Facoltativo) Migliorare la sicurezza di questa soluzione
- (Facoltativo) Limita l'accesso all'origine utilizzando l'elenco di prefissi AWS-managed per CloudFront

Configura CloudFront per aggiungere un'intestazione HTTP personalizzata alle richieste

È possibile CloudFront configurare l'aggiunta di un'intestazione HTTP personalizzata alle richieste inviate all'origine (in questo caso, un Application Load Balancer).

> **Important**
>
> Questo caso d'uso si basa sul mantenere segreti il nome dell'intestazione e il valore personalizzati. Se il nome e il valore dell'intestazione non sono segreti, altri client HTTP potrebbero potenzialmente includerli nelle richieste inviate direttamente a Application Load Balancer. Ciò può far sì che l'Application Load Balancer si comporti come se le richieste provenissero da CloudFront quando non provenivano. Per evitare ciò, mantieni segreti il nome dell'intestazione e il valore personalizzati.

È possibile CloudFront configurare l'aggiunta di un'intestazione HTTP personalizzata alle richieste di origine con la CloudFront console o CloudFormation l'API. CloudFront

Per aggiungere un'intestazione HTTP personalizzata (console) CloudFront

Nella CloudFront console, usa l'impostazione Origin Custom Headers nelle impostazioni di Origin. Immetti il Nome intestazione e il relativo Valore.

> **Note**
>
> In produzione, utilizza nomi e valori intestazione generati casualmente. Tratta i nomi e i valori delle intestazioni come credenziali sicure, ad esempio, nomi utente e password.

Puoi modificare l'impostazione Origin Custom Headers quando crei o modifichi un'origine per una CloudFront distribuzione esistente e quando crei una nuova distribuzione. Per ulteriori informazioni, consultare Aggiornamento di una distribuzione e Creazione di una distribuzione.

Come aggiungere un'intestazione HTTP personalizzata (CloudFormation)

In un CloudFormation modello, utilizzate la `OriginCustomHeaders` proprietà, come illustrato nell'esempio seguente.

> **Note**
>
> Il nome e il valore dell'intestazione in questo esempio sono solo per dimostrazione. In produzione, utilizza valori generati casualmente. Considera il nome e il valore dell'intestazione come credenziali protette, ad esempio un nome utente e una password.

```
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'
```

Per ulteriori informazioni, consulta Origin e OriginCustomHeaderproprietà nella Guida AWS CloudFormation per l'utente.

Per aggiungere un'intestazione HTTP (CloudFront API) personalizzata

Nell' CloudFront API, usa l'`CustomHeaders`oggetto all'interno`Origin`. Per ulteriori informazioni, consulta CreateDistributione UpdateDistributionconsulta Amazon CloudFront API Reference e la documentazione per il tuo SDK o altro client API.

Esistono alcuni nomi di intestazione che non è possibile specificare come intestazioni personalizzate di origine. Per ulteriori informazioni, consulta Intestazioni personalizzate che CloudFront non può aggiungere alle richieste di origine.

Configurazione di un Application Load Balancer per inoltrare solo le richieste che contengono un'intestazione specifica

Dopo aver CloudFront configurato l'aggiunta di un'intestazione HTTP personalizzata alle richieste inviate all'Application Load Balancer (vedi la sezione precedente), puoi configurare il load balancer per inoltrare solo le richieste che contengono questa intestazione personalizzata. A tale scopo, aggiungere una nuova regola e modificando la regola predefinita nel listener del sistema di bilanciamento del carico.

Prerequisiti

Per utilizzare le procedure seguenti, è necessario un Application Load Balancer con almeno un listener. Se non ne hai ancora creato uno, vedere Creare un Application Load Balancer nella Guida dell'utente per Application Load Balancer.

Le procedure seguenti modificano un listener HTTPS. È possibile utilizzare lo stesso processo per modificare un listener HTTP.

Per aggiornare le regole in un listener di Application Load Balancer

1. Aggiungi una nuova regola. Usa le istruzioni di Aggiungi una regola, con le seguenti modifiche:

   - Aggiungi la regola al load balancer che è l'origine della tua distribuzione. CloudFront
   - Per Aggiungi condizione, scegli Intestazione HTTP. Specificate il nome e il valore dell'intestazione HTTP che avete aggiunto come intestazione personalizzata di origine. CloudFront

- Per Aggiungi azione, scegli Inoltra a. Scegliere il gruppo target in cui si desidera inoltrare le richieste.

2. Modifica la regola predefinita nel listener del bilanciatore del carico. Usa le istruzioni di Modifica una regola, con le seguenti modifiche:

   - Modifica la regola predefinita del load balancer che è l'origine della tua distribuzione. CloudFront
   - Elimina l'azione predefinita, quindi per Aggiungi azione, scegli Restituzione risposta fissa.
   - Per Codice risposta, immettere **`403`**.
   - Per Corpo risposta, immettere **`Access denied`**.

Dopo aver completato queste fasi, il listener del bilanciatore del carico dispone di due regole. Una regola inoltra le richieste che contengono l'intestazione HTTP (richieste che provengono da). CloudFront L'altra regola invia una risposta fissa a tutte le altre richieste (richieste che non provengono da CloudFront).

Puoi verificare che la soluzione funzioni inviando una richiesta alla tua CloudFront distribuzione e una all'Application Load Balancer. La richiesta di CloudFront restituzione dell'applicazione o del contenuto Web e quella inviata direttamente all'Application Load Balancer restituiscono una `403` risposta con un messaggio di testo semplice. `Access denied`

(Facoltativo) Migliorare la sicurezza di questa soluzione

Per migliorare la sicurezza di questa soluzione, puoi configurare la tua CloudFront distribuzione in modo che utilizzi sempre HTTPS quando invii richieste all'Application Load Balancer. Ricorda che questa soluzione funziona solo se si mantengono segreti il nome dell'intestazione e il valore personalizzati. L'utilizzo di HTTPS può aiutare a impedire a un intercettore di scoprire il nome e il valore dell'intestazione. Si consiglia inoltre di ruotare periodicamente il nome e il valore dell'intestazione.

Usa HTTPS per le richieste di origine

CloudFront Per configurare l'utilizzo di HTTPS per le richieste di origine, imposta l'impostazione Origin Protocol Policy su Solo HTTPS. Questa impostazione è disponibile nella CloudFront console CloudFormation e nell' CloudFront API. Per ulteriori informazioni, consulta Protocollo (solo origini personalizzate).

Quanto segue si applica anche quando si configura l'utilizzo CloudFront di HTTPS per le richieste di origine:

- È necessario CloudFront configurare l'inoltro dell'`Host`intestazione all'origine con la policy di richiesta di origine. È possibile utilizzare la policy di richiesta di origine AllViewer gestita.
- Assicurati che Application Load Balancer disponga di un listener HTTPS (come illustrato nella sezione precedente). Per ulteriori informazioni, consulta la sezione relativa alla creazione di un listener HTTPS nella Guida utente per Application Load Balancer. L'utilizzo di un listener HTTPS richiede un SSL/TLS certificato che corrisponda al nome di dominio indirizzato all'Application Load Balancer.
- I certificati SSL/TLS per CloudFront possono essere richiesti (o importati) solo in (ACM). `us-east-1` Regione AWS AWS Certificate Manager CloudFront Trattandosi di un servizio globale, distribuisce automaticamente il certificato dalla `us-east-1` regione a tutte le regioni associate alla distribuzione. CloudFront
  - Ad esempio, se disponi di un Application Load Balancer (ALB) nella `ap-southeast-2` regione, devi configurare SSL/TLS i certificati sia nella `ap-southeast-2` regione (per utilizzare HTTPS tra CloudFront e l'origine ALB) che `us-east-1` nella regione (per utilizzare HTTPS tra i visualizzatori e). CloudFront Entrambi i certificati devono corrispondere al nome di dominio che viene instradato ad Application Load Balancer. Per ulteriori informazioni, consulta Regione AWS per AWS Certificate Manager.
- Se gli utenti finali (noti anche come visualizzatori o client) della tua applicazione Web possono utilizzare HTTPS, puoi anche configurare CloudFront per preferire (o addirittura richiedere) le connessioni HTTPS degli utenti finali. A tale scopo, utilizzare l'impostazione del criterio del protocollo Viewer. È possibile impostarlo per reindirizzare gli utenti finali da HTTP a HTTPS o per rifiutare le richieste che utilizzano HTTP. Questa impostazione è disponibile nella CloudFront console e CloudFormation nell' CloudFront API. Per ulteriori informazioni, consulta Viewer Protocol Policy (Policy protocollo visualizzatore).

Ruotare il nome e il valore dell'intestazione

Oltre a utilizzare HTTPS, si consiglia anche di ruotare periodicamente il nome e il valore dell'intestazione. I passaggi di alto livello per eseguire questa operazione sono i seguenti:

1. Configura CloudFront per aggiungere un'intestazione HTTP personalizzata aggiuntiva alle richieste inviate all'Application Load Balancer.

2. Aggiornare la regola del listener Application Load Balancer per inoltrare le richieste che contengono questa intestazione HTTP personalizzata aggiuntiva.
3. Configura CloudFront per interrompere l'aggiunta dell'intestazione HTTP personalizzata originale alle richieste inviate all'Application Load Balancer.
4. Aggiornare la regola del listener di Application Load Balancer per interrompere l'inoltro delle richieste contenenti l'intestazione HTTP personalizzata originale.

Per ulteriori informazioni sull'esecuzione di questi passaggi, vedere le sezioni precedenti.

(Facoltativo) Limita l'accesso all'origine utilizzando l'elenco di prefissi AWS-managed per CloudFront

Per limitare ulteriormente l'accesso all'Application Load Balancer, è possibile configurare il gruppo di sicurezza associato all'Application Load Balancer in modo che accetti solo il traffico CloudFront proveniente da quando il servizio utilizza AWS un elenco di prefissi -managed. Ciò impedisce al traffico non originario di raggiungere l'Application Load Balancer a livello di rete (livello 3) o di trasporto (livello 4). CloudFront

Per ulteriori informazioni, consulta il post del CloudFront blog Limita l'accesso alle tue origini utilizzando l'elenco dei prefissi AWS-managed per Amazon.

Limitazione della distribuzione geografica del contenuto

Puoi utilizzare le restrizioni geografiche, a volte note come blocchi geografici, per impedire agli utenti di aree geografiche specifiche di accedere ai contenuti che distribuisci tramite una distribuzione Amazon CloudFront . Per utilizzare le restrizioni geografiche, sono disponibili due opzioni:

- Utilizza la funzione di restrizioni CloudFront geografiche. Utilizzare questa opzione per limitare l'accesso a tutti i file associati a una distribuzione e per limitare l'accesso a livello di Paese.
- Utilizzare un servizio di geolocalizzazione di terze parti. Utilizza questa opzione per limitare l'accesso a un sottoinsieme dei file associati a una distribuzione o per limitare l'accesso a un livello più dettagliato che a livello di paese.

Argomenti

- Usa restrizioni CloudFront geografiche

- Utilizzo di un servizio di geolocalizzazione di terze parti

Usa restrizioni CloudFront geografiche

Quando un utente richiede i tuoi contenuti, CloudFront in genere fornisce il contenuto richiesto indipendentemente da dove si trova l'utente. Se devi impedire agli utenti di determinati paesi di accedere ai tuoi contenuti, puoi utilizzare la funzionalità di restrizioni CloudFront geografiche per eseguire una delle seguenti operazioni:

- Accordare agli utenti il permesso di accedere al contenuto solo se si trovano in uno dei Paesi inclusi in una lista di Paesi consentiti.
- Impedire agli utenti di accedere al contenuto se si trovano in uno dei Paesi inclusi in un elenco di Paesi rifiutati.

Ad esempio, se una richiesta proviene da un paese in cui non sei autorizzato a distribuire i tuoi contenuti, puoi utilizzare le restrizioni CloudFront geografiche per bloccare la richiesta.

> **Note**
>
> CloudFront determina la posizione degli utenti utilizzando un database di terze parti. La precisione della mappatura tra indirizzi IP e paesi varia in base alla regione. Sulla base di test recenti, la precisione globale è del 99,8%. Se non è in CloudFront grado di determinare la posizione di un utente, CloudFront fornisce il contenuto richiesto dall'utente.

Di seguito viene descritto il funzionamento delle restrizioni geografiche:

1. Supponiamo che hai i diritti per distribuire il tuo contenuto solo in Liechtenstein. Aggiorna la tua CloudFront distribuzione per aggiungere una lista consentita che contiene solo il Liechtenstein. In alternativa, puoi aggiungere un elenco di Paesi rifiutati che contiene ogni Paese eccetto il Liechtenstein.
2. Un utente di Monaco richiede i tuoi contenuti e il DNS indirizza la richiesta a una CloudFront edge location a Milano, Italia.
3. La posizione edge a Milano cerca la distribuzione e determina che l'utente a Monaco non ha l'autorizzazione per scaricare il contenuto.
4. CloudFront restituisce un codice di stato HTTP `403 (Forbidden)` all'utente.

Facoltativamente, è possibile CloudFront configurare la restituzione di un messaggio di errore personalizzato all'utente e specificare per quanto tempo si desidera CloudFront memorizzare nella cache la risposta all'errore per il file richiesto. Il valore predefinito è 10 secondi. Per ulteriori informazioni, consulta Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici.

Le restrizioni geografiche sono applicabili a un'intera distribuzione. Se devi applicare una restrizione a una parte dei tuoi contenuti e una restrizione diversa (o nessuna restrizione) a un'altra parte dei tuoi contenuti, devi creare CloudFront distribuzioni separate o utilizzare un servizio di geolocalizzazione di terze parti.

Se abiliti i log CloudFront standard (log di accesso), puoi identificare le richieste CloudFront rifiutate cercando le voci di registro in cui è riportato il valore di (il codice di `sc-status` stato HTTP). `403` Tuttavia, utilizzando solo i log standard, non è possibile distinguere una richiesta CloudFront rifiutata in base alla posizione dell'utente da una richiesta CloudFront rifiutata perché l'utente non aveva l'autorizzazione ad accedere al file per un altro motivo. Se disponi di un servizio di geolocalizzazione di terze parti come Digital Element or MaxMind, puoi identificare la posizione delle richieste in base all'indirizzo IP nella colonna `c-ip` (IP client) nei log di accesso. Per ulteriori informazioni sui log CloudFront standard, vedere. Registri di accesso (registri standard)

La procedura seguente spiega come utilizzare la CloudFront console per aggiungere restrizioni geografiche a una distribuzione esistente. Per informazioni su come utilizzare la console per creare una distribuzione, consulta Creazione di una distribuzione.

Per aggiungere restrizioni geografiche alla tua distribuzione CloudFront web (console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, scegli Distribuzioni, quindi scegli la distribuzione che desideri aggiornare.
3. Scegli la scheda Sicurezza, quindi scegli Restrizioni geografiche.
4. Scegli Modifica.
5. Seleziona Allow list (Elenco consentiti) per creare un elenco di Paesi consentiti, oppure Block list (Elenco di blocchi) per creare un elenco di Paesi bloccati.
6. Aggiungi i Paesi desiderati all'elenco, quindi scegli Save changes (Salva modifiche).

Utilizzo di un servizio di geolocalizzazione di terze parti

Con la funzione di restrizioni CloudFront geografiche, puoi controllare la distribuzione dei tuoi contenuti a livello nazionale per tutti i file che distribuisci con una determinata distribuzione web. Se hai un caso d'uso per le restrizioni geografiche in cui le restrizioni non seguono i confini nazionali o se desideri limitare l'accesso solo ad alcuni dei file che servi tramite una determinata distribuzione, puoi utilizzare un servizio di geolocalizzazione di terze parti. CloudFront Puoi così avere il controllo del contenuto in base non solo al Paese ma anche alla città, al CAP o persino alla latitudine e longitudine.

Quando utilizzi un servizio di geolocalizzazione di terze parti, ti consigliamo di utilizzare CloudFront signedURLs, con il quale puoi specificare una data e un'ora di scadenza dopo le quali l'URL non è più valido. Inoltre, ti consigliamo di utilizzare un bucket Amazon S3 come origine perché puoi quindi utilizzare un controllo di accesso di CloudFront origine per impedire agli utenti di accedere ai tuoi contenuti direttamente dall'origine. Per ulteriori informazioni sul controllo degli accessi firmati URLs e di origine, consulta. Offri contenuti privati con cookie firmati URLs e firmati

La procedura seguente descrive come controllare l'accesso ai file utilizzando un servizio di geolocalizzazione di terza parte.

Per utilizzare un servizio di geolocalizzazione di terze parti per limitare l'accesso ai file di una distribuzione CloudFront

1. Ottieni un account con un servizio di geolocalizzazione.
2. Carica il tuo contenuto in un bucket Amazon S3 (S3).
3. Configura Amazon CloudFront e Amazon S3 per offrire contenuti privati. Per ulteriori informazioni, consulta Offri contenuti privati con cookie firmati URLs e firmati.
4. Scrivi la tua applicazione Web per eseguire le operazioni seguenti:

   - Inviare l'indirizzo IP per ogni richiesta utente al servizio di geolocalizzazione.
   - Valuta il valore restituito dal servizio di geolocalizzazione per determinare se l'utente si trova in un luogo in cui desideri CloudFront distribuire i tuoi contenuti.
   - Se desideri distribuire i tuoi contenuti nella posizione dell'utente, genera un URL firmato per i tuoi CloudFront contenuti. Se non si desidera distribuire i contenuti in tale posizione, restituire il codice di stato HTTP `403 (Forbidden)` all'utente. In alternativa, puoi CloudFront configurare la restituzione di un messaggio di errore personalizzato. Per ulteriori informazioni, consulta the section called “Creazione di una pagina di errore personalizzata per codici di stato HTTP specifici”.

Per ulteriori informazioni, consulta la documentazione del servizio di geolocalizzazione che stai utilizzando.

Puoi utilizzare una variabile di server Web per ottenere gli indirizzi IP degli utenti che visitano il tuo sito Web. Nota quanto segue:

- Se il tuo server Web non è connesso a Internet attraverso un sistema di bilanciamento del carico, puoi utilizzare una variabile di server Web per ottenere l'indirizzo IP remoto. Tuttavia, questo indirizzo IP non è sempre l'indirizzo IP dell'utente. Può anche essere l'indirizzo IP di un server proxy, a seconda di come l'utente è connesso a Internet.
- Se il server Web è connesso a Internet attraverso un sistema di bilanciamento del carico, una variabile di server Web potrebbe contenere l'indirizzo IP del sistema di bilanciamento del carico e non l'indirizzo IP dell'utente. In questa configurazione, consigliamo di utilizzare l'ultimo indirizzo IP nell'intestazione HTTP `X-Forwarded-For`. Questa intestazione in genere contiene più di un indirizzo IP, molti dei quali sono per proxy o sistemi di bilanciamento del carico. L'ultimo indirizzo IP nell'elenco è quello che probabilmente è associato alla posizione geografica dell'utente.

Se il server Web non è connesso a un sistema di bilanciamento del carico, ti consigliamo di utilizzare variabili di server Web anziché l'intestazione `X-Forwarded-For` per evitare lo spoof di indirizzi IP.

Utilizzo della crittografia a livello di campo per la protezione dei dati sensibili

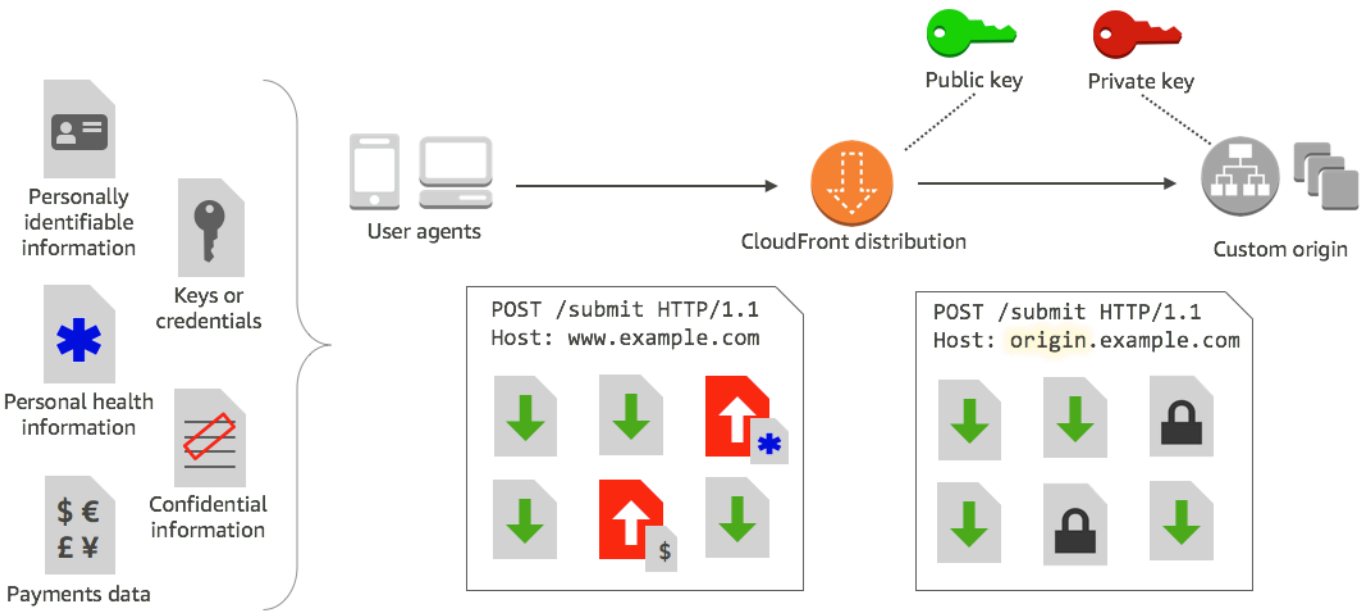
Con Amazon CloudFront, puoi applicare end-to-end connessioni sicure ai server di origine utilizzando HTTPS. La crittografia a livello di campo aggiunge un ulteriore livello di sicurezza che consente di proteggere dati specifici durante l'elaborazione del sistema, di modo che solo alcune applicazioni possano visualizzarli.

La crittografia a livello di campo consente agli utenti di caricare in modo sicuro informazioni sensibili nel server Web. Le informazioni sensibili fornite dagli utenti sono crittografate a livello di edge, vicino all'utente e rimangono crittografate in tutto lo stack di applicazioni. Questa crittografia garantisce che solo le applicazioni che necessitano dei dati, e dispongono delle credenziali per decrittarli, siano in grado di farlo.

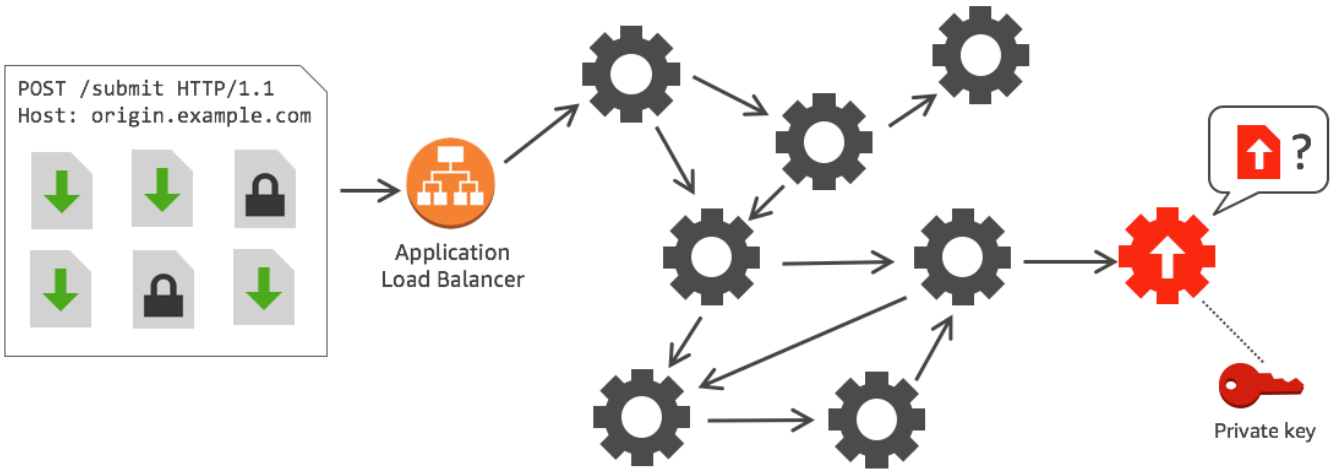
Per utilizzare la crittografia a livello di campo, quando configuri la CloudFront distribuzione, specifica il set di campi nelle richieste POST che desideri crittografare e la chiave pubblica da utilizzare per crittografarle. Puoi crittografare fino a 10 campi dati in una richiesta Non puoi crittografare tutti i dati in una richiesta con la crittografia a livello di campo; devi specificare singoli campi da crittografare.

Quando la richiesta HTTPS con crittografia a livello di campo viene inoltrata all'origine e la richiesta viene instradata al sottosistema o all'applicazione di origine, i dati sensibili sono ancora crittografati, riducendo il rischio di violazione o di perdita accidentale di dati sensibili. I componenti che richiedono l'accesso ai dati sensibili per ragioni commerciali, come un sistema di elaborazione dei pagamenti che richiede un numero di carta di credito, possono utilizzare la chiave privata appropriata per decrittografare i dati e accedervi.

> **Note**
>
> Per utilizzare la crittografia a livello di campo, la tua origine deve supportare la codifica in blocchi.



CloudFront la crittografia a livello di campo utilizza la crittografia asimmetrica, nota anche come crittografia a chiave pubblica. Fornisci una chiave pubblica e tutti i dati sensibili che specifichi vengono crittografati automaticamente. CloudFront La chiave fornita CloudFront non può essere utilizzata per decrittografare i valori crittografati; solo la tua chiave privata può farlo.



Argomenti

- Panoramica della crittografia a livello di campo
- Configurazione della crittografia a livello di campo
- Decrittografia dei campi dati nell'origine

Panoramica della crittografia a livello di campo

Di seguito viene fornita una panoramica della configurazione della crittografia a livello di campo. Per informazioni su specifiche fasi, consulta Configurazione della crittografia a livello di campo.

1. Ottieni una coppia chiave pubblica-chiave privata. Devi ottenere e aggiungere la chiave pubblica prima di iniziare la configurazione della crittografia a livello di campo in CloudFront.
2. Crea un profilo di crittografia a livello di campo. I profili di crittografia a livello di campo, utilizzati dall'utente CloudFront, definiscono i campi da crittografare.
3. Crea una configurazione di crittografia a livello di campo. Una configurazione specifica i profili da utilizzare, in base al tipo di contenuto della richiesta o a un argomento di query, per crittografare specifici campi dati. È inoltre possibile scegliere le opzioni di comportamento di inoltro richieste desiderate per diversi scenari. Ad esempio, è possibile impostare il comportamento in base al quale il nome del profilo specificato dall'argomento di interrogazione in un URL di richiesta non esiste in. CloudFront

4. Crea un collegamento a un comportamento cache. Collega la configurazione a un comportamento cache per una distribuzione, in modo da specificare quando CloudFront deve crittografare i dati.

Configurazione della crittografia a livello di campo

Segui le fasi riportate di seguito per iniziare a utilizzare la crittografia a livello di campo. Per informazioni sulle quote (precedentemente note come limiti) relative alla crittografia a livello di campo, consulta Quote.

- Fase 1: Creare una coppia di chiavi RSA
- Passaggio 2: aggiungi la tua chiave pubblica a CloudFront
- Fase 3. Creazione di un profilo per la crittografia a livello di campo
- Fase 4: Creazione di una configurazione
- Fase 5. Aggiunta di una configurazione a un comportamento cache

Fase 1: Creare una coppia di chiavi RSA

Per iniziare, è necessario creare una coppia di chiavi RSA che include una chiave pubblica e una chiave privata. La chiave pubblica consente di CloudFront crittografare i dati e la chiave privata consente ai componenti all'origine di decrittografare i campi che sono stati crittografati. Per creare una coppia di chiavi, puoi utilizzare OpenSSL o un altro strumento. La dimensione della chiave deve essere 2048 bit.

Ad esempio, se utilizzi OpenSSL, puoi utilizzare il seguente comando per generare una coppia di chiavi con una lunghezza di 2048 bit e salvarla nel file `private_key.pem`:

```
openssl genrsa -out private_key.pem 2048
```

Il file risultante contiene la chiave pubblica e quella privata. Per estrarre la chiave pubblica da quel file, esegui il seguente comando:

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Il file della chiave pubblica (`public_key.pem`) contiene il valore della chiave codificata che verrà incollato nella fase seguente.

Passaggio 2: aggiungi la tua chiave pubblica a CloudFront

Dopo aver ottenuto la coppia di chiavi RSA, aggiungi la tua chiave pubblica a CloudFront.

Per aggiungere la tua chiave pubblica a CloudFront (console)

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Public key (Chiave pubblica).
3. Scegli Add public key (Aggiungi chiave pubblica).
4. Per Key name (Nome chiave), digita un nome univoco per la chiave. Il nome non può contenere spazi e può includere solo caratteri alfanumerici, di sottolineatura (_) e trattini (-). Il numero massimo di caratteri è 128.
5. Per Key value (Valore chiave), incollare il valore della chiave codificata per la chiave pubblica, incluse le righe `-----BEGIN PUBLIC KEY-----` e `-----END PUBLIC KEY-----`.
6. Per Comment (Commento), aggiungi un commento facoltativo. Ad esempio, la data di scadenza della chiave pubblica.
7. Scegliere Aggiungi.

È possibile aggiungere altre chiavi da utilizzare CloudFront ripetendo i passaggi della procedura.

Fase 3. Creazione di un profilo per la crittografia a livello di campo

Dopo aver aggiunto almeno una chiave pubblica CloudFront, create un profilo che indichi CloudFront quali campi crittografare.

Creazione di un profilo per la crittografia a livello di campo (console)

1. Nel riquadro di navigazione, scegli Field-level encryption (Crittografia a livello di campo).
2. Scegli Create profile (Crea profilo).
3. Riempi i seguenti campi:

   Nome del profilo

   Digita un nome univoco per il profilo. Il nome non può contenere spazi e può includere solo caratteri alfanumerici, di sottolineatura (_) e trattini (-). Il numero massimo di caratteri è 128.

Public key name (Nome chiave pubblica)

Nell'elenco a discesa, scegli il nome di una chiave pubblica a cui hai aggiunto CloudFront nel passaggio 2. CloudFront utilizza la chiave per crittografare i campi specificati in questo profilo.

Nome del provider

Digitare una descrizione che consenta di identificare la chiave, ad esempio il provider dove hai ottenuto la coppia di chiavi. Questa informazione, insieme alla chiave privata, è necessaria quando le applicazioni decrittano i campi di dati. Il nome di provider non può contenere spazi e può includere solo caratteri alfanumerici, due punti (:), caratteri di sottolineatura (_) e trattini (-). Il numero massimo di caratteri è 128.

Field name pattern to match (Modello di nome di campo da abbinare)

Digita i nomi di campi dati, oppure i modelli che identificano i nomi di campi dati nella richiesta, che CloudFront deve crittografare. Scegli l'opzione + per aggiungere tutti i campi che desideri crittografare con questa chiave.

Per lo schema del nome del campo, puoi digitare il nome completo del campo dati, ad esempio DateOfBirth, o solo la prima parte del nome con un carattere jolly (*), ad esempio CreditCard *. Il modello di nome di campo deve includere solo caratteri alfanumerici, parentesi quadre ([e]), punti (.), caratteri di sottolineatura (_) e trattini (-), oltre al carattere jolly facoltativo (*).

Assicurati di non utilizzare caratteri che si sovrappongono per diversi modelli di nome di campo. Ad esempio, se disponi di un modello di nome di campo ABC*, non puoi aggiungere un altro modello di nome di campo AB*. Inoltre, i nomi di campo fanno distinzione tra maiuscole e minuscole e il numero massimo di caratteri che puoi utilizzare è 128.

Commento

(Facoltativo) Digita un commento sul profilo. Il numero massimo di caratteri che puoi utilizzare è 128.

4. Dopo che hai riempito i campi, scegli Create profile (Crea profilo).
5. Se desideri aggiungere ulteriori profili, scegli Add profile (Aggiungi profilo).

Fase 4: Creazione di una configurazione

Dopo aver creato uno o più profili di crittografia a livello di campo, create una configurazione che specifichi il tipo di contenuto della richiesta che include i dati da crittografare, il profilo da utilizzare per la crittografia e altre opzioni che specificano come gestire la crittografia. CloudFront

Ad esempio, quando non è CloudFront possibile crittografare i dati, è possibile specificare se bloccare o CloudFront inoltrare una richiesta all'origine nei seguenti scenari:

- Quando il tipo di contenuto di una richiesta non è in una configurazione: se non hai aggiunto un tipo di contenuto a una configurazione, puoi specificare se CloudFront inoltrare la richiesta con quel tipo di contenuto all'origine senza crittografare i campi di dati oppure bloccare la richiesta e restituire un errore.

  > **Note**
  >
  > Se aggiungi un tipo di contenuto a una configurazione ma non hai specificato un profilo da utilizzare con quel tipo, inoltra CloudFront sempre le richieste con quel tipo di contenuto all'origine.

- Quando il nome di profilo fornito in un argomento di query è sconosciuto: quando specifichi l'argomento della `fle-profile` query con un nome di profilo che non esiste per la tua distribuzione, puoi CloudFront specificare se inviare la richiesta all'origine senza crittografare i campi di dati oppure bloccare la richiesta e restituire un errore.

In una configurazione, puoi anche specificare se fornire un profilo come argomento di query in un URL sostituisce un profilo che hai mappato al tipo di contenuto per quella query. Per impostazione predefinita, CloudFront utilizza il profilo che hai mappato a un tipo di contenuto, se ne specifichi uno. Ciò ti consente di avere un profilo che viene utilizzato per impostazione predefinita ma di decidere, per alcune richieste, di applicare un altro profilo.

Quindi, ad esempio, puoi specificare nella tua configurazione **`SampleProfile`** come il profilo di argomento di query da utilizzare. Quindi puoi utilizzare l'URL `https://d1234.cloudfront.net?fle-profile=SampleProfile` anzichéhttps://d1234.cloudfront.net, da CloudFront utilizzare **`SampleProfile`** per questa richiesta, anziché il profilo che configureresti per il tipo di contenuto della richiesta.

Puoi creare fino a 10 configurazioni per un singolo account e quindi associare una delle configurazioni al comportamento cache di qualsiasi distribuzione per l'account.

Creazione di una configurazione per la crittografia a livello di campo (console)

1. Nella pagina Field-level encryption (Crittografia a livello di campo), scegli Create configuration (Crea configurazione).

   Nota: se non hai creato almeno un profilo, l'opzione per la creazione di una configurazione non sarà visualizzata.

2. Riempi i campi riportati di seguito per specificare il profilo da utilizzare Alcuni campi non possono essere modificati.

   Content type (Tipo di contenuto) (non modificabile)

   Il tipo di contenuto è impostato su `application/x-www-form-urlencoded` e non può essere modificato.

   Default profile ID (ID profilo di default) (facoltativo)

   Nell'elenco a discesa, scegli il profilo che intendi mappare al tipo di contenuto nel campo Content type (Tipo di contenuto).

   Content format (Formato contenuto) (non modificabile)

   Il formato del contenuto è impostato su `URLencoded` e non può essere modificato.

3. Se desideri modificare il comportamento CloudFront predefinito per le seguenti opzioni, seleziona la casella di controllo appropriata.

   Forward request to origin when request's content type is not configured (Inoltra richiesta all'origine quando il tipo di contenuto non è configurato)

   Seleziona la casella di controllo per consentire l'inoltro della richiesta all'origine se non hai specificato un profilo da utilizzare per il tipo di contenuto della richiesta.

   Override the profile for a content type with a provided query argument (Sovrascrivi il profilo per un tipo di contenuto con un argomento di query fornito)

   Seleziona la casella di controllo per consentire a un profilo fornito in un argomento di query di sovrascrivere il profilo che hai specificato per un tipo di contenuto.

4. Se selezioni la casella di controllo per consentire a un argomento di query di sovrascrivere il profilo di default, devi riempire i seguenti campi aggiuntivi per la configurazione. Puoi creare fino a cinque di queste mappature di argomento di query da utilizzare con le query.

Query argument (Argomento di query)

Digitate il valore che desiderate includere nell' URLs argomento della `fle-profile` query. Questo valore indica a CloudFront di utilizzare l'ID profilo (che specifichi nel campo successivo) associato a questo argomento di query per la crittografia a livello di campo di questa query.

Il numero massimo di caratteri che puoi utilizzare è 128. Questo valore non può contenere spazi e deve utilizzare solo caratteri alfanumerici o i seguenti caratteri: trattini (-), punti (.), caratteri di sottolineatura (_), asterischi (*), segni più (+), percentuali (%).

Profile ID (ID profilo)

Nell'elenco a discesa, scegli il profilo da associare al valore che hai digitato per Query argument (Argomento di query).

Forward request to origin when the profile specified in a query argument does not exist (Inoltra richiesta all'origine quando il profilo specificato in un argomento di query non esiste)

Seleziona la casella di controllo per consentire l'inoltro della richiesta all'origine se il profilo specificato in un argomento di query non è definito in CloudFront.

Fase 5. Aggiunta di una configurazione a un comportamento cache

Per utilizzare la crittografia a livello di campo, collega una configurazione a un comportamento cache per una distribuzione aggiungendo l'ID configurazione come valore per la distribuzione.

Important

Per collegare una configurazione di crittografia a livello di campo a un comportamento della cache, la distribuzione deve essere configurata per utilizzare sempre HTTPS e per accettare HTTP e richieste `POST` e `PUT` dai visualizzatori. Deve essere vera una delle condizioni seguenti:

- Viewer Protocol Policy (Policy protocollo visualizzatore) del comportamento della cache deve essere impostato su Redirect HTTP to HTTPS (Reindirizza HTTP a HTTPS) o su HTTPS Only (Solo HTTPS). (In CloudFormation o nell' CloudFront API, `ViewerProtocolPolicy` deve essere impostato su `redirect-to-https` o`https-only`.)

- Il valore Allowed HTTP Methods (Metodi HTTP consentiti) del comportamento della cache deve essere impostato su GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. (In CloudFormation o l' CloudFront API, `AllowedMethods` deve essere impostato su `GETHEAD,OPTIONS,PUT,POST,PATCH,DELETE`. Questi possono essere specificati in qualsiasi ordine.)
- Origin Protocol Policy (Policy protocollo origine) delle impostazioni dell'origine deve essere impostato su Match Viewer (Corrispondenza visualizzatore) o HTTPS Only (Solo HTTPS). (In CloudFormation o nell' CloudFront API, `OriginProtocolPolicy` deve essere impostato su `match-viewer` o`https-only`.)

Per ulteriori informazioni, consulta Riferimento a tutte le impostazioni di distribuzione.

Decrittografia dei campi dati nell'origine

CloudFront crittografa i campi di dati utilizzando. AWS Encryption SDK I dati rimangono crittografati nell'intero stack di applicazioni e sono accessibili solo alle applicazioni che dispongono delle credenziali per decrittografarli.

Dopo la crittografia, il testo cifrato è codificato in base64. Quando le applicazioni eseguono la decrittazione del testo nell'origine, devono prima decodificarlo e quindi utilizzare il kit SDK di crittografia AWS per decrittare i dati.

Il codice di esempio che segue illustra il modo in cui le applicazioni possono decrittare i dati nell'origine. Tieni presente quanto segue:

- Per semplificare l'esempio, le chiavi private e pubbliche (in formato DER) vengono caricate dai file nella directory di lavoro. In pratica, devi archiviare la chiave privata in una posizione offline protetta, ad esempio un modulo di protezione hardware offline, e distribuire la chiave pubblica al team di sviluppo.
- CloudFront utilizza informazioni specifiche durante la crittografia dei dati e lo stesso set di parametri deve essere utilizzato all'origine per decrittografarli. I parametri CloudFront utilizzati durante l'inizializzazione includono quanto segue: MasterKey
  - PROVIDER_NAME: hai specificato questo valore quando hai creato un profilo di crittografia a livello di campo. Utilizza lo stesso valore qui.
  - KEY_NAME: hai creato un nome per la tua chiave pubblica quando l'hai caricata su CloudFront, quindi hai specificato il nome della chiave nel profilo. Utilizza lo stesso valore qui.

- ALGORITMO: CloudFront utilizza `RSA/ECB/OAEPWithSHA-256AndMGF1Padding` come algoritmo per la crittografia, quindi è necessario utilizzare lo stesso algoritmo per decrittografare i dati.

- Se esegui il codice di esempio riportato di seguito con il testo cifrato come input, i dati decrittati vengono inviati alla console. Per ulteriori informazioni, consulta il codice di esempio Java nell'Encryption SDK. AWS

Codice di esempio

```
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));
    }
}
```

Video on demand e video in streaming live con CloudFront

Puoi utilizzarlo CloudFront per fornire video on demand (VOD) o video in streaming live utilizzando qualsiasi origine HTTP. Un modo per configurare i flussi di lavoro video nel cloud consiste nell'utilizzarli CloudFront insieme a AWS Media Services.

Argomenti

Informazioni sullo streaming video

È necessario utilizzare un codificatore per creare pacchetti di contenuti video prima di CloudFront poterli distribuire. Il processo di pacchettizzazione crea segmenti contenenti contenuti audio, video e sottotitoli. Genera anche file manifest, che descrivono in un ordine specifico quali segmenti riprodurre e quando. I formati più comuni per i pacchetti sono MPEG DASH, Apple HLS, Microsoft Smooth Streaming e CMAF.

streaming VOD

Per lo streaming VOD, i contenuti video vengono archiviati su un server e i visualizzatori possono guardarli in qualsiasi momento. Per creare una risorsa che i visualizzatori possono trasmettere in streaming, utilizzare un codificatore, ad esempio AWS Elemental MediaConvert, per formattare e impacchettare i file multimediali.

Dopo aver impacchettato il video nei formati corretti, puoi archiviarlo su un server o in un bucket Amazon S3 e distribuirlo come richiesto dagli CloudFront spettatori.

Streaming di video live

Per lo streaming video live, i contenuti video vengono trasmessi in streaming in tempo reale quando si verificano eventi dal vivo o sono impostati come canale live 24x7. Per creare output live per la trasmissione e la distribuzione in streaming, utilizza un codificatore, ad esempio AWS Elemental MediaLive, per comprimere il video e formattarlo per i dispositivi di visualizzazione.

Dopo aver codificato il video, puoi archiviarlo AWS Elemental MediaStore o convertirlo in diversi formati di distribuzione utilizzando. AWS Elemental MediaPackage Utilizza una di queste origini per configurare una CloudFront distribuzione per distribuire i contenuti. Per procedure e linee guida specifiche per la creazione di distribuzioni che funzionano con questi servizi, consulta Pubblica video utilizzandolo AWS Elemental MediaStore come origine e Distribuzione di video live formattati con AWS Elemental MediaPackage.

Wowza e Unified Streaming forniscono anche strumenti con cui puoi utilizzare per lo streaming di video. CloudFront Per ulteriori informazioni sull'utilizzo di Wowza con CloudFront, consulta Bring your Wowza Streaming Engine license to CloudFront live HTTP streaming sul sito web dedicato alla documentazione di Wowza. Per informazioni sull'utilizzo di Unified Streaming with CloudFront per lo streaming VOD, consulta il sito Web dedicato alla documentazione di Unified Streaming. CloudFront

Distribuisci video su richiesta con CloudFront

Per fornire streaming di video on demand (VOD) con CloudFront, utilizza i seguenti servizi:

- Amazon S3 per memorizzare il contenuto nel suo formato originale e per memorizzare il video transcodificato.
- Un codificatore (ad esempio AWS Elemental MediaConvert) per transcodificare il video in formati di streaming.
- CloudFront per distribuire il video transcodificato agli spettatori. Per Microsoft Smooth Streaming, vedere Configurazione di video on demand per Microsoft Smooth Streaming.

Per creare una soluzione VOD con CloudFront

1. Carica il tuo contenuto in un bucket Amazon S3 (S3). Per ulteriori informazioni su come lavorare con Amazon S3, consulta la Guida per l'utente di Amazon Simple Storage Service.
2. Transcodifica i tuoi contenuti utilizzando un MediaConvert job. Il lavoro converte il video nei formati richiesti dai lettori utilizzati dagli spettatori. È inoltre possibile utilizzare il processo per creare risorse che variano in risoluzione e bitrate. Queste risorse vengono utilizzate per lo streaming con bitrate adattivo (ABR), che regola la qualità di visualizzazione in base alla larghezza di banda disponibile dello spettatore. MediaConvert archivia il video transcodificato in un bucket S3.
3. Distribuisci i contenuti convertiti utilizzando una distribuzione. CloudFront Gli spettatori possono guardare i contenuti su qualsiasi dispositivo, in qualsiasi momento.

Configurazione di video on demand per Microsoft Smooth Streaming

Sono disponibili le seguenti opzioni CloudFront da utilizzare per distribuire contenuti video on demand (VOD) transcodificati nel formato Microsoft Smooth Streaming:

- Specificare un server Web che esegue Microsoft IIS e supporti Smooth Streaming come origine per la distribuzione.
- Abilita Smooth Streaming nei comportamenti della cache di una distribuzione. CloudFront Poiché è possibile utilizzare più comportamenti della cache in una distribuzione, è possibile utilizzare una distribuzione per file multimediali Smooth Streaming e altri contenuti.

> **Important**
>
> Se specificate un server Web che esegue Microsoft IIS come origine, non attivate Smooth Streaming nei comportamenti di cache della CloudFront distribuzione. CloudFront non è possibile utilizzare un server Microsoft IIS come origine se si abilita Smooth Streaming come comportamento della cache.

Se attivi Smooth Streaming in un comportamento della cache (ovvero, non si dispone di un server che esegue Microsoft IIS), tieni presente quanto segue:

- Puoi ancora distribuire altro contenuto utilizzando lo stesso comportamento cache se il contenuto corrisponde al valore di Path Pattern (Modello di percorso) per quel comportamento cache.
- CloudFront può utilizzare un bucket Amazon S3 o un'origine personalizzata per i file multimediali Smooth Streaming. CloudFront non è possibile utilizzare un server Microsoft IIS come origine se si abilita Smooth Streaming per il comportamento della cache.
- Non puoi invalidare file multimediali in formato Smooth Streaming. Se vuoi aggiornare dei file prima della scadenza, devi rinominarli. Per ulteriori informazioni, consulta Aggiunta, rimozione o sostituzione di contenuti distribuiti da CloudFront.

Per informazioni sui client Smooth Streaming, consulta Smooth Streaming nella documentazione presente sul sito web di Microsoft.

Da utilizzare CloudFront per distribuire file Smooth Streaming quando un server Web Microsoft IIS non è l'origine

1. Transcodifica i tuoi file multimediali in formato frammentato MP4 Smooth Streaming.
2. Esegui una delle seguenti operazioni:
   - Se utilizzi la CloudFront console: quando crei o aggiorni una distribuzione, abilita Smooth Streaming in uno o più comportamenti della cache della distribuzione.
   - Se utilizzi l' CloudFront API: aggiungi l'`SmoothStreaming`elemento al tipo `DistributionConfig` complesso per uno o più comportamenti della cache della distribuzione.
3. Carica i file Smooth Streaming nella tua origine.
4. Crea un file `clientaccesspolicy.xml` o `crossdomainpolicy.xml` e aggiungilo a una posizione accessibile nella radice della distribuzione, ad esempio, `https://d111111abcdef8.cloudfront.net/clientaccesspolicy.xml`. Di seguito è riportato un esempio di policy:

   ```
   <?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>
   ```

   Per ulteriori informazioni, consulta Making a Service Available Across Domain Boundaries sul sito Web di Microsoft Developer Network.
5. Per i collegamenti nella tua applicazione (ad esempio a un lettore multimediale), specifica l'URL per il file multimediale nel formato seguente:

   `https://d111111abcdef8.cloudfront.net/video/presentation.ism/Manifest`

Offri lo streaming video con CloudFront e AWS Media Services

Per utilizzare AWS Media Services CloudFront per distribuire contenuti live a un pubblico globale, consulta le seguenti linee guida.

Utilizza AWS Elemental MediaLive per codificare i flussi video in tempo reale. Per codificare un flusso video di grandi dimensioni, MediaLive comprimilo in versioni più piccole (codifiche) che possono essere distribuite ai tuoi spettatori.

Dopo aver compresso un flusso video in diretta, puoi utilizzare una delle due opzioni principali seguenti per preparare e distribuire il contenuto:

- Conversione del contenuto nei formati richiesti e successiva distribuzione: se hai bisogno di contenuti in più formati, usa AWS Elemental MediaPackage per impacchettare il contenuto per diversi tipi di dispositivo. Quando impacchetti i contenuti, puoi anche implementare funzionalità aggiuntive e aggiungere DRM (Digital Rights Management) per impedire l'uso non autorizzato del contenuto. Per step-by-step istruzioni su come utilizzare per CloudFront fornire contenuti formattati, consulta. MediaPackage Distribuzione di video live formattati con AWS Elemental MediaPackage
- Archivia e servi i tuoi contenuti utilizzando un'origine scalabile: se i contenuti MediaLive sono codificati nei formati richiesti da tutti i dispositivi utilizzati dagli spettatori, utilizza un'origine altamente scalabile, ad esempio AWS Elemental MediaStore, per distribuire i contenuti. Per step-by-step istruzioni su come CloudFront servire contenuti archiviati in un MediaStore contenitore, consulta. Pubblica video utilizzandolo AWS Elemental MediaStore come origine

Dopo aver configurato il server di origine utilizzando una di queste opzioni, puoi distribuire video in streaming live ai visualizzatori tramite CloudFront.

> **Tip**
>
> Puoi scoprire una AWS soluzione che implementa automaticamente i servizi per creare un'esperienza di visualizzazione in tempo reale ad alta disponibilità. Per leggere la procedura relativa alla distribuzione automatica di questa soluzione, consulta Distribuzione automatica in streaming live.

Argomenti

- Distribuzione di video live formattati con AWS Elemental MediaPackage
- video-on-demandOffri contenuti con AWS Elemental MediaPackage

Pubblica video utilizzandolo AWS Elemental MediaStore come origine

Se hai un video archiviato in un AWS Elemental MediaStorecontenitore, puoi creare una CloudFront distribuzione per servire il contenuto.

Per iniziare, concedi CloudFront l'accesso al tuo MediaStore contenitore. Quindi crei una CloudFront distribuzione e la configuri per utilizzarla MediaStore.

Per fornire contenuti da un AWS Elemental MediaStore contenitore

1. Segui la procedura riportata in Consentire CloudFront ad Amazon di accedere al tuo AWS Elemental MediaStore container, quindi torna a questi passaggi per creare la tua distribuzione.
2. Creazione di una distribuzione con le impostazioni seguenti:

    a. Dominio di origine: l'endpoint di dati assegnato al tuo MediaStore contenitore. Dall'elenco a discesa, scegli il MediaStore contenitore per il tuo video in diretta.

    b. Percorso di origine: la struttura delle cartelle nel MediaStore contenitore in cui sono archiviati gli oggetti. Per ulteriori informazioni, consulta the section called “Percorso origine”.

    c. Aggiungi intestazioni personalizzate: aggiungi nomi e valori di intestazione se desideri CloudFront aggiungere intestazioni personalizzate quando inoltra le richieste all'origine.

    d. Policy del protocollo del visualizzatore: scegli Reindirizza a HTTPS. Per ulteriori informazioni, consulta the section called “Viewer Protocol Policy (Policy protocollo visualizzatore)”.

    e. Policy di cache e Policy di richiesta origine

    - Per Cache policy (Policy della cache), scegli Create policy (Crea policy) e quindi crea una policy della cache appropriata per le esigenze di caching e di durata dei segmenti. Dopo aver creato la policy, aggiorna l'elenco delle policy della cache e scegli la policy creata.
    - Per la politica di richiesta di Origin, scegli CORS- CustomOrigin dall'elenco a discesa.

    Per le altre impostazioni, è possibile impostare valori specifici in base ad altri requisiti tecnici o le esigenze del tuo business. Per un elenco di tutte le opzioni per le distribuzioni e informazioni sulla configurazione, consulta the section called “Tutte le impostazioni distribuzione”.

3. Per i link nella tua applicazione (ad esempio, un lettore multimediale), specifica il nome del file multimediale nello stesso formato che usi per gli altri oggetti che stai distribuendo. CloudFront

Distribuzione di video live formattati con AWS Elemental MediaPackage

Se hai formattato un live streaming utilizzando AWS Elemental MediaPackage, puoi creare una CloudFront distribuzione e configurare i comportamenti della cache per servire il live streaming. Il seguente processo presuppone che tu abbia già creato un canale e aggiunto gli endpoint per i video live utilizzando MediaPackage.

Per creare MediaPackage manualmente una CloudFront distribuzione per, segui questi passaggi:

Fase 1: Creare e configurare una CloudFront distribuzione

Completa la seguente procedura per configurare una CloudFront distribuzione per il canale video in diretta con cui hai creato MediaPackage.

Per creare una distribuzione Web per il canale video live

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli Create Distribution (Crea distribuzione).
3. Scegli le impostazioni per la distribuzione, comprese le seguenti:

   Dominio origine

   L'origine in cui si trovano il canale video MediaPackage in diretta e gli endpoint. Scegli il campo di testo, quindi dall'elenco a discesa scegli il dominio di MediaPackage origine per il tuo video live. Puoi mappare un dominio a vari endpoint di origine.

   Se hai creato il dominio di origine utilizzando un altro account AWS , digita il valore dell'URL di origine nel campo. L'origine deve essere un URL di tipo HTTPS.

   Ad esempio, per un endpoint HLS come `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, il dominio di origine è `3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com`.

   Per ulteriori informazioni, consulta the section called “Dominio origine”.

Origin Path (Percorso origine)

Il percorso verso l' MediaPackage endpoint da cui viene servito il contenuto.

Per ulteriori informazioni su come funziona un percorso di origine, consulta the section called “Percorso origine”.

> **Important**
>
> Il percorso con i caratteri jolly * è necessario per eseguire il routing in un punto qualsiasi della CloudFront distribuzione. Per evitare che le richieste che non corrispondono a un percorso esplicito vengano indirizzate all'origine reale, crea un'origine "fittizia" per quel percorso con caratteri jolly.

Example : creazione di un'origine "fittizia"

Nell'esempio seguente, gli endpoint `abc123` e `def456` indirizzano all'origine "reale", ma le richieste di contenuti video di qualsiasi altro endpoint vengono indirizzate a `mediapackage.us-west-2.amazonaws.com` senza il sottodominio appropriato, che si traduce in un errore HTTP `404`.

MediaPackage punti finali:

```
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 comportamento della 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
```

Per le altre impostazioni della distribuzione, è possibile impostare valori specifici in base ad altri requisiti tecnici o alle esigenze del tuo business. Per un elenco di tutte le opzioni per le distribuzioni e informazioni sulla configurazione, consulta the section called “Tutte le impostazioni distribuzione”.

Al termine della scelta delle altre impostazioni di distribuzione, scegli Create Distribution (Crea distribuzione).

4. Scegli la distribuzione appena creata, quindi scegli la scheda Behaviors (Comportamenti).
5. Seleziona il comportamento di default della cache da aggiornare, quindi scegli Edit (Modifica). Specifica le impostazioni corrette per il comportamento cache nel canale scelto come origine. Puoi aggiungere una o più origini in un secondo momento e modificare le relative impostazioni per il comportamento cache.
6. Vai alla pagina delle CloudFront distribuzioni.
7. Attendi che il valore della colonna Ultima modifica per la tua distribuzione passi da Deploying a una data e un'ora, a indicare che la distribuzione CloudFront è stata creata.

Passaggio 2: aggiungi Origins per i domini dei tuoi endpoint MediaPackage

Ripeti questi passaggi per aggiungere ogni endpoint del tuo MediaPackage canale alla tua distribuzione, tenendo presente la necessità di creare un'origine «fittizia».

Per aggiungere altri endpoint come origini

1. Sulla CloudFront console, scegli la distribuzione che hai creato per il tuo canale.
2. Sceglie Origins (Origini), quindi scegli Create origin (Crea origine).
3. Per il dominio Origin, nell'elenco a discesa, scegli un MediaPackage endpoint per il tuo canale.
4. Per le altre impostazioni, imposta i valori in base ad altri requisiti tecnici o alle esigenze del tuo business. Per ulteriori informazioni, consulta the section called “Origin Settings (Impostazioni di origine)”.
5. Scegli Create Origin (Crea origine).

Fase 3: configurazione dei comportamenti della cache per tutti gli endpoint

Per ogni endpoint, è necessario configurare comportamenti cache per aggiungere modelli di percorso che instradino le richieste correttamente. I modelli di percorso specificati dipendono dal formato video che fornisci. La procedura seguente include le informazioni sui pattern di percorso da utilizzare per i formati Apple HLS, CMAF, DASH e Microsoft Smooth Streaming.

In genere vengono impostati due comportamenti cache per ciascun endpoint:

- Il manifest padre, che è l'indice dei tuoi file.
- I segmenti, che sono i file dei contenuti video.

Per creare un comportamento cache per un endpoint

1. Sulla CloudFront console, scegli la distribuzione che hai creato per il tuo canale.
2. Scegli Behaviors (Comportamenti) quindi scegli Create Behavior (Crea comportamento).
3. Per Path pattern, usa un MediaPackage `OriginEndpoint` GUID specifico come prefisso di percorso.

   Modelli di percorso

   Per un endpoint HLS come `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, crea questi due comportamenti della cache:

   - Per i manifest padre e figlio, utilizza `/out/v1/abc123/*.m3u8`.
   - Per i segmenti di contenuto, utilizza `/out/v1/abc123/*.ts`.

   Per un endpoint CMAF come `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, crea questi due comportamenti della cache:

   - Per i manifest padre e figlio, utilizza `/out/v1/abc123/*.m3u8`.
   - Per i segmenti di contenuto, utilizza `/out/v1/abc123/*.mp4`.

   Per un endpoint DASH come `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.mpd`, crea questi due comportamenti della cache:

   - Per il manifest padre, utilizza `/out/v1/abc123/*.mpd`.

- Per i segmenti di contenuto, utilizza `/out/v1/abc123/*.mp4`.

Per gli endpoint Microsoft Smooth Streaming come `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.ism`, è previsto solo un manifesto, perciò va creato un solo comportamento della cache: `out/v1/abc123/index.ism/*`.

4. Specifica i valori per le impostazioni seguenti per ciascun comportamento cache:

Viewer Protocol Policy (Policy protocollo visualizzatore)

Scegli Redirect HTTP to HTTPS (Reindirizza HTTP a HTTPS).

Policy della cache e policy di richiesta origine

Per Cache policy (Policy cache), scegli Create policy (Crea policy). Per la nuova policy della cache, specificare le seguenti impostazioni:

Minimum TTL (TTL minimo)

Imposta su 5 secondi o meno, per evitare la distribuzione di contenuti obsoleti.

Stringhe di query

Per Query strings (Stringhe di query) (in Cache key settings (Impostazioni chiave cache)), scegli Include specified query strings (Includi stringhe di query specificate). Per Allow (Permetti), aggiungi i valori seguenti digitandoli e scegliendo Add item (Aggiungi elemento):

- Aggiungi `m` come parametro della stringa di query che desideri utilizzare come base CloudFront per la memorizzazione nella cache. La MediaPackage risposta include sempre il tag `?m=###` per registrare l'ora modificata dell'endpoint. Se il contenuto è già memorizzato nella cache con un valore diverso per questo tag, CloudFront richiede un nuovo manifesto invece di fornire la versione memorizzata nella cache.
- Se utilizzi la funzionalità di visualizzazione con spostamento temporale in MediaPackage, specifica `start` e `end` come parametri aggiuntivi della stringa di query sul comportamento della cache per le richieste manifeste (`*.m3u8`, `*.mpd` e). `index.ism/*` In questo modo, i contenuti vengono forniti nello specifico per il periodo di tempo indicato nella richiesta di manifest. Per ulteriori informazioni sulla visualizzazione in differita e sulla formattazione dei parametri di richiesta relativi a inizio e fine dei contenuti, consulta Visualizzazione in differita nella Guida per l'utente di AWS Elemental MediaPackage .

- Se utilizzi la funzionalità di filtro del manifesto in MediaPackage, specifica `aws.manifestfilter` come parametro aggiuntivo della stringa di query per la politica della cache che utilizzi con il comportamento della cache per le richieste manifeste (`*.m3u8`*`.mpd`, e). `index.ism/*` Ciò configura la distribuzione per inoltrare la stringa di `aws.manifestfilter` query all' MediaPackage origine, necessaria per il funzionamento della funzionalità di filtro del manifesto. Per ulteriori informazioni, consulta Filtraggio dei manifest nella Guida per l'utente di AWS Elemental MediaPackage .
- Se utilizzi HLS a bassa latenza (LL-HLS), specifica `_HLS_msn` e `_HLS_part` come parametri aggiuntivi della stringa di query per la policy della cache utilizzata con il comportamento della cache per le richieste manifesto (`*.m3u8`). Ciò configura la distribuzione per inoltrare `_HLS_msn` e `_HLS_part` interrogare le stringhe all'MediaPackage origine, il che è necessario per il funzionamento della funzione di blocco delle playlist LL-HLS.

5. Scegli Create (Crea).
6. Dopo aver creato la policy della cache, torna al flusso di lavoro di creazione del comportamento della cache. Aggiorna l'elenco delle policy della cache e scegli la policy appena creata.
7. Scegli Create behavior (Crea comportamento).
8. Se l'endpoint non è un endpoint Microsoft Smooth Streaming, ripeti questa procedura per creare un secondo comportamento della cache.

Fase 4: Abilita l'autorizzazione CDN basata sull'intestazione MediaPackage

Consigliamo di abilitare l'autorizzazione MediaPackage CDN basata sull'intestazione tra gli endpoint e la distribuzione. MediaPackage CloudFront Per ulteriori informazioni, consulta Abilita l'autorizzazione CDN nella MediaPackage Guida per l'utente.AWS Elemental MediaPackage

Passaggio 5: utilizzare CloudFront per servire il canale di live streaming

Dopo aver creato la distribuzione, aggiunto le origini, creato i comportamenti della cache e abilitato l'autorizzazione CDN basata sulle intestazioni, puoi servire il canale di live streaming utilizzando. CloudFront CloudFront indirizza le richieste dai visualizzatori agli MediaPackage endpoint corretti in base alle impostazioni configurate per i comportamenti della cache.

Per i link presenti nell'applicazione (ad esempio, un lettore multimediale), specificate l'URL del file multimediale nel formato standard di. CloudFront URLs Per ulteriori informazioni, consulta the section called “Personalizzazione degli URL dei file”.

video-on-demandOffri contenuti con AWS Elemental MediaPackage

Se crei i tuoi contenuti video-on-demand (VOD) da un' AWS Elemental MediaPackage origine, puoi creare una CloudFront distribuzione e configurare comportamenti ottimizzati della cache per offrire i contenuti VOD agli spettatori. Il processo seguente presuppone che abbiate già creato un gruppo di pacchetti con una configurazione di pacchetto e che abbiate importato una risorsa con. MediaPackage

Per creare MediaPackage manualmente una CloudFront distribuzione per, procedi nel seguente modo:

Fase 1: Creare e configurare una CloudFront distribuzione

Completate la seguente procedura per impostare una CloudFront distribuzione per il gruppo di pacchetti con cui avete creato MediaPackage.

Come creare una distribuzione per i contenuti VOD

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli Create Distribution (Crea distribuzione).
3. Scegli le impostazioni per la distribuzione, comprese le seguenti:

   Dominio origine

   L'origine del tuo gruppo di MediaPackage imballaggio. Digita il valore dell'URL di origine nel campo di testo. L'origine deve essere un URL di tipo HTTPS.

   Ad esempio, per un endpoint HLS come `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, il dominio di origine è `3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com`.

   Per ulteriori informazioni, consulta the section called “Dominio origine”.

   Origin Path (Percorso origine)

   Il percorso da cui viene servito il contenuto.

Per ulteriori informazioni su come funziona un percorso di origine, consulta the section called “Percorso origine”.

> **Important**
>
> Il percorso dei caratteri jolly `*` è necessario per eseguire il routing in un punto qualsiasi della CloudFront distribuzione. Per evitare che le richieste che non corrispondono a un percorso esplicito vengano indirizzate all'origine reale, crea un'origine "fittizia" per quel percorso con caratteri jolly.

Example : creazione di un'origine "fittizia"

Nell’esempio seguente, le configurazioni di packaging `def456` e `321xyz` instradano all’origine “reale”, ma le richieste per qualsiasi altro contenuto video vengono instradate a `mediapackage-vod.us-west-2.amazonaws.com` senza il sottodominio corretto, causando un errore HTTP `404`.

MediaPackage contenuto URLs per una singola risorsa per un gruppo di pacchetti con due configurazioni di imballaggio:

```
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/def456/ghi789/index.m3u8
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/321xyz/654uvw/index.m3u8
```

CloudFront Origine A:

```
Domain: 3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

CloudFront Origine B:

```
Domain: mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

CloudFront comportamento della cache:

```
1. Path: /out/v1/*/def456/* forward to Origin A
2. Path: /out/v1/*/321xyz/* forward to Origin A
3. Path: * forward to Origin B
```

Per le altre impostazioni della distribuzione, è possibile impostare valori specifici in base ad altri requisiti tecnici o alle esigenze del tuo business. Per un elenco di tutte le opzioni per le distribuzioni e informazioni sulla configurazione, consulta the section called “Tutte le impostazioni distribuzione”.

Al termine della scelta delle altre impostazioni di distribuzione, scegli Create Distribution (Crea distribuzione).

4. Scegli la distribuzione appena creata, quindi scegli la scheda Behaviors (Comportamenti).
5. Seleziona il comportamento di default della cache da aggiornare, quindi scegli Edit (Modifica). Specifica le impostazioni corrette relative al comportamento cache per la configurazione di pacchetti scelta per l’origine. Puoi aggiungere una o più origini in un secondo momento e modificare le relative impostazioni per il comportamento cache.
6. Vai alla pagina delle CloudFront distribuzioni.
7. Attendi che il valore della colonna Ultima modifica per la tua distribuzione passi da Deploying a una data e un'ora, a indicare che la distribuzione CloudFront è stata creata.

Passaggio 2: aggiungi Origins per i domini dei tuoi gruppi di pacchetti MediaPackage

Ripeti i passaggi seguenti per aggiungere ciascuno dei tuoi gruppi di MediaPackage imballaggi alla tua distribuzione, tenendo presente la necessità di creare un'origine «fittizia».

Come aggiungere altri gruppi di pacchetti come origini

1. Sulla CloudFront console, scegli la distribuzione che hai creato per il tuo canale.
2. Sceglie Origins (Origini), quindi scegli Create origin (Crea origine).
3. Per il dominio Origin, digita l'URL del gruppo di MediaPackage pacchetti.
4. Per le altre impostazioni, imposta i valori in base ad altri requisiti tecnici o alle esigenze del tuo business. Per ulteriori informazioni, consulta the section called “Origin Settings (Impostazioni di origine)”.
5. Scegli Create Origin (Crea origine).

Fase 3: configurazione dei comportamenti cache per tutte le configurazioni di creazioni di pacchetti

Per ogni configurazione di creazione di pacchetti, è necessario configurare comportamenti cache per aggiungere modelli di percorso che instradino le richieste correttamente. I modelli di percorso specificati dipendono dal formato video che fornisci. La procedura seguente include le informazioni sui pattern di percorso da utilizzare per i formati Apple HLS, CMAF, DASH e Microsoft Smooth Streaming.

In genere si impostano più comportamenti cache per ogni configurazione di creazione di pacchetti:

- Il manifest padre, che è l'indice dei tuoi file.
- I segmenti, che sono i file dei contenuti video. Un formato può utilizzare più di un'estensione per contenuti, a seconda della configurazione. È necessario un comportamento cache per ogni estensione.

Come creare un comportamento cache per una configurazione di creazione pacchetti

1. Sulla CloudFront console, scegli la distribuzione che hai creato per il tuo canale.
2. Scegli Behaviors (Comportamenti) quindi scegli Create Behavior (Crea comportamento).
3. Per Path pattern, utilizzate un GUID di configurazione MediaPackage del pacchetto VOD specifico come prefisso di percorso. Questo è il secondo GUID in un percorso VOD. MediaPackage

   Modelli di percorso

   Per contenuti HLS come `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, crea i comportamenti cache seguenti:

   - Per i manifest padre e figlio, utilizza `/out/v1/*/def456/*.m3u8`.
   - Per i segmenti dei contenuti, utilizza `/out/v1/*/def456/*.ts` e ripeti l'operazione per tutte le estensioni dei segmenti necessarie.

   Per contenuti CMAF come `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, crea i comportamenti cache seguenti:

   - Per i manifest padre e figlio, utilizza `/out/v1/*/def456/*.m3u8`.

- Per i segmenti dei contenuti, utilizza `/out/v1/*/def456/*.mp4` e ripeti l'operazione per tutte le estensioni dei segmenti necessarie.

Per contenuti DASH come `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.mpd`, crea i comportamenti cache seguenti:

- Per il manifest padre, utilizza `/out/v1/*/def456/*.mpd`.
- Per i segmenti di contenuto, utilizza `/out/v1/*/def456/*.mp4`.

Per gli endpoint Microsoft Smooth Streaming come `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.ism/Manifest`, è previsto solo un manifesto, perciò va creato un solo comportamento della cache: `out/v1/*/def456/*/index.ism/*`.

4. Specifica i valori per le impostazioni seguenti per ciascun comportamento cache:

Viewer Protocol Policy (Policy protocollo visualizzatore)

Scegli Redirect HTTP to HTTPS (Reindirizza HTTP a HTTPS).

Policy della cache e policy di richiesta origine

Per Cache policy (Policy cache), scegli Create policy (Crea policy). Per la nuova policy della cache, specificare le seguenti impostazioni:

Minimum TTL (TTL minimo)

Imposta su 5 secondi o meno, per evitare la distribuzione di contenuti obsoleti.

Stringhe di query

Per Query strings (Stringhe di query) (in Cache key settings (Impostazioni chiave cache)), scegli Include specified query strings (Includi stringhe di query specificate). Per Allow (Permetti), aggiungi i valori seguenti digitandoli e scegliendo Add item (Aggiungi elemento):

- Se utilizzate la funzionalità di filtro del manifesto in MediaPackage, specificate `aws.manifestfilter` come parametro aggiuntivo della stringa di query per la politica della cache da utilizzare con il comportamento della cache per le richieste manifeste (`*.m3u8*.mpd`, e). `index.ism/*` Ciò configura la distribuzione per inoltrare la stringa di `aws.manifestfilter` query all' MediaPackage origine,

necessaria per il funzionamento della funzionalità di filtro del manifesto. Per ulteriori informazioni, consulta Filtraggio dei manifest nella Guida per l'utente di AWS Elemental MediaPackage .

5. Scegli Create (Crea).
6. Dopo aver creato la policy della cache, torna al flusso di lavoro di creazione del comportamento della cache. Aggiorna l'elenco delle policy della cache e scegli la policy appena creata.
7. Scegli Create behavior (Crea comportamento).
8. Se l'endpoint non è un endpoint Microsoft Smooth Streaming, ripeti questa procedura per creare un secondo comportamento della cache.

Passaggio 4: abilitare l'autorizzazione CDN basata sull' MediaPackage intestazione

Consigliamo di abilitare l'autorizzazione MediaPackage CDN basata sull'intestazione tra MediaPackage il contenuto VOD e la distribuzione. CloudFront Per ulteriori informazioni, consulta Abilita l'autorizzazione CDN nella MediaPackage Guida per l'utente.AWS Elemental MediaPackage

Fase 5: Utilizzare CloudFront per servire il contenuto VOD

Dopo aver creato la distribuzione, aggiunto le origini, creato i comportamenti della cache e abilitato l'autorizzazione CDN basata sulle intestazioni, potete servire il contenuto VOD utilizzando. CloudFront CloudFront indirizza le richieste dei visualizzatori al contenuto MediaPackage VOD corretto in base alle impostazioni configurate per i comportamenti della cache.

Per i link presenti nell'applicazione (ad esempio, un lettore multimediale), specificate l'URL del file multimediale nel formato standard di. CloudFront URLs Per ulteriori informazioni, consulta the section called “Personalizzazione degli URL dei file”.

MQAR (Media Quality-Aware Resiliency)

La resilienza basata sulla qualità dei media (MQAR) è una funzionalità integrata tra Amazon CloudFront e Media Services.AWS MQAR fornisce una selezione automatica dell’origine tra le regioni basata sul Media Quality Confidence Score (MQCS). MQCS è sintetizzato da AWS Elemental MediaLive in base a parametri che influiscono sull’esperienza di qualità multimediale percepita da visualizzatori. Puoi configurare CloudFront AWS Media Services per offrire lo streaming di eventi dal vivo con elevata resilienza utilizzando diverse opzioni che puoi specificare nei criteri di failover del CloudFront gruppo di origine.

Quando abiliti la funzionalità MQAR per la tua distribuzione, autorizzi CloudFront a selezionare automaticamente l'origine che si ritiene abbia il punteggio di qualità più elevato.

Il punteggio di qualità rappresenta i problemi di qualità dello streaming multimediale percepiti dalle origini, come fotogrammi neri, fotogrammi congelati o persi o fotogrammi ripetuti. Ad esempio, se le tue origini AWS Elemental MediaPackage v2 vengono distribuite in due versioni diverse Regioni AWS e una riporta un punteggio di qualità multimediale superiore rispetto all'altra, CloudFront passerà automaticamente all'origine che riporta il punteggio più alto.

Per raggiungere questo obiettivo, CloudFront effettua le seguenti operazioni:

1. CloudFront inoltra una `GET` richiesta all' MediaPackage origine primaria e contemporaneamente avvia anche una `HEAD` richiesta all' MediaPackage origine secondaria. CloudFront riceve il punteggio di qualità multimediale nelle intestazioni di risposta da ciascuna origine.
2. Successivamente, CloudFront tiene traccia del punteggio per ciascuna origine e utilizza queste informazioni per determinare l'origine con il punteggio più alto quando arriva una nuova richiesta.

Il punteggio di qualità multimediale relativo alle tue origini può cambiare in tempo reale. CloudFront determina ciò utilizzando le modifiche MQCS e passa da un'origine all'altra per garantire che gli spettatori vedano contenuti di qualità multimediale superiore. Per ulteriori informazioni, consulta Sfruttamento dei punteggi di qualità multimediale MediaPackage nella Guida per l'utente della AWS Elemental MediaPackage versione 2.

MQAR aiuta a CloudFront determinare, il prima possibile, se esiste un problema che potrebbe avere un impatto potenziale sui clienti. Ad esempio, problemi quali connessione di rete, elaborazione video, perdita o interruzioni dell'audio, problemi di velocità dell'encoder possono influire sul punteggio di qualità multimediale per i visualizzatori.

MQAR offre un passaggio senza interruzioni da un'origine all'altra, in modo da poter implementare un flusso di lavoro di distribuzione end-to-end multimediale resiliente e interregionale e fornire contenuti di qualità AWS ai tuoi spettatori.

> **Note**
>
> Attualmente, questa funzionalità supporta solo le origini v2. MediaPackage

Per abilitare questa funzionalità per la distribuzione, completa le seguenti fasi:

1. Se non l'hai già fatto, crea le tue origini MediaPackage v2 e abilita questa funzionalità nella configurazione dell'endpoint. Per una distribuzione interregionale, crea un canale secondario in un altro canale Regione AWS con le stesse impostazioni. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS Elemental MediaPackage V2:
   - Creazione di un canale e di un endpoint
   - Abilitazione del punteggio di qualità multimediale
2. Per utilizzare le tue origini MediaPackage v2 per CloudFront, crea o aggiorna una CloudFront distribuzione. Consulta Creazione di una distribuzione e Aggiornamento di una distribuzione.
3. Crea un gruppo di origine e seleziona le due origini come principale e secondaria. Nel gruppo di origine, abilita l'opzione Punteggio di qualità multimediale. Per ulteriori informazioni, consulta Creazione di un gruppo di origine.
4. Nel comportamento cache per la distribuzione, seleziona il gruppo di origine creato. Si consiglia di impostare il comportamento cache in modo che corrisponda al modello del percorso del canale.

Se CloudFront determina che entrambe le origini MediaPackage v2 hanno lo stesso punteggio, inoltra la richiesta all'origine primaria elencata nel gruppo di origine. Se l'origine selezionata inizialmente risponde con un codice di errore corrispondente ai criteri di failover specificati nel gruppo di origine, CloudFront riprova la richiesta all'origine alternativa nel gruppo di origine indipendentemente dal punteggio di qualità multimediale.

> **Note**
>
> - CloudFront tiene traccia del punteggio di qualità per ogni comportamento della cache che utilizza un gruppo di origine abilitato per il punteggio di qualità multimediale. Se lo stesso gruppo di origini viene utilizzato per più canali che emettono un punteggio di qualità multimediale, crea un comportamento cache separato per il modello di percorso di ciascun canale per evitare di mescolare i punteggi. Per ulteriori informazioni sulle quote dei gruppi di origini, consulta Quote generali sulle distribuzioni.
> - Al momento, MQAR non è disponibile quando utilizzi una funzione Lambda@Edge nei trigger rivolti all'origine (richiesta origine e risposta origine) associati al comportamento cache della distribuzione. Per ulteriori informazioni, consulta Cache Behavior Settings (Impostazioni del comportamento della cache).
> - Se hai abilitato la funzionalità MQAR e il controllo di accesso origine (OAC), aggiungi l'azione `mediapackagev2:GetHeadObject` alla policy IAM. MQAR richiede questa autorizzazione per inviare `HEAD` richieste all'origine MediaPackage v2. Per ulteriori

informazioni su OAC, consulta Limita l'accesso a un'origine AWS Elemental MediaPackage v2.

Campi di log MQAR

CloudFront fornisce i seguenti campi nei registri di accesso in tempo reale per riflettere il punteggio di qualità e l'origine selezionata. È possibile abilitare questi campi nei registri dei registri di accesso CloudFront in tempo reale:

- `r-host`
- `sr-reason`
- `x-edge-mqcs`

Per ulteriori informazioni, consulta Campi 65-67.

Personalizzazione a livello di edge con le funzioni

Con Amazon CloudFront, puoi scrivere il tuo codice per personalizzare il modo in cui le tue CloudFront distribuzioni elaborano le richieste e le risposte HTTP. Il codice viene eseguito fisicamente vicino ai visualizzatori (utenti) in modo da ridurre al minimo la latenza e non è necessario gestire server o altra infrastruttura. Puoi scrivere codice per manipolare le richieste e le risposte che arrivano CloudFront, eseguire l'autenticazione e l'autorizzazione di base, generare risposte HTTP all'edge e altro ancora.

Il codice che scrivi e alleghi alla tua CloudFront distribuzione è chiamato funzione edge. CloudFront offre due modi per scrivere e gestire le funzioni edge:

CloudFront Funzioni

Puoi scrivere funzioni leggere JavaScript per personalizzazioni CDN su larga scala e sensibili alla latenza. L'ambiente di runtime CloudFront Functions offre tempi di avvio inferiori al millisecondo, è immediatamente scalabile per gestire milioni di richieste al secondo ed è estremamente sicuro. CloudFront Functions è una funzionalità nativa di CloudFront, il che significa che puoi creare, testare e distribuire il codice interamente all'interno. CloudFront

Lambda@Edge

Lambda@Edge è una estensione di AWS Lambda che fornisce elaborazione serverless potente e flessibile per funzioni complesse e una logica delle applicazioni completa più vicina ai visualizzatori. Le funzioni di Lambda@Edge vengono eseguite in un ambiente di runtime Node.js o Python. Li pubblichi su un singolo Regione AWS, ma quando associ la funzione a una CloudFront distribuzione, Lambda @Edge replica automaticamente il tuo codice in tutto il mondo.

Se esegui AWS WAF su CloudFront, puoi utilizzare le intestazioni AWS WAF inserite sia per CloudFront Functions che per Lambda @Edge. Questo funziona per le richieste e le risposte visualizzatore e origini.

Argomenti

- Differenze tra CloudFront Functions e Lambda @Edge
- Personalizza a 360° con CloudFront Functions
- Personalizza con le funzioni di CloudFront connessione
- Personalizzazione al livello di edge con Lambda@Edge

- Restrizioni sulle funzioni edge

Differenze tra CloudFront Functions e Lambda @Edge

CloudFront Functions e Lambda @Edge forniscono entrambi un modo per eseguire codice in risposta agli CloudFront eventi.

CloudFront Functions è ideale per funzioni leggere e di breve durata per i seguenti casi d'uso:

- Normalizzazione della chiave della cache: trasformare gli attributi delle richieste HTTP (intestazioni, stringhe di query, cookie, anche il percorso dell'URL) per creare una chiave della cache ottimale, che può migliorare la percentuale di riscontri nella cache.
- Manipolazione delle intestazioni: inserire, modificare o eliminare intestazioni HTTP nella richiesta o nella risposta. Ad esempio, è possibile aggiungere una intestazione `True-Client-IP` a ogni richiesta.
- Reindirizzamenti o riscritture di URL: reindirizzare i visualizzatori ad altre pagine in base alle informazioni nella richiesta o reindirizzare tutta la richiesta da un percorso a un altro.
- Richiesta di autorizzazione: puoi convalidare token di autorizzazione con hash, come token Web JSON (JWT), ispezionando le intestazioni dell'autorizzazione o altri metadati della richiesta.

Per iniziare a usare CloudFront Functions, consultaPersonalizza a 360° con CloudFront Functions.

Lambda@Edge è la soluzione ideale per i seguenti casi d'uso:

- Funzioni che richiedono diversi millisecondi o più per il completamento
- Funzioni che richiedono CPU o memoria regolabili
- Funzioni che dipendono da librerie di terze parti (incluso l' AWS SDK, per l'integrazione con altre Servizi AWS)
- Funzioni che richiedono l'accesso alla rete per utilizzare servizi esterni per l'elaborazione
- Funzioni che richiedono l'accesso al file system o l'accesso al corpo delle richieste HTTP

Per iniziare a utilizzare Lambda@Edge, consulta Personalizzazione al livello di edge con Lambda@Edge.

Per aiutarti a scegliere l'opzione per il tuo caso d'uso, usa la tabella seguente per comprendere le differenze tra CloudFront Functions e Lambda @Edge. Per informazioni sulle differenze che si

applicano ai metodi di assistente di gestione alla modifica dell'origine, consulta Scegli tra CloudFront Functions e Lambda @Edge.

	CloudFront Funzioni	Lambda@Edge
Linguaggi di programmazione	JavaScript (conforme alla ECMAScript versione 5.1)	Node.js e Python
Origini eventi	• Richiesta visualizzatore • Risposta visualizzatore	• Richiesta visualizzatore • Risposta visualizzatore • Richiesta origine • Risposta origine
Supporta Amazon CloudFront KeyValueStore	Sì CloudFront KeyValueStore supporta JavaScript solo il runtime 2.0	No
Dimensionare	Fino a milioni di richieste al secondo	Fino a 10.000 richieste al secondo per regione
Durata della funzione	Submillisecondo	Fino a 30 secondi (richiesta e risposta del visualizzatore) Fino a 30 secondi (richiesta origine e risposta origine)
Dimensione massima della memoria di funzione	2 MB	128 MB (richiesta e risposta del visualizzatore) 10.240 MB (10 GB) (richiesta origine e risposta origine)

	CloudFront Funzioni	Lambda@Edge
		Per ulteriori informazioni, consulta Quote di Lambda@Edge.
Dimensione massima del codice funzione e delle librerie incluse	10 KB	50 MB (richiesta e risposta del visualizzatore) 50 MB (richiesta origine e risposta origine)
Accesso alla rete	No	Sì
Accesso al file system	No	Sì
Accesso al corpo della richiesta	No	Sì
Accesso alla geolocalizzazione e ai dati del dispositivo	Sì	No (richiesta visualizzatore e risposta visualizzatore) Sì (richiesta origine e risposta origine)
Può creare e testare interamente all'interno CloudFront	Sì	No
Registrazione delle funzioni e parametri	Sì	Sì

Personalizza a 360° con CloudFront Functions

Con CloudFront Functions, puoi scrivere funzioni leggere JavaScript per personalizzazioni CDN su larga scala e sensibili alla latenza. Le tue funzioni possono manipolare le richieste e le risposte che arrivano CloudFront, eseguire l'autenticazione e l'autorizzazione di base, generare risposte HTTP all'edge e altro ancora. L'ambiente di runtime CloudFront Functions offre tempi di avvio inferiori al millisecondo, è immediatamente scalabile per gestire milioni di richieste al secondo ed è

estremamente sicuro. CloudFront Functions è una funzionalità nativa di CloudFront, il che significa che puoi creare, testare e distribuire il codice interamente all'interno. CloudFront

Quando associ una CloudFront funzione a una CloudFront distribuzione, CloudFront intercetta le richieste e le risposte nelle postazioni CloudFront periferiche e le trasmette alla tua funzione. È possibile richiamare CloudFront Functions quando si verificano i seguenti eventi:

- Quando CloudFront riceve una richiesta da un visualizzatore (richiesta del visualizzatore)
- Before CloudFront restituisce la risposta allo spettatore (risposta del visualizzatore)
- Durante la creazione della connessione TLS (richiesta di connessione), attualmente disponibile per le connessioni TLS (mTLS) reciproche

Per ulteriori informazioni sulle CloudFront funzioni, consulta i seguenti argomenti:

Argomenti

Tutorial: Creazione di una funzione semplice con Funzioni CloudFront

Questo tutorial illustra come iniziare a utilizzare Funzioni CloudFront. Puoi creare una semplice funzione che reindirizza il visualizzatore a un URL diverso e che restituisce anche un'intestazione di risposta personalizzata.

Indice

- Verifica della funzione

Prerequisiti

Per utilizzare CloudFront Functions, è necessaria una distribuzione CloudFront. Se non disponi di un account, consulta Inizia con una distribuzione CloudFront standard.

Creazione della funzione

Puoi utilizzare la console CloudFront per creare una funzione semplice che reindirizza il visualizzatore a un URL diverso e restituisce anche un'intestazione di risposta personalizzata.

Come creare una funzione CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Funzioni, quindi seleziona Crea funzione.
3. Nella pagina Crea funzione, per Nome, inserisci un nome di funzione come *MyFunctionName*.
4. (Facoltativo) In Descrizione, immetti una descrizione per la funzione, ad esempio **Simple test function**.
5. Per Runtime, mantieni la versione JavaScript selezionata predefinita.
6. Scegli Crea funzione.
7. Copia il codice funzione riportato di seguito. Questo codice funzione reindirizza il visualizzatore a un URL diverso e restituisce anche un'intestazione di risposta personalizzata.

```
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. Per Codice funzione, incolla il codice nell'editor di codice per sostituire il codice predefinito.
9. Scegli Save changes (Salva modifiche).
10. (Facoltativo) Puoi testare la funzione prima di pubblicarla. In questo tutorial non viene descritto come testare una funzione. Per ulteriori informazioni, consulta Test delle funzioni.
11. Scegli la scheda Pubblica, quindi seleziona funzione Pubblica. Devi pubblicare la funzione prima di poterla associare alla distribuzione CloudFront.
12. Quindi, puoi associare la funzione a una distribuzione e al comportamento cache. Nella pagina *MyFunctionName*, seleziona la scheda Pubblica.

    > **Warning**
    >
    > Nella procedura seguente, seleziona una distribuzione o un comportamento cache utilizzati per il test. Non associare questa funzione di test a una distribuzione o comportamento cache utilizzati in produzione.

13. Scegliere Add Association (Aggiungi associazione).
14. Nella finestra di dialogo Associa, seleziona una distribuzione e/o un comportamento cache. Per Tipo di evento, mantieni il valore predefinito.
15. Scegliere Add Association (Aggiungi associazione).

    La tabella Distribuzione associata mostra la distribuzione associata.
16. Attendere alcuni minuti affinché la distribuzione associata finisca la distribuzione. Per verificare lo stato della distribuzione, selezionala nella tabella Distribuzioni associate e scegli Visualizza distribuzione.

    Quando lo stato della distribuzione è Distribuito, sarà possibile verificare che la funzione funziona.

Verifica della funzione

Dopo aver distribuito la funzione, puoi verificare che funzioni correttamente per la distribuzione.

Come verificare la funzione

1. Nel browser web, vai al nome di dominio della distribuzione (ad esempio, `https://d111111abcdef8.cloudfront.net`).

La funzione restituisce un reindirizzamento al browser, quindi il browser passa automaticamente a `https://aws.amazon.com/cloudfront/`.

2. In una finestra della riga di comando, puoi utilizzare uno strumento come curl per inviare una richiesta al nome di dominio della distribuzione.

```
curl -v https://d111111abcdef8.cloudfront.net/
```

Nella risposta, vengono visualizzati la risposta di reindirizzamento (`302 Found`) e le intestazioni di risposta personalizzate aggiunte dalla funzione. L'aspetto della risposta potrebbe essere simile a quella del seguente esempio.

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==
```

Tutorial: creazione di una funzione CloudFront che includa valori delle chiavi

Questo tutorial mostra come includere valori delle chiavi con la funzione CloudFront. I valori delle chiavi fanno parte di una coppia chiave-valore. Il nome (della coppia chiave-valore) viene incluso nel codice della funzione. Quando la funzione viene eseguita, CloudFront sostituisce il nome con il valore.

Le coppie chiave-valore sono variabili memorizzate in un archivio di valori delle chiavi. Se vi utilizzi una chiave (anziché valori a codifica fissa), la funzione è più flessibile. Puoi modificare il valore della chiave senza dover implementare modifiche al codice. Le coppie chiave-valore possono anche ridurre le dimensioni della funzione. Per ulteriori informazioni, consulta ???.

Indice

Prerequisiti

Se non hai familiarità con le Funzioni CloudFront e l'archivio di valori delle chiavi, ti consigliamo di seguire il tutorial in the section called "Tutorial: Creazione di una funzione CloudFront semplice".

Dopo aver completato il tutorial, puoi seguirlo per estendere la funzione che hai creato. Per questo tutorial, ti consigliamo di creare prima l'archivio di valori delle chiavi.

Creazione dell'archivio di valori delle chiavi

Innanzitutto, crea l'archivio di valori delle chiavi da utilizzare per la funzione.

Come creare l'archivio di valori delle chiavi

1. Pianifica le coppie chiave-valore da includere nella funzione. Annota i nomi delle chiavi. Le coppie chiave-valore da utilizzare in una funzione devono trovarsi in un unico archivio di valori delle chiavi.
2. Decidi l'ordine di lavoro. Puoi procedere in due modi:
   - Crea un archivio di valori delle chiavi e aggiungi coppie chiave-valore. Quindi puoi creare (o modificare) la funzione e incorporare i nomi delle chiavi.
   - In alternativa, puoi creare (o modificare) la funzione e incorporare i nomi delle chiavi da utilizzare. Quindi, crea un archivio di valori delle chiavi e aggiungi le coppie chiave-valore.
3. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.

4. Nel riquadro di navigazione, scegli Funzioni, quindi seleziona la scheda KeyValueStores.
5. Scegli Crea KeyValueStore e completa i campi seguenti:
   - Immetti un nome e una descrizione (facoltativa) per l'archivio.
   - Lascia vuoto il campo URI S3. In questo tutorial le coppie chiave-valore verranno inserite manualmente.
6. Seleziona Create (Crea). Viene visualizzata la pagina dei dettagli relativa al nuovo archivio di valori delle chiavi. Questa pagina include una sezione Coppie chiave-valore che al momento è vuota.

Aggiunta di coppie chiave-valore all'archivio di valori delle chiavi

Successivamente, aggiungi manualmente un elenco di coppie chiave-valore all'archivio di valori delle chiavi creato in precedenza.

Come aggiungere coppie chiave-valore all'archivio di valori delle chiavi

1. Nella sezione Coppie chiave-valore, scegli Aggiungi coppie chiave-valore.
2. Scegli Aggiungi coppia e quindi inserisci una chiave e un valore. Seleziona il segno di spunta per confermare le modifiche e ripeti questa fase per aggiungerne altre.
3. Al termine, scegli Salva modifiche per salvare le coppie chiave-valore nell'archivio di valori delle chiavi. Nel finestra di dialogo di conferma, seleziona Fatto.

Ora hai un archivio di valori delle chiavi che contiene un gruppo di coppie chiave-valore.

Associazione dell'archivio di valori delle chiavi alla funzione

Ora hai creato l'archivio di valori delle chiavi. Hai inoltre creato o modificato una funzione che include i nomi delle chiavi dall'archivio di valori delle chiavi. Ora puoi associare l'archivio di valori delle chiavi e la funzione. È possibile creare tale associazione dall'interno della funzione.

Come associare l'archivio di valori delle chiavi alla funzione

1. Nel riquadro di navigazione, seleziona Funzioni. Per impostazione predefinita, la scheda Funzioni viene visualizzata in alto.
2. Scegli il nome della funzione e nella sezione KeyValueStore associato, scegli Associa KeyValueStore esistente.

3. Seleziona l'archivio di valori delle chiavi e scegli Associa KeyValueStore.

> **Note**
>
> Puoi associare un solo archivio di valori delle chiavi a ciascuna funzione.

Test e pubblicazione del codice della funzione

Dopo aver associato l'archivio dei valori delle chiavi alla funzione, puoi testare e pubblicare il codice della funzione. È sempre consigliabile testare il codice della funzione a ogni modifica, anche per le seguenti operazioni:

- Associazione dell'archivio di valori delle chiavi alla funzione
- Modifica la funzione e il rispettivo archivio di valori delle chiavi per includere una nuova coppia chiave-valore.
- Modifica il valore di una coppia chiave-valore.

Come eseguire il test e pubblicare il codice della funzione

1. Per ulteriori informazioni su come testare una funzione, consulta the section called "Test delle funzioni". Verifica di aver scelto di testare la funzione nella fase `DEVELOPMENT`.
2. Pubblica la funzione quando hai tutto pronto per utilizzarla (con le coppie chiave-valore nuove o modificate) in un ambiente `LIVE`.

   Quando esegui la pubblicazione, CloudFront copia la versione della funzione dalla fase `DEVELOPMENT` alla fase live. La funzione ha il nuovo codice ed è associata all'archivio di valori delle chiavi. Non è necessario ripetere l'associazione nella fase live.

   Per ulteriori informazioni su come pubblicare una funzione, consulta the section called "Pubblicazione di funzioni".

Scrittura del codice della funzione

Puoi usare CloudFront Functions per scrivere funzioni leggere JavaScript per personalizzazioni CDN su larga scala e sensibili alla latenza. Il codice funzionale può manipolare le richieste e le risposte che

fluiscono CloudFront, eseguire l'autenticazione e l'autorizzazione di base, generare risposte HTTP all'edge e altro ancora.

Per aiutarti a scrivere il codice funzionale per CloudFront Functions, consulta i seguenti argomenti. Per esempi di codice, consulta CloudFront Esempi di funzioni per CloudFront e il amazon-cloudfront-functions repository on GitHub.

Argomenti

- Scelta dello scopo della funzione
- CloudFront Funzioni, struttura degli eventi
- Funzionalità di runtime JavaScript per CloudFront Functions
- Metodi helper per archivi di valori delle chiavi
- Metodi di assistente di gestione per la modifica dell'origine
- Metodi di supporto per le proprietà di CloudFront SaaS Manager
- Uso di async e await
- Supporto CWT per le funzioni CloudFront
- Metodi generali di supporto

Scelta dello scopo della funzione

Prima di scrivere il codice funzione, è necessario determinare lo scopo della funzione. La maggior parte CloudFront delle funzioni di Functions ha uno dei seguenti scopi.

Argomenti

- Modifica della richiesta HTTP in un tipo di evento di richiesta visualizzatore
- Generazione di una risposta HTTP in un tipo di evento di richiesta visualizzatore
- Modifica della risposta HTTP in un tipo di evento di risposta visualizzatore
- Convalida le connessioni MTL in un tipo di evento di richiesta di connessione
- Informazioni correlate

Indipendentemente dallo scopo della funzione, `handler` è il punto di ingresso per qualsiasi funzione. Richiede un solo argomento chiamato`event`, che viene passato alla funzione da CloudFront. `event` è un oggetto JSON che contiene una rappresentazione della richiesta HTTP (e la risposta, se la funzione modifica la risposta HTTP).

Modifica della richiesta HTTP in un tipo di evento di richiesta visualizzatore

La funzione può modificare la richiesta HTTP CloudFront ricevuta dal visualizzatore (client) e restituire la richiesta modificata a CloudFront per continuare l'elaborazione. Ad esempio, il codice funzione potrebbe normalizzare la chiave cache o modificare le intestazioni delle richieste.

Dopo aver creato e pubblicato una funzione che modifica la richiesta HTTP, assicurati di aggiungere un'associazione per il tipo di evento richiesta visualizzatore. Per ulteriori informazioni, consulta Creazione della funzione. In questo modo la funzione viene eseguita ogni volta che CloudFront riceve una richiesta da un visualizzatore, prima di verificare se l'oggetto richiesto è nella CloudFront cache.

Example Esempio

Il seguente pseudocodice mostra la struttura di una funzione che modifica la richiesta HTTP.

```
function handler(event) {
    var request = event.request;

    // Modify the request object here.

    return request;
}
```

La funzione restituisce l'`request`oggetto modificato a CloudFront. CloudFrontcontinua a elaborare la richiesta restituita controllando la CloudFront presenza di un hit nella cache e inviando la richiesta all'origine, se necessario.

Generazione di una risposta HTTP in un tipo di evento di richiesta visualizzatore

La funzione può generare una risposta HTTP all'edge e restituirla direttamente al visualizzatore (client) senza verificare la presenza di una risposta memorizzata nella cache o ulteriori elaborazioni da parte CloudFront di. Ad esempio, il codice funzione potrebbe reindirizzare la richiesta a un nuovo URL oppure verificare l'autorizzazione e restituire una risposta `401` o `403` a richieste non autorizzate.

Quando crei una funzione che genera una risposta HTTP, assicurati di scegliere il tipo di evento richiesta del visualizzatore. Ciò significa che la funzione viene eseguita ogni volta che CloudFront riceve una richiesta da un visualizzatore, prima CloudFront di eseguire qualsiasi ulteriore elaborazione della richiesta.

Example Esempio

Il seguente pseudocodice mostra la struttura di una funzione che genera una risposta HTTP.

```
function handler(event) {
    var request = event.request;

    var response = ...; // Create the response object here,
                        // using the request properties if needed.

    return response;
}
```

La funzione restituisce un `response` oggetto a CloudFront, che ritorna CloudFront immediatamente al visualizzatore senza controllare la CloudFront cache o inviare una richiesta all'origine.

Modifica della risposta HTTP in un tipo di evento di risposta visualizzatore

La funzione può modificare la risposta HTTP prima di CloudFront inviarla al visualizzatore (client), indipendentemente dal fatto che la risposta provenga dalla CloudFront cache o dall'origine. Ad esempio, il codice funzione potrebbe aggiungere o modificare le intestazioni, i codici di stato e i contenuti del corpo della risposta.

Quando crei una funzione che modifica la risposta HTTP, assicurati di scegliere il tipo di evento risposta del visualizzatore . Ciò significa che la funzione viene eseguita prima di CloudFront restituire una risposta al visualizzatore, indipendentemente dal fatto che la risposta provenga dalla CloudFront cache o dall'origine.

Example Esempio

Il seguente pseudocodice mostra la struttura di una funzione che modifica la risposta 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 funzione restituisce l'`response`oggetto modificato a CloudFront, che ritorna CloudFront immediatamente al visualizzatore.

Convalida le connessioni MTL in un tipo di evento di richiesta di connessione

Le funzioni di connessione sono un tipo di CloudFront funzioni che vengono eseguite durante le connessioni TLS per fornire una logica di convalida e autenticazione personalizzata. Le funzioni di connessione sono attualmente disponibili per le connessioni TLS reciproche (MTLS), in cui è possibile convalidare i certificati client e implementare una logica di autenticazione personalizzata oltre alla convalida dei certificati standard. Le funzioni di connessione vengono eseguite durante il processo di handshake TLS e possono consentire o negare le connessioni in base alle proprietà del certificato, agli indirizzi IP dei client o ad altri criteri.

Dopo aver creato e pubblicato una funzione di connessione, assicuratevi di aggiungere un'associazione per il tipo di evento di richiesta di connessione con una distribuzione abilitata per MTLS. In questo modo la funzione viene eseguita ogni volta che un client tenta di stabilire una connessione MTLS con. CloudFront

Example

Il seguente pseudocodice mostra la struttura di una funzione di connessione:

```
function connectionHandler(connection) {
    // Validate certificate and connection properties here.

    if (/* validation passes */) {
        connection.allow();
    } else {
        connection.deny();
    }
}
```

La funzione utilizza metodi di supporto per determinare se consentire o negare la connessione. A differenza delle funzioni di richiesta e risposta del visualizzatore, le funzioni di connessione non possono modificare le richieste o le risposte HTTP.

Informazioni correlate

Per ulteriori informazioni sull'utilizzo CloudFront delle funzioni, consultate i seguenti argomenti:

- Struttura degli eventi
- Funzionalità di runtime JavaScript
- CloudFront Esempi di funzioni

- Restrizioni sulle funzioni edge

CloudFront Funzioni, struttura degli eventi

CloudFront Functions passa un `event` oggetto al codice della funzione come input quando esegue la funzione. Quando si testa una funzione, si crea l'oggetto `event` e lo si passa alla funzione. Quando si crea un oggetto `event` per testare una funzione, puoi omettere i campi `distributionDomainName`, `distributionId` e `requestId` nell'oggetto `context`. Assicuratevi che i nomi delle intestazioni siano in minuscolo, come accade sempre nell'`event`oggetto che CloudFront Functions passa alla funzione in produzione.

Di seguito viene illustrata una panoramica della struttura di questo oggetto evento.

```
{
    "version": "1.0",
    "context": {
        <context object>
    },
    "viewer": {
        <viewer object>
    },
    "request": {
        <request object>
    },
    "response": {
        <response object>
    }
}
```

Per ulteriori informazioni, consulta i seguenti argomenti:

Argomenti

- Campo Versione
- Oggetto Context
- Struttura degli eventi di connessione
- Oggetto Viewer
- Oggetto Request
- Oggetto Response

- Codice di stato e corpo
- Struttura di una stringa di query, un'intestazione o cookie
- Oggetto risposta di esempio
- Oggetto evento di esempio

Campo Versione

Il `version` campo contiene una stringa che specifica la versione dell'oggetto evento Functions. CloudFront La versione corrente è `1.0`.

Oggetto Context

L'oggetto `context` contiene informazioni contestuali sull'evento. Include i seguenti campi:

`distributionDomainName`

Il nome di CloudFront dominio (ad esempio, d111111abcdef8.cloudfront.net) della distribuzione standard associata all'evento.

Il campo `distributionDomainName` viene visualizzato solo quando la funzione viene invocata per le distribuzioni standard.

`endpoint`

Il nome di CloudFront dominio (ad esempio, d111111abcdef8.cloudfront.net) del gruppo di connessione associato all'evento.

Il campo `endpoint` viene visualizzato solo quando la funzione viene invocata per le distribuzioni multi-tenant.

`distributionId`

L'ID della distribuzione (ad esempio, EXAMPLE) associata all'evento. EDFDVBD6

`eventType`

Il tipo di evento, `viewer-request` o `viewer-response`.

`requestId`

Una stringa che identifica in modo univoco una CloudFront richiesta (e la risposta associata).

Struttura degli eventi di connessione

Le funzioni di connessione ricevono una struttura degli eventi diversa rispetto alle funzioni di visualizzazione. Per informazioni dettagliate sulla struttura degli eventi di connessione e sul formato di risposta, vedereAssociare una funzione di CloudFront connessione.

Oggetto Viewer

L'oggetto `viewer` contiene un campo `ip` il cui valore è l'indirizzo IP del visualizzatore (client) che ha inviato la richiesta. Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico per inviare la richiesta, il valore è l'indirizzo IP del proxy o del sistema di bilanciamento del carico.

Oggetto Request

L'`request`oggetto contiene una rappresentazione di una richiesta viewer-to-CloudFront HTTP. Nell'`event`oggetto passato alla funzione, l'`request`oggetto rappresenta la richiesta effettiva CloudFront ricevuta dal visualizzatore.

Se il codice della funzione restituisce un `request` oggetto a CloudFront, deve utilizzare la stessa struttura.

L'oggetto `request` include i seguenti campi:

`method`

Metodo HTTP nella richiesta. Se il codice funzione restituisce `request`, non può modificare questo campo. Questo è l'unico campo di sola lettura nell'oggetto `request`.

`uri`

Il percorso relativo dell'oggetto richiesto.

> **Note**
>
> Se la funzione Lambda modifica il valore `uri`, si applica quanto segue:
>
> - Il nuovo valore `uri` deve iniziare con una barra (`/`).
> - Se una funzione modifica il valore di `uri`, l'oggetto richiesto dal visualizzatore viene modificato.
> - Se una funzione modifica il valore di `uri`, il comportamento della cache per la richiesta o l'origine a cui la richiesta viene inoltrata non viene modificato.

querystring

Un oggetto che rappresenta la stringa di query nella richiesta. Se la richiesta non include una stringa di query, l'oggetto `request` include comunque un oggetto `querystring` vuoto.

L'oggetto `querystring` contiene un campo per ogni parametro della stringa di query nella richiesta.

headers

Un oggetto che rappresenta le intestazioni HTTP nella richiesta. Se la richiesta contiene intestazioni `Cookie`, queste non faranno parte dell'oggetto `headers`. I cookie sono rappresentati separatamente nell'oggetto `cookies`.

L'oggetto `headers` contiene un campo per ogni intestazione della richiesta. I nomi delle intestazioni vengono convertiti in caratteri minuscoli ASCII nell'oggetto evento e i nomi delle intestazioni devono essere caratteri minuscoli ASCII quando vengono aggiunti dal codice della funzione. Quando CloudFront Functions riconverte l'oggetto evento in una richiesta HTTP, la prima lettera di ogni parola nei nomi delle intestazioni è in maiuscolo, se si tratta di una lettera ASCII. CloudFront Functions non applica alcuna modifica ai simboli non ASCII nei nomi delle intestazioni. Ad esempio, `TÈst-header` diventerà `tÈst-header` all'interno della funzione. Il simbolo non ASCII `È` rimane invariato.

Le parole sono separate da un trattino (`-`). Ad esempio, se il codice della funzione aggiunge un'intestazione denominata`example-header-name`, la CloudFront converte in nella richiesta HTTP. `Example-Header-Name`

cookies

Un oggetto che rappresenta i cookie nella richiesta (intestazioni `Cookie`).

L'oggetto `cookies` contiene un campo per ogni cookie nella richiesta.

Per ulteriori informazioni sulla struttura delle stringhe di query, delle intestazioni e dei cookie, consulta Struttura di una stringa di query, un'intestazione o cookie.

Per un oggetto `event` di esempio, consulta Oggetto evento di esempio.

Oggetto Response

L'`response`oggetto contiene una rappresentazione di una risposta CloudFront-to-viewer HTTP. Nell'`event`oggetto passato alla funzione, l'`response`oggetto rappresenta la risposta effettiva CloudFront di un utente a una richiesta del visualizzatore.

Se il codice funzione restituisce un oggetto `response`, deve utilizzare la stessa struttura.

L'oggetto `response` include i seguenti campi:

`statusCode`

Il codice di stato HTTP per la risposta. Questo valore è un numero intero, non una stringa.

La funzione può generare o modificare il `statusCode`.

`statusDescription`

Descrizione dello stato HTTP della risposta. Se il codice funzione genera una risposta, questo campo è facoltativo.

`headers`

Un oggetto che rappresenta le intestazioni HTTP nella risposta. Se la risposta contiene intestazioni `Set-Cookie`, queste non faranno parte dell'oggetto `headers`. I cookie sono rappresentati separatamente nell'oggetto `cookies`.

L'oggetto `headers` contiene un campo per ogni intestazione della risposta. I nomi delle intestazioni vengono convertiti in minuscolo nell'oggetto evento e i nomi delle intestazioni devono essere in minuscolo quando vengono aggiunti dal codice della funzione. Quando CloudFront Functions riconverte l'oggetto evento in una risposta HTTP, la prima lettera di ogni parola nei nomi delle intestazioni viene scritta in maiuscolo. Le parole sono separate da un trattino (`-`). Ad esempio, se il codice della funzione aggiunge un'intestazione denominata`example-header-name`, la CloudFront converte in nella risposta HTTP. `Example-Header-Name`

`cookies`

Un oggetto che rappresenta i cookie nella risposta (intestazioni `Set-Cookie`).

L'oggetto `cookies` contiene un campo per ogni cookie nella risposta.

`body`

L'aggiunta del campo `body` è facoltativa e non sarà presente nell'oggetto`response` a meno che non venga specificato nella funzione. La funzione non ha accesso al corpo originale restituito dalla

CloudFront cache o dall'origine. Se non specificate il `body` campo nella funzione di risposta del visualizzatore, il corpo originale restituito dalla CloudFront cache o dall'origine viene restituito al visualizzatore.

Se desideri CloudFront restituire un corpo personalizzato al visualizzatore, specifica il contenuto del corpo nel `data` campo e la codifica del corpo nel `encoding` campo. Puoi specificare la codifica come testo normale (`"encoding": "text"`) o come contenuto con codifica Base64 (`"encoding": "base64"`).

Come scelta rapida, puoi anche specificare il contenuto del corpo direttamente nel campo `body` (`"body": "<specify the body content here>"`). Quando esegui questa operazione, ometti i campi `data` e`encoding`. CloudFront in questo caso tratta il corpo come testo semplice.

`encoding`

La codifica del contenuto `body` (campo `data`). Le uniche codifiche valide sono `text` e `base64`.

Se si specifica `encoding` come `base64` ma il corpo non è valido base64, CloudFront restituisce un errore.

`data`

Il contenuto `body`.

Per ulteriori informazioni sui codici di stato modificati e sul contenuto del corpo, consultare Codice di stato e corpo.

Per ulteriori informazioni sulla struttura delle intestazioni e dei cookie, consulta Struttura di una stringa di query, un'intestazione o cookie.

Per un oggetto `response` di esempio, consulta Oggetto risposta di esempio.

Codice di stato e corpo

Con CloudFront Functions, puoi aggiornare il codice di stato della risposta del visualizzatore, sostituire l'intero corpo della risposta con uno nuovo o rimuovere il corpo della risposta. Alcuni scenari comuni per l'aggiornamento della risposta del visualizzatore dopo aver valutato alcuni aspetti della risposta dalla CloudFront cache o dall'origine includono quanto segue:

- Modifica dello stato per impostare un codice di stato HTTP 200 e creazione di contenuto di corpo statico da restituire al visualizzatore.

- Modifica dello stato per impostare un codice di stato HTTP 301 o 302 per reindirizzare l'utente a un altro sito Web.
- Decidere se fornire o eliminare il corpo della risposta visualizzatore.

> **Note**
>
> Se l'origine restituisce un errore HTTP pari o superiore a 400, la CloudFront funzione non verrà eseguita. Per ulteriori informazioni, consulta Restrizioni su tutte le funzioni edge.

Quando lavori con la risposta HTTP, CloudFront Functions non ha accesso al corpo della risposta. Puoi sostituire un contenuto del corpo impostandolo sul valore desiderato oppure puoi rimuovere il corpo impostando il valore in modo da essere vuoto. Se non aggiorni il campo body della tua funzione, il corpo originale restituito dalla CloudFront cache o dall'origine viene restituito al visualizzatore.

> **Tip**
>
> Quando usi CloudFront Functions per sostituire un corpo, assicurati di allineare le intestazioni corrispondenti, ad esempio`content-encoding`, or `content-type``content-length`, al nuovo contenuto del corpo.
> Ad esempio, se l' CloudFront origine o la cache restituiscono `content-encoding: gzip` ma la funzione di risposta del visualizzatore imposta un corpo in testo semplice, la funzione deve anche modificare le `content-type` intestazioni `content-encoding` e di conseguenza.

Se la CloudFront funzione è configurata per restituire un errore HTTP pari o superiore a 400, il visualizzatore non visualizzerà una pagina di errore personalizzata specificata per lo stesso codice di stato.

Struttura di una stringa di query, un'intestazione o cookie

Le stringhe di query, le intestazioni e i cookie condividono la stessa struttura. Le stringhe di query possono apparire nelle richieste. Le intestazioni vengono visualizzate nelle richieste e nelle risposte. I cookie vengono visualizzati nelle richieste e nelle risposte.

Ogni stringa di query, intestazione o cookie è un campo univoco all'interno dell'oggetto padre `querystring`, `headers` o `cookies`. Il nome del campo è il nome della stringa di query, dell'intestazione o del cookie. Ogni campo contiene una proprietà `value` con il valore della stringa di query, dell'intestazione o del cookie.

Indice

Valori stringa di query od oggetti stringa di query

Oltre a un oggetto, una funzione può restituire un valore stringa di query. È possibile utilizzare il valore stringa di query per disporre i parametri della stringa di query in qualsiasi ordine personalizzato.

Example Esempio

Per modificare una stringa di query nel codice funzione, utilizza un codice come il seguente.

```
var request = event.request;
request.querystring =
 'ID=42&Exp=1619740800&TTL=1440&NoValue=&querymv=val1&querymv=val2,val3';
```

Considerazioni speciali per le intestazioni

Solo per le intestazioni, i nomi delle intestazioni vengono convertiti in minuscolo nell'oggetto evento e i nomi delle intestazioni devono essere in minuscolo quando vengono aggiunti dal codice della funzione. Quando CloudFront Functions riconverte l'oggetto evento in una richiesta o risposta HTTP, la prima lettera di ogni parola nei nomi delle intestazioni viene scritta in maiuscolo. Le parole sono separate da un trattino (`-`). Ad esempio, se il codice della funzione aggiunge un'intestazione denominata`example-header-name`, la CloudFront converte nella richiesta o `Example-Header-Name` nella risposta HTTP.

Example Esempio

Considera la seguente intestazione `Host` in una richiesta HTTP:

```
Host: video.example.com
```

Questa intestazione è rappresentata come segue nell'oggetto `request`:

```
"headers": {
    "host": {
        "value": "video.example.com"
    }
}
```

Per accedere all'intestazione `Host` nel codice funzione, utilizza un codice come il seguente:

```
var request = event.request;
var host = request.headers.host.value;
```

Per aggiungere o modificare un'intestazione nel codice funzione, utilizza un codice come il seguente (questo codice aggiunge un'intestazione denominata `X-Custom-Header` con il valore `example value`):

```
var request = event.request;
request.headers['x-custom-header'] = {value: 'example value'};
```

Stringhe di query, intestazioni e cookie duplicati (array **`multiValue`**)

Una richiesta o una risposta HTTP può contenere più di una stringa di query, intestazione o cookie con lo stesso nome. In questo caso, le stringhe di query, le intestazioni o i cookie duplicati vengono compressi in un campo nell'oggetto `request` o `response`, ma questo campo conterrà una proprietà aggiuntiva denominata `multiValue`. La proprietà `multiValue` contiene un array con i valori di ciascuna delle stringhe di query, intestazioni o cookie duplicati.

Example Esempio

Considera una richiesta HTTP con le intestazioni `Accept` seguenti:

```
Accept: application/json
Accept: application/xml
Accept: text/html
```

Queste intestazioni sono rappresentate come segue nell'oggetto `request`.

```
"headers": {
    "accept": {
        "value": "application/json",
        "multiValue": [
            {
                "value": "application/json"
            },
            {
                "value": "application/xml"
            },
            {
                "value": "text/html"
            }
        ]
    }
}
```

> **Note**
>
> Il valore della prima intestazione (in questo caso, `application/json`) viene ripetuto in entrambe le proprietà `value` e `multiValue`. Ciò consente di accedere a tutti i valori di passare attraverso l'array `multiValue`.

Se il codice della funzione modifica una stringa di query, un'intestazione o un cookie con un `multiValue` array, CloudFront Functions utilizza le seguenti regole per applicare le modifiche:

1. Se l'array `multiValue` esiste e ha una qualsiasi modifica, allora tale modifica viene applicata. Il primo elemento della proprietà `value` viene ignorato.
2. In caso contrario, viene applicata qualsiasi modifica alla proprietà `value` e i valori successivi (se presenti) rimangono invariati.

La proprietà `multiValue` viene utilizzata solo quando la richiesta HTTP o la risposta contiene stringhe di query duplicate, intestazioni o cookie con lo stesso nome, come illustrato nell'esempio precedente. Tuttavia, se sono presenti più valori in una singola stringa di query, intestazione o cookie, la proprietà `multiValue` non viene utilizzata.

Example Esempio

Considera una richiesta con un'intestazione `Accept` che contiene tre valori.

```
Accept: application/json, application/xml, text/html
```

Questa intestazione è rappresentata come segue nell'oggetto `request`.

```
"headers": {
    "accept": {
        "value": "application/json, application/xml, text/html"
    }
}
```

Attributi cookie

In una intestazione `Set-Cookie` in una risposta HTTP, l'intestazione contiene la coppia nome-valore per il cookie e facoltativamente un insieme di attributi separati da punto e virgola.

Example Esempio

```
Set-Cookie: cookie1=val1; Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT
```

Nell'oggetto `response`, questi attributi sono rappresentati nella proprietà `attributes` del campo cookie. Ad esempio, l'intestazione `Set-Cookie` precedente è rappresentata come segue:

```
"cookie1": {
    "value": "val1",
    "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
}
```

Oggetto risposta di esempio

L'esempio seguente mostra un oggetto `response`, l'output di una funzione di risposta del visualizzatore, in cui il corpo è stato sostituito da una funzione di risposta del visualizzatore.

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

Oggetto evento di esempio

Di seguito viene illustrato un esempio di oggetto `event` completo. Questo è un esempio di invocazione per una distribuzione standard, non per una distribuzione multi-tenant. Per le distribuzioni multi-tenant, il `endpoint` campo viene utilizzato al posto di The value of è `distributionDomainName` il nome di `endpoint` CloudFront dominio (ad esempio, d111111abcdef8.cloudfront.net) del gruppo di connessione associato all'evento.

> **Note**
>
> L'oggetto `event` è l'input per la tua funzione. La funzione restituisce solo l'oggetto `request` o `response`, non l'oggetto `event` completo.

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

Funzionalità di runtime JavaScript per CloudFront Functions

L'ambiente runtime JavaScript di CloudFront Functions è compatibile con ECMAScript (ES) versione 5.1 e supporta anche alcune funzionalità di ES versioni da 6 a 12.

Per le funzionalità più aggiornate, ti consigliamo di utilizzare il runtime JavaScript 2.0.

Le funzionalità del runtime JavaScript 2.0 presentano le seguenti modifiche rispetto alla versione 1.0:

- Sono disponibili metodi del modulo Buffer
- Non sono disponibili i seguenti metodi di prototipo per stringhe non standard:
  - `String.prototype.bytesFrom()`
  - `String.prototype.fromBytes()`
  - `String.prototype.fromUTF8()`
  - `String.prototype.toBytes()`
  - `String.prototype.toUTF8()`
- Il modulo crittografico presenta le seguenti modifiche:
  - `hash.digest()`: il tipo di restituzione viene modificato in `Buffer` se non viene fornita alcuna codifica
  - `hmac.digest()`: il tipo di restituzione viene modificato in `Buffer` se non viene fornita alcuna codifica
- Per ulteriori informazioni sulle nuove funzionalità aggiuntive, consulta Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront.

Argomenti

Funzionalità di runtime JavaScript 1.0 per Funzioni CloudFront

L'ambiente runtime JavaScript di CloudFront Functions è compatibile con ECMAScript (ES) versione 5.1 e supporta anche alcune funzionalità di ES versioni da 6 a 9. Fornisce anche alcuni metodi non standard che non fanno parte delle specifiche ES.

Negli argomenti seguenti sono elencate tutte le funzionalità linguistiche supportate.

Argomenti

Caratteristiche principali

Sono supportate le seguenti caratteristiche principali di ES.

Tipi

Sono supportati tutti i tipi ES 5.1. Tra questi vi sono valori booleani, numeri, stringhe, oggetti, matrici, funzioni, costruttori di funzioni ed espressioni regolari.

Operatori

Sono supportati tutti gli operatori ES 5.1.

È supportato l'operatore esponenziale ES 7 (`**`).

Dichiarazioni

> **Note**
>
> Le istruzioni `const` e `let` non sono supportate.

Sono supportate le seguenti istruzioni ES 5.1:

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`

- `for`
- `for-in`
- `if`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`
- Istruzioni etichettate

Valori letterali

Sono supportati i valori letterali modello ES 6: stringhe multilinea, interpolazione di espressioni e modelli di nidificazione.

Funzioni

Sono supportate tutte le funzioni ES 5.1.

Sono supportate le funzioni freccia ES 6 ed è supportata la sintassi del parametro rest ES 6.

Unicode

Il testo di origine e i valori letterali stringa possono contenere caratteri codificati in Unicode. Sono supportate anche sequenze di escape dei punti di codice Unicode di sei caratteri (ad esempio, `\uXXXX`).

Modalità rigorosa

Le funzioni funzionano in modalità rigorosa per impostazione predefinita, quindi non è necessario aggiungere una istruzione `use strict` nel codice funzione. Non possono essere modificate.

Oggetti primitivi

Sono supportati i seguenti oggetti primitivi di ES.

Oggetto

Sono supportati i seguenti metodi ES 5.1 sugli oggetti:

- `create` (senza elenco delle proprietà)

- defineProperties
- defineProperty
- freeze
- getOwnPropertyDescriptor
- getOwnPropertyNames
- getPrototypeOf
- hasOwnProperty
- isExtensible
- isFrozen
- prototype.isPrototypeOf
- isSealed
- keys
- preventExtensions
- prototype.propertyIsEnumerable
- seal
- prototype.toString
- prototype.valueOf

Sono supportati i seguenti metodi ES 6 sugli oggetti:

- assign
- is
- prototype.setPrototypeOf

Sono supportati i seguenti metodi ES 8 sugli oggetti:

- entries
- values

Stringa

Sono supportati i seguenti metodi ES 5.1 sulle stringhe:

- 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`

Sono supportati i seguenti metodi ES 6 sulle stringhe:

- `fromCodePoint`
- `prototype.codePointAt`
- `prototype.endsWith`
- `prototype.includes`
- `prototype.repeat`
- `prototype.startsWith`

Sono supportati i seguenti metodi ES 8 sulle stringhe:

- `prototype.padStart`
- `prototype.padEnd`

Sono supportati i seguenti metodi ES 9 sulle stringhe:

- `prototype.trimStart`
- `prototype.trimEnd`

Sono supportati i seguenti metodi non standard sulle stringhe:

- `prototype.bytesFrom(`*`array | string, encoding`*`)`

  Crea una stringa di byte da un array di ottetti o da una stringa codificata. Le opzioni di codifica delle stringhe sono `hex`, `base64` e `base64url`.

- `prototype.fromBytes(start[, end])`

  Crea una stringa Unicode da una stringa di byte in cui ogni byte viene sostituito con il corrispondente punto di codice Unicode.
- `prototype.fromUTF8(start[, end])`

  Crea una stringa Unicode da una stringa di byte codificata UTF-8. Se la codifica non è corretta, viene restituito `null`.
- `prototype.toBytes(start[, end])`

  Crea una stringa di byte da una stringa Unicode. Tutti i caratteri devono essere compresi nell'intervallo [0,255]. In caso contrario, restituisce `null`.
- `prototype.toUTF8(start[, end])`

  Crea una stringa di byte codificata UTF-8 da una stringa Unicode.

Numero

Sono supportati tutti i metodi ES 5.1 sui numeri.

Sono supportati i seguenti metodi ES 6 sui numeri:

- `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`

Oggetti incorporati

Sono supportati i seguenti oggetti incorporati di ES.

Math

Sono supportati tutti i metodi matematici ES 5.1.

> **Note**
>
> Nell'ambiente runtime CloudFront Functions, l'implementazione `Math.random()` utilizza OpenBSD `arc4random` predefinito con il timestamp di quando viene eseguita la funzione.

Sono supportati i seguenti metodi matematici ES 6:

- `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`

Data

Sono supportate tutte le funzioni `Date` ES 5.1.

> **Note**
>
> Per motivi di sicurezza, restituisce `Date` sempre lo stesso valore, ovvero l'ora di inizio della funzione, durante la durata di una singola esecuzione di una funzione. Per ulteriori informazioni, consulta Funzionalità con restrizioni.

Funzione

Sono supportati i metodi `apply`, `bind` e `call`.

I costruttori di funzioni non sono supportati.

Espressioni regolari

Sono supportate tutte le funzioni di espressione regolare ES 5.1. Il linguaggio delle espressioni regolari è compatibile con Perl. Sono supportati i gruppi di acquisizione denominati di ES 9.

JSON

Sono supportate tutte le funzionalità JSON di ES 5.1, incluso `parse` e `stringify`.

Array

Sono supportati i seguenti metodi ES 5.1 sugli array:

- `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`

Sono supportati i seguenti metodi ES 6 sugli array:

- `of`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.find`
- `prototype.findIndex`

Sono supportati i seguenti metodi ES 7 sugli array:

- `prototype.includes`

Array tipizzati

Sono supportati i seguenti array tipizzati ES 6:

- `Int8Array`

- `Uint8Array`
- `Uint8ClampedArray`
- `Int16Array`
- `Uint16Array`
- `Int32Array`
- `Uint32Array`
- `Float32Array`
- `Float64Array`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.join`
- `prototype.set`
- `prototype.slice`
- `prototype.subarray`
- `prototype.toString`

ArrayBuffer

Sono supportati i seguenti metodi su `ArrayBuffer`:

- `prototype.isView`
- `prototype.slice`

Promessa

Sono supportati i seguenti metodi sulle promesse:

- `reject`
- `resolve`
- `prototype.catch`
- `prototype.finally`
- `prototype.then`

Crittografia

Il modulo di crittografia fornisce helper standard hash e HMAC (Hash Message Authentication Code). È possibile caricare il modulo usando `require('crypto')`. Il modulo espone i seguenti metodi che si comportano esattamente come le loro controparti Node.js:

- `createHash(algorithm)`
- `hash.update(data)`
- `hash.digest([encoding])`
- `createHmac(algorithm, secret key)`
- `hmac.update(data)`
- `hmac.digest([encoding])`

Per ulteriori informazioni, consulta Crittografia (hash e HMAC) nella sezione dei moduli incorporati.

Console

Questo è un oggetto helper per il debug. Supporta solo il metodo `log()` per registrare i messaggi di log.

> **Note**
>
> Funzioni CloudFront non supporta la sintassi delle virgole, ad esempio `console.log('a', 'b')`. Utilizzare invece il formato `console.log('a' + ' ' + 'b')`.

Tipi di errore

Sono supportati i seguenti oggetti di errore:

- `Error`
- `EvalError`
- `InternalError`
- `MemoryError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Elementi globali

L'oggetto `globalThis` è supportato.

Sono supportate le seguenti funzioni globali ES 5.1:

- `decodeURI`
- `decodeURIComponent`
- `encodeURI`
- `encodeURIComponent`
- `isFinite`
- `isNaN`
- `parseFloat`
- `parseInt`

Sono supportate le seguenti costanti globali:

- `NaN`
- `Infinity`
- `undefined`

Moduli incorporati

Sono supportati i seguenti moduli incorporati:

Modules

- Crittografia (hash e HMAC)
- Stringa di query

Crittografia (hash e HMAC)

Il modulo di crittografia (`crypto`) fornisce helper di hashing standard e HMAC (Hash Message Authentication Code). È possibile caricare il modulo usando `require('crypto')`. Il modulo fornisce i seguenti metodi che si comportano esattamente come le controparti Node.js.

Metodi di hashing

`crypto.createHash(algorithm)`

Crea e restituisce un oggetto hash che è possibile utilizzare per generare digest hash utilizzando il dato algoritmo: `md5`, `sha1`, o `sha256`.

`hash.update(data)`

Aggiorna il contenuto hash con il dato `data`.

`hash.digest([encoding])`

Calcola il digest di tutti i dati passati tramite `hash.update()`. La codifica può essere `hex`, `base64` o `base64url`.

Metodi HMAC

`crypto.createHmac(algorithm, secret key)`

Crea e restituisce un oggetto HMAC che utilizza il dato `algorithm` e `secret key`. L'algoritmo può essere `md5`, `sha1` o `sha256`.

`hmac.update(data)`

Aggiorna il contenuto HMAC con il dato `data`.

`hmac.digest([encoding])`

Calcola il digest di tutti i dati passati tramite `hmac.update()`. La codifica può essere `hex`, `base64` o `base64url`.

Stringa di query

> **Note**
>
> L'oggetto evento di CloudFront Functions analizza automaticamente le stringhe di query URL per tuo conto. Ciò significa che nella maggior parte dei casi non è necessario utilizzare questo modulo.

Il modulo stringa di query (`querystring`) fornisce metodi per l'analisi e la formattazione delle stringhe di query URL. È possibile caricare il modulo usando `require('querystring')`. Il modulo fornisce i metodi seguenti:

`querystring.escape(string)`

URL che codifica il dato `string`, restituendo una stringa di query con escape. Il metodo viene utilizzato da `querystring.stringify()` e non deve essere utilizzato direttamente.

`querystring.parse(string[, separator[, equal[, options]]])`

Analizza una stringa di query (`string`) e restituisce un oggetto.

Il parametro `separator` è una sottostringa per delimitare coppie chiave e valore nella stringa di query. Per impostazione predefinita, tale valore è &.

Il parametro `equal` è una sottostringa per la delimitazione di chiavi e valori nella stringa di query. Per impostazione predefinita, tale valore è =.

Il parametro `options` è un oggetto con le seguenti chiavi:

`decodeURIComponent function`

Un funzione per decodificare i caratteri codificati in percentuale nella stringa di query. Per impostazione predefinita, tale valore è `querystring.unescape()`.

`maxKeys number`

Il numero massimo di chiavi da analizzare. Per impostazione predefinita, tale valore è `1000`. Utilizza un valore `0` per rimuovere le limitazioni per il conteggio delle chiavi.

Per impostazione predefinita, si presuppone che i caratteri con codifica in percentuale all'interno della stringa di query utilizzino la codifica UTF-8. Le sequenze UTF-8 non valide vengono sostituite con il carattere sostitutivo `U+FFFD`.

Ad esempio, per la seguente stringa di query:

```
'name=value&abc=xyz&abc=123'
```

Il valore restituito di `querystring.parse()` è:

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` è un alias per `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Serializza un `object` e restituisce una stringa di query.

Il parametro `separator` è una sottostringa per delimitare coppie chiave e valore nella stringa di query. Per impostazione predefinita, tale valore è &.

Il parametro `equal` è una sottostringa per la delimitazione di chiavi e valori nella stringa di query. Per impostazione predefinita, tale valore è =.

Il parametro `options` è un oggetto con le seguenti chiavi:

`encodeURIComponent` *`function`*

La funzione da utilizzare per convertire caratteri non sicuri dell'URL in codifica percentuale nella stringa di query. Per impostazione predefinita, tale valore è `querystring.escape()`.

Per impostazione predefinita, i caratteri che richiedono la codifica percentuale all'interno della stringa di query sono codificati come UTF-8. Per utilizzare una codifica diversa, specifica l'opzione `encodeURIComponent`.

Ad esempio, per il seguente codice:

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

Il valore restituito è:

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` è un alias per `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Decodifica i caratteri codificati in percentuale URL nel dato `string`, restituendo una stringa di query senza escape. Questo metodo viene utilizzato da `querystring.parse()` e non deve essere utilizzato direttamente.

Funzionalità con restrizioni

Le seguenti funzionalità del linguaggio JavaScript non sono supportate o sono limitate a causa di problemi di sicurezza.

Valutazione dinamica del codice

La valutazione dinamica del codice non è supportata. Entrambi i costruttori `eval()` e `Function` generano un errore se tentato. Ad esempio, `const sum = new Function('a', 'b', 'return a + b')` genera un errore.

Timer

Le funzioni `setTimeout()`, `setImmediate()` e `clearTimeout()` non sono supportate. Non vi è alcuna disposizione per differire o cedere all'interno di un'esecuzione di funzione. La funzione deve essere eseguita in modo sincrono fino al completamento.

Data e timestamp

Per motivi di sicurezza, non è possibile accedere ai timer ad alta risoluzione. Tutti i metodi `Date` per interrogare l'ora corrente restituiscono sempre lo stesso valore durante la durata di una singola esecuzione di funzione. Il timestamp restituito è il momento in cui la funzione ha iniziato l'esecuzione. Di conseguenza, non è possibile misurare il tempo trascorso nella vostra funzione.

Accesso al file system

Nessun accesso al file system. Ad esempio, non esiste un modulo `fs` per l'accesso al file system come invece è presente in Node.js.

Accesso al processo

Non è possibile accedere al processo. Ad esempio, non esiste un oggetto globale `process` per l’elaborazione dell’accesso alle informazioni come in Node.js.

Variabili di ambiente

Non è possibile accedere alle variabili d’ambiente.

È invece possibile utilizzare KeyValueStore di CloudFront per creare un datastore centralizzato di coppie chiave-valore per le Funzioni CloudFront. KeyValueStore di CloudFront consente aggiornamenti dinamici dei dati di configurazione senza dover implementare modifiche al codice. Passare a JavaScript runtime 2.0 per utilizzare KeyValueStore di CloudFront. Per ulteriori informazioni, consulta Amazon CloudFront KeyValueStore.

Accesso alla rete

Non è disponibile alcun supporto per le chiamate di rete. Ad esempio, XHR, HTTP(S) e socket non sono supportati.

Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront

L'ambiente runtime JavaScript di CloudFront Functions è compatibile con ECMAScript (ES) versione 5.1 e supporta anche alcune funzionalità di ES versioni da 6 a 12. Fornisce anche alcuni metodi non standard che non fanno parte delle specifiche ES. Negli argomenti seguenti sono elencate tutte le funzionalità supportate in questo runtime.

Argomenti

Caratteristiche principali

Sono supportate le seguenti caratteristiche principali di ES.

Tipi

Sono supportati tutti i tipi ES 5.1. Tra questi vi sono valori booleani, numeri, stringhe, oggetti, matrici, funzioni ed espressioni regolari.

Operatori

Sono supportati tutti gli operatori ES 5.1.

È supportato l'operatore esponenziale ES 7 (`**`).

Dichiarazioni

Sono supportate le seguenti istruzioni ES 5.1:

- `break`
- `catch`
- `continue`
- `do-while`

- `else`
- `finally`
- `for`
- `for-in`
- `if`
- `label`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`

Sono supportate le seguenti istruzioni ES 6:

- `const`
- `let`

Sono supportate le seguenti istruzioni ES 8:

- `async`
- `await`

> **Note**
>
> `async`, `await`, `const` e `let` sono supportati nel runtime JavaScript 2.0.
> `await` può essere utilizzato solo all'interno delle funzioni `async`. Argomenti e chiusure `async` non sono supportati.

Valori letterali

Sono supportati i valori letterali modello ES 6: stringhe multilinea, interpolazione di espressioni e modelli di nidificazione.

Funzioni

Sono supportate tutte le funzioni ES 5.1.

Sono supportate le funzioni freccia ES 6 ed è supportata la sintassi del parametro rest ES 6.

Unicode

Il testo di origine e i valori letterali stringa possono contenere caratteri codificati in Unicode. Sono supportate anche sequenze di escape dei punti di codice Unicode di sei caratteri (ad esempio, `\uXXXX`).

Modalità rigorosa

Le funzioni funzionano in modalità rigorosa per impostazione predefinita, quindi non è necessario aggiungere una istruzione `use strict` nel codice funzione. Non possono essere modificate.

Oggetti primitivi

Sono supportati i seguenti oggetti primitivi di ES.

Oggetto

Sono supportati i seguenti metodi ES 5.1 sugli oggetti:

- `Object.create()` (senza elenco delle proprietà)
- `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()`

Sono supportati i seguenti metodi ES 6 sugli oggetti:

- `Object.assign()`

Sono supportati i seguenti metodi ES 8 sugli oggetti:

- `Object.entries()`
- `Object.values()`

Sono supportati i seguenti metodi di prototipo ES 5.1 sugli oggetti:

- `Object.prototype.hasOwnProperty()`
- `Object.prototype.isPrototypeOf()`
- `Object.prototype.propertyIsEnumerable()`
- `Object.prototype.toString()`
- `Object.prototype.valueOf()`

Sono supportati i seguenti metodi di prototipo ES 6 sugli oggetti:

- `Object.prototype.is()`
- `Object.prototype.setPrototypeOf()`

Stringa

Sono supportati i seguenti metodi ES 5.1 sulle stringhe:

- `String.fromCharCode()`

Sono supportati i seguenti metodi ES 6 sulle stringhe:

- `String.fromCodePoint()`

Sono supportati i seguenti metodi di prototipo ES 5.1 sulle stringhe:

- `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()`

Sono supportati i seguenti metodi di prototipo ES 6 sulle stringhe:

- `String.prototype.codePointAt()`
- `String.prototype.endsWith()`
- `String.prototype.includes()`
- `String.prototype.repeat()`
- `String.prototype.startsWith()`

Sono supportati i seguenti metodi di prototipo ES 8 sulle stringhe:

- `String.prototype.padStart()`
- `String.prototype.padEnd()`

Sono supportati i seguenti metodi di prototipo ES 9 sulle stringhe:

- `String.prototype.trimStart()`
- `String.prototype.trimEnd()`

Sono supportati i seguenti metodi di prototipo ES 12 sulle stringhe:

- `String.prototype.replaceAll()`

> **Note**
>
> `String.prototype.replaceAll()` rappresenta una novità nel runtime JavaScript 2.0.

Numero

Sono supportati TUTTI i numeri ES 5.

Sono supportate le seguenti proprietà ES 6 sui numeri:

- `Number.EPSILON`
- `Number.MAX_SAFE_INTEGER`
- `Number.MIN_SAFE_INTEGER`
- `Number.MAX_VALUE`

- `Number.MIN_VALUE`
- `Number.NaN`
- `Number.NEGATIVE_INFINITY`
- `Number.POSITIVE_INFINITY`

Sono supportati i seguenti metodi ES 6 sui numeri:

- `Number.isFinite()`
- `Number.isInteger()`
- `Number.isNaN()`
- `Number.isSafeInteger()`
- `Number.parseInt()`
- `Number.parseFloat()`

Sono supportati i seguenti metodi di prototipo ES 5.1 sui numeri:

- `Number.prototype.toExponential()`
- `Number.prototype.toFixed()`
- `Number.prototype.toPrecision()`

Sono supportati i separatori numerici ES 12.

> **Note**
>
> I separatori numerici ES 12 rappresentano una novità nel runtime JavaScript 2.0.

Oggetti incorporati

Sono supportati i seguenti oggetti incorporati di ES.

Math

Sono supportati tutti i metodi matematici ES 5.1.

> **Note**
>
> Nell'ambiente runtime CloudFront Functions, l'implementazione `Math.random()` utilizza OpenBSD `arc4random` predefinito con il timestamp di quando viene eseguita la funzione.

Sono supportate le seguenti proprietà matematiche ES 6:

- `Math.E`
- `Math.LN10`
- `Math.LN2`
- `Math.LOG10E`
- `Math.LOG2E`
- `Math.PI`
- `Math.SQRT1_2`
- `Math.SQRT2`

Sono supportati i seguenti metodi matematici ES 6:

- `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()`

Data

Sono supportate tutte le funzioni `Date` ES 5.1.

> **Note**
>
> Per motivi di sicurezza, restituisce `Date` sempre lo stesso valore, ovvero l'ora di inizio della funzione, durante la durata di una singola esecuzione di una funzione. Per ulteriori informazioni, consulta Funzionalità con restrizioni.

Funzione

Sono supportati i seguenti metodi di prototipo ES 5.1:

- `Function.prototype.apply()`
- `Function.prototype.bind()`
- `Function.prototype.call()`

I costruttori di funzioni non sono supportati.

Espressioni regolari

Sono supportate tutte le funzioni di espressione regolare ES 5.1. Il linguaggio delle espressioni regolari è compatibile con Perl.

Sono supportate le seguenti proprietà di accessor per prototipo ES 5.1:

- `RegExp.prototype.global`
- `RegExp.prototype.ignoreCase`
- `RegExp.protoype.multiline`
- `RegExp.protoype.source`
- `RegExp.prototype.sticky`
- `RegExp.prototype.flags`

> **Note**
>
> `RegExp.prototype.sticky` e `RegExp.prototype.flags` rappresentano delle novità nel runtime JavaScript 2.0.

Sono supportati i seguenti metodi di prototipo ES 5.1:

- `RegExp.prototype.exec()`
- `RegExp.prototype.test()`
- `RegExp.prototype.toString()`
- `RegExp.prototype[@@replace]()`
- `RegExp.prototype[@@split]()`

> **Note**
>
> `RegExp.prototype[@@split]()` rappresenta una novità nel runtime JavaScript 2.0.

Sono supportate le seguenti proprietà di istanza ES 5.1:

- `lastIndex`

Sono supportati i gruppi di acquisizione denominati di ES 9.

JSON

Sono supportati i seguenti metodi ES 5.1:

- `JSON.parse()`
- `JSON.stringify()`

Array

Sono supportati i seguenti metodi ES 5.1 sugli array:

- `Array.isArray()`

Sono supportati i seguenti metodi ES 6 sugli array:

- `Array.of()`

Sono supportati i seguenti metodi di prototipo ES 5.1:

- `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()`

Sono supportati i seguenti metodi di prototipo ES 6:

- `Array.prototype.copyWithin()`
- `Array.prototype.fill()`
- `Array.prototype.find()`
- `Array.prototype.findIndex()`

Sono supportati i seguenti metodi di prototipo ES 7:

- `Array.prototype.includes()`

Array tipizzati

Sono supportati i seguenti costruttori di array tipizzati ES 6:

- `Float32Array`
- `Float64Array`
- `Int8Array`
- `Int16Array`
- `Int32Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Uint16Array`
- `Uint32Array`

Sono supportati i seguenti metodi ES 6:

- `TypedArray.from()`
- `TypedArray.of()`

> **Note**
>
> `TypedArray.from()` e `TypedArray.of()` rappresentano delle novità nel runtime JavaScript 2.0.

Sono supportati i seguenti metodi di prototipo ES 6:

- `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.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()` e `TypedArray.prototype.some()` rappresentano delle novità nel runtime JavaScript 2.0.

ArrayBuffer

Sono supportati i seguenti metodi ES 6 su ArrayBuffer:

- `isView()`

Sono supportati i seguenti metodi di prototipo ES 6 su ArrayBuffer:

- `ArrayBuffer.prototype.slice()`

Promessa

Sono supportati i seguenti metodi ES 6 sulle promesse:

- `Promise.all()`
- `Promise.allSettled()`
- `Promise.any()`
- `Promise.reject()`
- `Promise.resolve()`
- `Promise.race()`

> **Note**
>
> `Promise.all()`, `Promise.allSettled()`, `Promise.any()` e `Promise.race()` rappresentano delle novità nel runtime JavaScript 2.0.

Sono supportati i seguenti metodi di prototipo ES 6 sulle promesse:

- `Promise.prototype.catch()`
- `Promise.prototype.finally()`
- `Promise.prototype.then()`

DataView

Sono supportati i seguenti metodi di prototipo ES 6:

- `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**
>
> Tutti i metodi di prototipo DataView ES 6 rappresentano delle novità nel runtime JavaScript 2.0.

Symbol

Sono supportati i seguenti metodi ES 6:

- `Symbol.for()`
- `Symbol.keyfor()`

> **Note**
>
> Tutti i metodi Symbol ES 6 rappresentano delle novità nel runtime JavaScript 2.0.

TextDecoder

Sono supportati i seguenti metodi di prototipo:

- `TextDecoder.prototype.decode()`

Sono supportate le seguenti proprietà di accessor per prototipo:

- `TextDecoder.prototype.encoding`
- `TextDecoder.prototype.fatal`
- `TextDecoder.prototype.ignoreBOM`

TextEncoder

Sono supportati i seguenti metodi di prototipo:

- `TextEncoder.prototype.encode()`
- `TextEncoder.prototype.encodeInto()`

Tipi di errore

Sono supportati i seguenti oggetti di errore:

- `Error`
- `EvalError`
- `InternalError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Elementi globali

L'oggetto `globalThis` è supportato.

Sono supportate le seguenti funzioni globali ES 5.1:

- `decodeURI()`
- `decodeURIComponent()`
- `encodeURI()`
- `encodeURIComponent()`
- `isFinite()`
- `isNaN()`
- `parseFloat()`
- `parseInt()`

Sono supportate le seguenti funzioni globali ES 6:

- `atob()`
- `btoa()`

> **Note**
>
> `atob()` e `btoa()` rappresentano delle novità nel runtime JavaScript 2.0.

Sono supportate le seguenti costanti globali:

- `NaN`
- `Infinity`
- `undefined`
- `arguments`

Moduli incorporati

Sono supportati i seguenti moduli incorporati:

Modules

- Buffer
- Stringa di query
- Crittografia

Buffer

Il modulo fornisce i metodi seguenti:

- `Buffer.alloc(size[, fill[, encoding]])`

  Alloca un `Buffer`.

  - `size`: dimensione del buffer. Immetti un numero intero.
  - `fill`: facoltativo. Immetti una stringa, `Buffer`, Uint8Array o un numero intero. Il valore predefinito è “”. `0`.
  - `encoding`: facoltativo. Quando `fill` è una stringa, immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.

- `Buffer.allocUnsafe(size)`

  Alloca un `Buffer` non inizializzato.

  - `size`: immetti un numero intero.
- `Buffer.byteLength(value[, encoding])`

  Restituisce la lunghezza di un valore, in byte.

  - `value`: una stringa, `Buffer`, TypedArray, Dataview o Arraybuffer.
  - `encoding`: facoltativo. Quando `value` è una stringa, immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.
- `Buffer.compare(buffer1, buffer2)`

  Confronta due `Buffer` per semplificare l'ordinamento degli array. Restituisce `0` se sono uguali, `-1` se viene prima `buffer1` o `1` se viene prima `buffer2`.

  - `buffer1`: immetti un `Buffer`.
  - `buffer2`: immetti un altro `Buffer`.
- `Buffer.concat(list[, totalLength])`

  Concatena più `Buffer`. Restituisce `0` se non ce ne sono. Restituisce fino a `totalLength`.

  - `list`: immetti un elenco di `Buffer`. Tieni presente che verrà troncato a `totalLength`.
  - `totalLength`: facoltativo. Inserisci un numero intero senza segno. Usa la somma delle istanze `Buffer` nell'elenco se vuoto.
- `Buffer.from(array)`

  Crea un `Buffer` da un array.

  - `array`: immetti un array di byte da `0` a `255`.
- `Buffer.from(arrayBuffer, byteOffset[, length]))`

  Crea una vista da `arrayBuffer`, partendo dall'offset `byteOffset` con lunghezza `length`.

  - `arrayBuffer`: immetti una matrice `Buffer`.
  - `byteOffset`: immetti un numero intero.
  - `length`: facoltativo. Immetti un numero intero.
- `Buffer.from(buffer)`

  Crea una copia del `Buffer`.

  - `buffer`: immetti un `Buffer`.
- `Buffer.from(object[, offsetOrEncoding[, length]])`

  Crea un `Buffer` da un oggetto. Restituisce `Buffer.from(object.valueOf(), offsetOrEncoding, length)` se `valueOf()` non è uguale all'oggetto.

  - `object`: immetti un oggetto.
  - `offsetOrEncoding`: facoltativo. Immetti un numero intero o una stringa di codifica.
  - `length`: facoltativo. Immetti un numero intero.
- `Buffer.from(string[, encoding])`

  Crea un `Buffer` da una stringa.

  - `string`: immetti una stringa.
  - `encoding`: facoltativo. Immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.
- `Buffer.isBuffer(object)`

  Controlla se `object` è un buffer. Restituisce `true` o `false`.

  - `object`: immetti un oggetto.
- `Buffer.isEncoding(encoding)`

  Verifica se `encoding` è supportato. Restituisce `true` o `false`.

  - `encoding`: facoltativo. Immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.

Il modulo fornisce i seguenti metodi di prototipo del buffer:

- `Buffer.prototype.compare(target[, targetStart[, targetEnd[, sourceStart[, sourceEnd]]]])`

  Confronta `Buffer` con l'obiettivo. Restituisce `0` se sono uguali, `1` se viene prima `buffer` o `-1` se viene prima `target`.

  - `target`: immetti un `Buffer`.
  - `targetStart`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `targetEnd`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza di `target`.

  - `sourceStart`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `sourceEnd`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza di `Buffer`.
- `Buffer.prototype.copy(target[, targetStart[, sourceStart[, sourceEnd]]])`

  Copia il buffer su `target`.
  - `target`: immetti un `Buffer` o `Uint8Array`.
  - `targetStart`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `sourceStart`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `sourceEnd`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza di `Buffer`.
- `Buffer.prototype.equals(otherBuffer)`

  Confronta `Buffer` con `otherBuffer`. Restituisce `true` o `false`.
  - `otherBuffer`: immetti una stringa.
- `Buffer.prototype.fill(value[, offset[, end][, encoding])`

  Compila `Buffer` con `value`.
  - `value`: immetti una stringa, `Buffer` o un numero intero.
  - `offset`: facoltativo. Immetti un numero intero.
  - `end`: facoltativo. Immetti un numero intero.
  - `encoding`: facoltativo. Immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.
- `Buffer.prototype.includes(value[, byteOffset][, encoding])`

  Cerca `value` in `Buffer`. Restituisce `true` o `false`.
  - `value`: immetti una stringa, `Buffer`, `Uint8Array` o un numero intero.
  - `byteOffset`: facoltativo. Immetti un numero intero.
  - `encoding`: facoltativo. Immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è “”. `utf8`.
- `Buffer.prototype.indexOf(value[, byteOffset][, encoding])`

  Cerca il primo `value` in `Buffer`. Restituisce `index` se trovato e `-1` se non trovato.
  - `value`: immetti una stringa, `Buffer`, Unit8Array o un numero intero compreso tra 0 e 255.

  - `byteOffset`: facoltativo. Immetti un numero intero.
  - `encoding`: facoltativo. Se `value` è una stringa, immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è "". `utf8`.
- `Buffer.prototype.lastIndexOf(value[, byteOffset][, encoding])`

  Cerca l'ultimo `value` in `Buffer`. Restituisce `index` se trovato e `-1` se non trovato.
  - `value`: immetti una stringa, `Buffer`, Unit8Array o un numero intero compreso tra 0 e 255.
  - `byteOffset`: facoltativo. Immetti un numero intero.
  - `encoding`: facoltativo. Se `value` è una stringa, immetti uno dei seguenti valori: `utf8`, `hex`, `base64`, `base64url`. Il valore predefinito è "". `utf8`.
- `Buffer.prototype.readInt8(offset)`

  Leggi `Int8` in `offset` a partire da `Buffer`.
  - `offset`: immetti un numero intero.
- `Buffer.prototype.readIntBE(offset, byteLength)`

  Leggi `Int` come big-endian in `offset` da `Buffer`.
  - `offset`: immetti un numero intero.
  - `byteLength`: facoltativo. Immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.readInt16BE(offset)`

  Leggi `Int16` come big-endian in `offset` da `Buffer`.
  - `offset`: immetti un numero intero.
- `Buffer.prototype.readInt32BE(offset)`

  Leggi `Int32` come big-endian in `offset` da `Buffer`.
  - `offset`: immetti un numero intero.
- `Buffer.prototype.readIntLE(offset, byteLength)`

  Leggi `Int` come little-endian in `offset` da `Buffer`.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.readInt16LE(offset)`

  Leggi `Int16` come little-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
- `Buffer.prototype.readInt32LE(offset)`

  Leggi `Int32` come little-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
- `Buffer.prototype.readUInt8(offset)`

  Leggi `UInt8` in `offset` a partire da `Buffer`.

  - `offset`: immetti un numero intero.
- `Buffer.prototype.readUIntBE(offset, byteLength)`

  Leggi `UInt` come big-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.readUInt16BE(offset)`

  Leggi `UInt16` come big-endian in `offset` da `Buffer`.
- • `offset`: immetti un numero intero.
- `Buffer.prototype.readUInt32BE(offset)`

  Leggi `UInt32` come big-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
- `Buffer.prototype.readUIntLE(offset, byteLength)`

  Leggi `UInt` come little-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.readUInt16LE(offset)`

  Leggi `UInt16` come little-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.
- `Buffer.prototype.readUInt32LE(offset)`

  Leggi `UInt32` come little-endian in `offset` da `Buffer`.

  - `offset`: immetti un numero intero.

- `Buffer.prototype.readDoubleBE([offset])`

  Leggi un file a doppia precisione a 64 bit come big-endian in `offset` da `Buffer`.

  - `offset`: facoltativo. Immetti un numero intero.
- `Buffer.prototype.readDoubleLE([offset])`

  Leggi un file a doppia precisione a 64 bit come little-endian in `offset` da `Buffer`.

  - `offset`: facoltativo. Immetti un numero intero.
- `Buffer.prototype.readFloatBE([offset])`

  Leggi un file a virgola mobile a 32 bit come big-endian in `offset` da `Buffer`.

  - `offset`: facoltativo. Immetti un numero intero.
- `Buffer.prototype.readFloatLE([offset])`

  Leggi un file a virgola mobile a 32 bit come little-endian in `offset` da `Buffer`.

  - `offset`: facoltativo. Immetti un numero intero.
- `Buffer.prototype.subarray([start[, end]])`

  Restituisce una copia di `Buffer` con offset e ritaglio con nuovi valori per `start` e `end`.

  - `start`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `end`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza del buffer.
- `Buffer.prototype.swap16()`

  Scambia l'ordine dei byte dell'array `Buffer`, trattandolo come un array di numeri a 16 bit. La lunghezza di `Buffer` deve essere divisibile per 2, altrimenti riceverai un errore.
- `Buffer.prototype.swap32()`

  Scambia l'ordine dei byte dell'array `Buffer`, trattandolo come un array di numeri a 32 bit. La lunghezza di `Buffer` deve essere divisibile per 4, altrimenti riceverai un errore.
- `Buffer.prototype.swap64()`

  Scambia l'ordine dei byte dell'array `Buffer`, trattandolo come un array di numeri a 64 bit. La lunghezza di `Buffer` deve essere divisibile per 8, altrimenti riceverai un errore.
- `Buffer.prototype.toJSON()`

  Restituisce `Buffer` come file JSON.

- `Buffer.prototype.toString([encoding[, start[, end]]])`

  Converti `Buffer`, da `start` a `end`, in una stringa codificata.

  - `encoding`: facoltativo. Immetti uno dei seguenti valori: `utf8`, `hex`, `base64` o `base64url`. Il valore predefinito è “”. `utf8`.
  - `start`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `end`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza del buffer.
- `Buffer.prototype.write(string[, offset[, length]][, encoding])`

  Scrivi il valore `string` codificato su `Buffer` se c'è spazio a sufficienza o un valore `string` troncato se non c'è abbastanza spazio.

  - `string`: immetti una stringa.
  - `offset`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
  - `length`: facoltativo. Immetti un numero intero. Il valore predefinito è la lunghezza della stringa.
  - `encoding`: facoltativo. Facoltativamente, immetti uno dei seguenti valori: `utf8`, `hex`, `base64` o `base64url`. Il valore predefinito è “”. `utf8`.
- `Buffer.prototype.writeInt8(value, offset, byteLength)`

  Scrivi `Int8` `value` di `byteLength` a `offset` su `Buffer`.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeIntBE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeInt16BE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeInt32BE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeIntLE(offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeInt16LE(offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeInt32LE(offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeUInt8(value, offset, byteLength)`

  Scrivi `UInt8` `value` di `byteLength` a `offset` su `Buffer`.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeUIntBE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.
- `Buffer.prototype.writeUInt16BE(value, offset, byteLength)`

Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

- `value`: immetti un numero intero.
- `offset`: immetti un numero intero.
- `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeUInt32BE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeUIntLE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeUInt16LE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeUInt32LE(value, offset, byteLength)`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `value`: immetti un numero intero.
  - `offset`: immetti un numero intero.
  - `byteLength`: immetti un numero intero compreso tra 1 e 6.

- `Buffer.prototype.writeDoubleBE(value, [offset])`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.

- `Buffer.prototype.writeDoubleLE(value, [offset])`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `value`: immetti un numero intero.
  - `offset`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
- `Buffer.prototype.writeFloatBE(value, [offset])`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo big-endian.

  - `value`: immetti un numero intero.
  - `offset`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.
- `Buffer.prototype.writeFloatLE(value, [offset])`

  Scrivi `value` a `offset` su `Buffer`, usando il metodo little-endian.

  - `value`: immetti un numero intero.
  - `offset`: facoltativo. Immetti un numero intero. Il valore predefinito è 0.

Sono supportati i seguenti metodi di istanza:

- `buffer[index]`

  Ottieni e imposta l'ottetto (byte) a `index` in `Buffer`.

  - Ottieni un numero da `0` a `255`. In alternativa, imposta un numero da `0` a `255`.

Sono supportate le seguenti proprietà di istanza:

- `buffer`

  Ottieni l'oggetto `ArrayBuffer` per il buffer.
- `byteOffset`

  Ottieni il valore `byteOffset` per l'oggetto `Arraybuffer` del buffer.
- `length`

  Ottieni il conteggio dei byte del buffer.

> **Note**
>
> Tutti i metodi del modulo Buffer rappresentano delle novità nel runtime JavaScript 2.0.

Stringa di query

> **Note**
>
> L'oggetto evento di CloudFront Functions analizza automaticamente le stringhe di query URL per tuo conto. Ciò significa che nella maggior parte dei casi non è necessario utilizzare questo modulo.

Il modulo stringa di query (`querystring`) fornisce metodi per l'analisi e la formattazione delle stringhe di query URL. È possibile caricare il modulo usando `require('querystring')`. Il modulo fornisce i metodi seguenti:

`querystring.escape(`*`string`*`)`

URL che codifica il dato `string`, restituendo una stringa di query con escape. Il metodo viene utilizzato da `querystring.stringify()` e non deve essere utilizzato direttamente.

`querystring.parse(`*`string`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Analizza una stringa di query (`string`) e restituisce un oggetto.

Il parametro `separator` è una sottostringa per delimitare coppie chiave e valore nella stringa di query. Per impostazione predefinita, tale valore è &.

Il parametro `equal` è una sottostringa per la delimitazione di chiavi e valori nella stringa di query. Per impostazione predefinita, tale valore è =.

Il parametro `options` è un oggetto con le seguenti chiavi:

`decodeURIComponent` *`function`*

Un funzione per decodificare i caratteri codificati in percentuale nella stringa di query. Per impostazione predefinita, tale valore è `querystring.unescape()`.

`maxKeys` *`number`*

Il numero massimo di chiavi da analizzare. Per impostazione predefinita, tale valore è `1000`. Utilizza un valore `0` per rimuovere le limitazioni per il conteggio delle chiavi.

Per impostazione predefinita, si presuppone che i caratteri con codifica in percentuale all'interno della stringa di query utilizzino la codifica UTF-8. Le sequenze UTF-8 non valide vengono sostituite con il carattere sostitutivo `U+FFFD`.

Ad esempio, per la seguente stringa di query:

```
'name=value&abc=xyz&abc=123'
```

Il valore restituito di `querystring.parse()` è:

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` è un alias per `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Serializza un `object` e restituisce una stringa di query.

Il parametro `separator` è una sottostringa per delimitare coppie chiave e valore nella stringa di query. Per impostazione predefinita, tale valore è &.

Il parametro `equal` è una sottostringa per la delimitazione di chiavi e valori nella stringa di query. Per impostazione predefinita, tale valore è =.

Il parametro `options` è un oggetto con le seguenti chiavi:

`encodeURIComponent` *`function`*

La funzione da utilizzare per convertire caratteri non sicuri dell'URL in codifica percentuale nella stringa di query. Per impostazione predefinita, tale valore è `querystring.escape()`.

Per impostazione predefinita, i caratteri che richiedono la codifica percentuale all'interno della stringa di query sono codificati come UTF-8. Per utilizzare una codifica diversa, specifica l'opzione `encodeURIComponent`.

Ad esempio, per il seguente codice:

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

Il valore restituito è:

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` è un alias per `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Decodifica i caratteri codificati in percentuale URL nel dato `string`, restituendo una stringa di query senza escape. Questo metodo viene utilizzato da `querystring.parse()` e non deve essere utilizzato direttamente.

Crittografia

Il modulo di crittografia (`crypto`) fornisce helper di hashing standard e HMAC (Hash Message Authentication Code). È possibile caricare il modulo usando `require('crypto')`.

Metodi di hashing

`crypto.createHash(`*`algorithm`*`)`

Crea e restituisce un oggetto hash che è possibile utilizzare per generare digest hash utilizzando il dato algoritmo: `md5`, `sha1`, o `sha256`.

`hash.update(`*`data`*`)`

Aggiorna il contenuto hash con il dato `data`.

`hash.digest([`*`encoding`*`])`

Calcola il digest di tutti i dati passati tramite `hash.update()`. La codifica può essere `hex`, `base64` o `base64url`.

Metodi HMAC

`crypto.createHmac(`*`algorithm, secret key`*`)`

Crea e restituisce un oggetto HMAC che utilizza il dato `algorithm` e `secret key`. L'algoritmo può essere `md5`, `sha1` o `sha256`.

`hmac.update(data)`

Aggiorna il contenuto HMAC con il dato `data`.

`hmac.digest([encoding])`

Calcola il digest di tutti i dati passati tramite `hmac.update()`. La codifica può essere `hex`, `base64` o `base64url`.

Funzionalità con restrizioni

Le seguenti funzionalità del linguaggio JavaScript non sono supportate o sono limitate a causa di problemi di sicurezza.

Valutazione dinamica del codice

La valutazione dinamica del codice non è supportata. Entrambi i costruttori `eval()` e `Function` generano un errore se tentato. Ad esempio, `const sum = new Function('a', 'b', 'return a + b')` genera un errore.

Timer

Le funzioni `setTimeout()`, `setImmediate()` e `clearTimeout()` non sono supportate. Non vi è alcuna disposizione per differire o cedere all'interno di un'esecuzione di funzione. La funzione deve essere eseguita in modo sincrono fino al completamento.

Data e timestamp

Per motivi di sicurezza, non è possibile accedere ai timer ad alta risoluzione. Tutti i metodi `Date` per interrogare l'ora corrente restituiscono sempre lo stesso valore durante la durata di una singola esecuzione di funzione. Il timestamp restituito è il momento in cui la funzione ha iniziato l'esecuzione. Di conseguenza, non è possibile misurare il tempo trascorso nella vostra funzione.

Accesso al file system

Nessun accesso al file system. Ad esempio, non esiste un modulo `fs` per l'accesso al file system come invece è presente in Node.js.

Accesso al processo

Non è possibile accedere al processo. Ad esempio, non esiste un oggetto globale `process` per l’elaborazione dell’accesso alle informazioni come in Node.js.

Variabili di ambiente

Non è possibile accedere alle variabili d'ambiente. È invece possibile utilizzare KeyValueStore di CloudFront per creare un datastore centralizzato di coppie chiave-valore per le Funzioni CloudFront. KeyValueStore di CloudFront consente aggiornamenti dinamici dei dati di configurazione senza dover implementare modifiche al codice. Per ulteriori informazioni, consulta Amazon CloudFront KeyValueStore.

Accesso alla rete

Non è disponibile alcun supporto per le chiamate di rete. Ad esempio, XHR, HTTP(S) e socket non sono supportati.

Metodi helper per archivi di valori delle chiavi

> **Note**
>
> Le chiamate al metodo di supporto Key Value Store da CloudFront Functions non attivano un evento di AWS CloudTrail dati. Questi eventi non vengono registrati nella cronologia degli CloudTrail eventi. Per ulteriori informazioni, consulta Registrazione di log delle chiamate API Amazon CloudFront utilizzando AWS CloudTrail.

Questa sezione si applica se utilizzi CloudFront Key Value Store per includere valori chiave nella funzione che crei. CloudFront Functions ha un modulo che fornisce tre metodi di supporto per leggere i valori dall'archivio di valori chiave.

Per utilizzare questo modulo nel codice della funzione, assicurati di aver associato un archivio di valori delle chiavi alla funzione.

Quindi, includi le seguenti istruzioni nelle prime righe del codice della funzione:

```
import cf from 'cloudfront';
const kvsHandle = cf.kvs();
```

Metodo **`get()`**

Utilizza questo metodo per restituire il valore della chiave per il nome chiave specificato.

Richiesta

```
get("key", options);
```

- `key`: il nome della chiave di cui è necessario recuperare il valore
- `options`: è presente un'opzione, `format`. Assicura che la funzione analizzi correttamente i dati. Valori possibili:
  - `string`: (Predefinito) UTF8 codificato
  - `json`
  - `bytes`: buffer di dati binari non elaborati

Esempio di richiesta

```
const value = await kvsHandle.get("myFunctionKey", { format: "string"});
```

Risposta

La risposta è una `promise` che si risolve in un valore nel formato richiesto utilizzando `options`. Per impostazione predefinita, il valore viene restituito come stringa.

Gestione degli errori

Il metodo `get()` restituirà un errore quando la chiave richiesta non esiste nell'archivio di valori delle chiavi associato. Per gestire questo caso d'uso, puoi aggiungere un blocco `catch` e `try` al codice.

> **Warning**
>
> L'uso dei combinatori di promesse (ad esempio, `Promise.all`, `Promise.any`) e dei metodi di catena di promesse (ad esempio, `then` e `catch`) può richiedere un elevato utilizzo della memoria delle funzioni. Se la funzione supera la quota massima di memoria delle funzioni, non verrà eseguita. Per evitare questo errore, ti consigliamo di utilizzare la sintassi `await` in modo sequenziale o in loop per richiedere più valori.
> Esempio
>
> ```
> var value1 = await kvs.get('key1');
> var value2 = await kvs.get('key2');
> ```
>
> Attualmente, l'uso dei combinatori di promesse per ottenere più valori non migliora le prestazioni, come nell'esempio seguente.

```
var values = await Promise.all([kvs.get('key1'), kvs.get('key2'),]);
```

Metodo **exists()**

Utilizza questo metodo per verificare se la chiave è presente o meno nell'archivio di valori delle chiavi.

Richiesta

```
exists("key");
```

Esempio di richiesta

```
const exist = await kvsHandle.exists("myFunctionkey");
```

Risposta

La risposta è un `promise` che restituisce un valore booleano (`true` o `false`). Questo valore specifica se la chiave esiste o meno nell'archivio di valori delle chiavi.

Metodo **meta()**

Utilizza questo metodo per restituire i metadati relativi all'archivio di valori delle chiavi.

Richiesta

```
meta();
```

Esempio di richiesta

```
const meta = await kvsHandle.meta();
```

Risposta

La risposta è un valore `promise` che si risolve in un oggetto con le seguenti proprietà:

- `creationDateTime`: la data e l'ora di creazione dell'archivio di valori delle chiavi, nel formato ISO 8601.
- `lastUpdatedDateTime`: la data e l'ora dell'ultima sincronizzazione dell'archivio di valori delle chiavi, nel formato ISO 8601. Il valore non include il tempo di propagazione verso l'edge.
- `keyCount`: il numero totale di chiavi in KVS dopo l'ultima sincronizzazione dalla sorgente.

Esempio di risposta

```
{keyCount:3,creationDateTime:2023-11-30T23:07:55.765Z,lastUpdatedDateTime:2023-12-15T03:57:52.4
```

Metodi di assistente di gestione per la modifica dell'origine

Questa sezione si applica se aggiorni o modifichi dinamicamente l'origine utilizzata nella richiesta all'interno del codice CloudFront Functions. Puoi aggiornare l'origine solo su richiesta del visualizzatore CloudFront Functions. CloudFront Functions dispone di un modulo che fornisce metodi di supporto per aggiornare o modificare dinamicamente l'origine.

Per utilizzare questo modulo, create una CloudFront funzione utilizzando JavaScript runtime 2.0 e includete la seguente dichiarazione nella prima riga del codice della funzione:

```
import cf from 'cloudfront';
```

Per ulteriori informazioni, consulta Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront.

> **Note**
>
> Le pagine della console Esegui test API ed Esegui test non controllano se si è verificata una modifica dell'origine. Tuttavia, il test garantisce che il codice della funzione venga eseguito senza errori.

Scegli tra CloudFront Functions e Lambda @Edge

Puoi aggiornare le tue origini utilizzando CloudFront Functions o Lambda @Edge.

Quando si utilizza CloudFront Functions per aggiornare le origini, si utilizza il trigger dell'evento Viewer Request, il che significa che questa logica verrà eseguita su ogni richiesta quando viene

utilizzata questa funzione. Quando si utilizza Lambda@Edge, le funzionalità di aggiornamento dell'origine si trovano nel trigger dell'evento di richiesta origine, il che significa che questa logica viene eseguita solo in caso di perdita della cache.

La scelta dipende in gran parte dal carico di lavoro e dall'eventuale utilizzo esistente di CloudFront Functions e Lambda @Edge nelle distribuzioni. Le seguenti considerazioni possono aiutarti a decidere se utilizzare CloudFront Functions o Lambda @Edge per aggiornare le tue origini.

CloudFront Functions è particolarmente utile nelle seguenti situazioni:

- Quando le tue richieste sono dinamiche (il che significa che non possono essere memorizzate nella cache) e andranno sempre all'origine. CloudFront Functions offre prestazioni migliori e costi complessivi inferiori.
- Se disponi già di una CloudFront funzione di richiesta del visualizzatore che verrà eseguita su ogni richiesta, puoi aggiungere la logica di aggiornamento dell'origine alla funzione esistente.

Per utilizzare CloudFront Functions per aggiornare le origini, consultate i metodi di supporto nei seguenti argomenti.

Lambda@Edge è particolarmente utile nelle seguenti situazioni:

- Quando si dispone di contenuti altamente memorizzabili nella cache, Lambda @Edge può essere più efficiente in termini di costi perché viene eseguito solo in caso di errori di cache, mentre Functions viene eseguito su ogni richiesta. CloudFront
- Se disponi già di una funzione Lambda@Edge per le richieste origine, puoi aggiungere la logica di aggiornamento dell'origine alla funzione esistente.
- Quando la logica di aggiornamento dell'origine richiede il recupero di dati da origini dati di terze parti, come Amazon DynamoDB o Amazon S3.

Per ulteriori informazioni su Lambda@Edge, consulta Personalizzazione al livello di edge con Lambda@Edge.

updateRequestOriginmetodo ()

Utilizza il metodo `updateRequestOrigin()` per aggiornare le impostazioni di origine per una richiesta. Puoi utilizzare questo metodo per aggiornare le proprietà di origine esistenti per le origini già definite nella distribuzione o per definire una nuova origine per la richiesta. A tale scopo, specifica le proprietà che desideri modificare.

> **Important**
>
> Tutte le impostazioni non specificate in `updateRequestOrigin()` erediteranno le stesse impostazioni dalla configurazione dell'origine esistente.

L'origine impostata dal `updateRequestOrigin()` metodo può essere qualsiasi endpoint HTTP e non è necessario che sia un'origine esistente all'interno della CloudFront distribuzione.

> **Note**
>
> - Se stai aggiornando un'origine che fa parte di un gruppo di origine, viene aggiornata solo l'origine principale del gruppo di origine. L'origine secondaria rimane invariata. Qualsiasi codice di risposta proveniente dall'origine modificata che soddisfi i criteri di failover attiverà un failover all'origine secondaria.
> - Se stai modificando il tipo di origine e hai abilitato l'OAC, assicurati che il tipo di origine in `originAccessControlConfig` corrisponda al nuovo tipo di origine.
> - Non puoi utilizzare il metodo `updateRequestOrigin()` per aggiornare VPC Origins. La richiesta non andrà a buon fine.

Richiesta

```
updateRequestOrigin({origin properties})
```

Le `origin properties` possono contenere i seguenti valori:

domainName (facoltativo)

Il nome di dominio dell'origine. Se non è fornito, viene utilizzato il nome di dominio dell'origine assegnata.

Per origini personalizzate

Specifica un nome di dominio DNS, ad esempio `www.example.com`. Il nome di dominio non può includere i due punti (`:`) e non può essere un indirizzo IP. Il nome di dominio può contenere fino a 253 caratteri.

Per origini S3

Specifica il nome di dominio DNS del bucket Amazon S3, ad esempio `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. Il nome può contenere fino a 128 caratteri e deve essere tutto in minuscolo.

HostHeader (opzionale, per origini personalizzate non S3)

L'intestazione host da utilizzare quando si effettua la richiesta all'origine. Se questo non viene fornito, viene utilizzato il valore del parametro DomainName. Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'intestazione host non può includere i due punti (`:`) e non può essere un indirizzo IP. L'intestazione host può contenere fino a 253 caratteri.

originPath (facoltativo)

Il percorso di directory sul server di origine in cui la richiesta deve trovare il contenuto. Il percorso può iniziare, ma non deve terminare, con una barra (/). Ad esempio, non deve terminare con `example-path/`. Se questo non è fornito, viene utilizzato il percorso di origine dall'origine assegnata.

Per origini personalizzate

Il percorso deve essere codificato URL e avere una lunghezza massima di 255 caratteri.

customHeaders (facoltativo)

Puoi includere intestazioni personalizzate con la richiesta specificando un nome di intestazione e una coppia di valori per ogni intestazione personalizzata. Il formato è diverso da quello delle intestazioni di richiesta e risposta nella struttura dell'evento. Utilizza la seguente sintassi della coppia chiave-valore:

```
{"key1": "value1", "key2": "value2", ...}
```

Non è possibile aggiungere intestazioni non consentite e un'intestazione con lo stesso nome non può essere presente anche nelle `headers` della richiesta in entrata. Il nome dell'intestazione deve essere in minuscolo nel codice della funzione. Quando CloudFront Functions riconverte l'oggetto evento in una richiesta HTTP, la prima lettera di ogni parola nei nomi delle intestazioni viene scritta in maiuscolo e le parole sono separate da un trattino.

Ad esempio, se il codice di funzione aggiunge un'intestazione denominata`example-header-name`, la CloudFront converte in nella richiesta HTTP. `Example-Header-Name` Per ulteriori

informazioni, consultare Intestazioni personalizzate che CloudFront non può aggiungere alle richieste di origine e Restrizioni sulle funzioni edge.

Se questo non viene fornito, vengono utilizzate le intestazioni personalizzate dell'origine assegnata.

connectionAttempts (facoltativo)

Il numero di volte che CloudFront tenta di connettersi all'origine. Il valore minimo è 1 e il valore massimo è 3. Se questo non viene fornito, vengono utilizzati i tentativi di connessione dall'origine assegnata.

originShield (facoltativo)

Ciò abilita o aggiorna CloudFront Origin Shield. L'utilizzo di Origin Shield può contribuire a ridurre il carico sulla tua origine. Per ulteriori informazioni, consulta Usa Amazon CloudFront Origin Shield. Se questo non è fornito, vengono utilizzate le impostazioni Origin Shield dall'origine assegnata.

enabled (obbligatorio)

Espressione booleana per abilitare o disabilitare Origin Shield. Accetta un valore `true` o `false`.

region (obbligatorio se abilitato)

The Regione AWS for Origin Shield. Specifica la Regione AWS con la latenza più bassa all'origine. Utilizza il codice della regione, non il nome della regione. Ad esempio, utilizza `us-east-2` per specificare la regione Stati Uniti orientali (Ohio).

Quando abiliti CloudFront Origin Shield, devi specificare Regione AWS il nome. Per un elenco delle Regioni AWS disponibili e informazioni sulla scelta della regione migliore per l'origine, consulta Scegli la AWS regione per Origin Shield.

originAccessControlConfig (opzionale)

L'identificativo univoco di un controllo di accesso origine (OAC) per tale origine. Viene utilizzato solo quando l'origine supporta un CloudFront OAC, come Amazon S3, la URLs funzione MediaStore Lambda e V2. MediaPackage Se questo non viene fornito, vengono utilizzate le impostazioni OAC dell'origine assegnata.

Questo non supporta l'identità di accesso origine (OAI) legacy. Per ulteriori informazioni, consulta Limitazione dell'accesso a un'origine AWS.

enabled (obbligatorio)

Espressione booleana per abilitare o disabilitare OAC. Accetta un valore `true` o `false`.

signingBehavior (obbligatorio se abilitato)

Speciifica a quali richieste si riferisce (aggiunge le CloudFront informazioni di autenticazione). Specifica `always` per il caso d'uso più comune. Per ulteriori informazioni, consulta Impostazioni avanzate per il controllo dell'accesso all'origine.

Questo campo può avere uno dei seguenti valori:

- `always`— CloudFront firma tutte le richieste di origine, sovrascrivendo l'`Authorization`intestazione della richiesta del visualizzatore, se ne esiste una.
- `never`— CloudFront non firma alcuna richiesta di origine. Questo valore disattiva il controllo di accesso origine per l'origine.
- `no-override`— Se la richiesta del visualizzatore non contiene l'`Authorization`intestazione, CloudFront firma la richiesta di origine. Se la richiesta del visualizzatore contiene l'`Authorization`intestazione, CloudFront non firma la richiesta di origine e trasmette invece l'`Authorization`intestazione della richiesta del visualizzatore.

> **Warning**
>
> Per trasmettere l'intestazione `Authorization` dalla richiesta visualizzatore, è necessario aggiungerla a una policy di richiesta origine per tutti i comportamenti cache che utilizzano origini associate a questo controllo di accesso origine. Per ulteriori informazioni, consulta Controllo delle richieste di origine con una policy.

signingProtocol (richiesto se abilitato)

Il protocollo di firma dell'OAC, che determina il modo in cui CloudFront firma (autentica) le richieste. L'unico valore valido è `sigv4`.

originType (richiesto se abilitato)

Il tipo di origine per questo OAC. I valori validi includono `s3`, `mediapackagev2`, `mediastore` e `lambda`.

timeout (facoltativo)

I timeout che puoi specificare per quanto tempo CloudFront devono cercare di attendere che le origini rispondano o inviino dati. Se questo non viene fornito, vengono utilizzate le impostazioni di timeout dell'origine assegnata.

> **Note**
>
> Se non diversamente specificato, questi timeout supportano sia origini personalizzate che origini Amazon S3.

readTimeout (facoltativo)

`readTimeout` si applica a entrambi i seguenti valori:

- Quanto tempo (in secondi) CloudFront attende una risposta dopo l'inoltro di una richiesta all'origine.
- Quanto tempo (in secondi) CloudFront attende dopo aver ricevuto un pacchetto di risposta dall'origine e prima di ricevere il pacchetto successivo.

Il timeout minimo è di 1 secondo e quello massimo è di 120 secondi. Per ulteriori informazioni, consulta Timeout di risposta.

responseCompletionTimeout (facoltativo)

Il tempo (in secondi) durante il quale una richiesta dall' CloudFront origine può rimanere aperta e attendere una risposta. Se la risposta completa non viene ricevuta dall'origine entro quest'ora, CloudFront termina la connessione.

Il valore per `responseCompletionTimeout` deve essere maggiore o uguale al valore per `readTimeout`. Per ulteriori informazioni, consulta Timeout completamento risposta.

keepAliveTimeout (facoltativo)

Questo timeout si applica solo alle origini personalizzate, non alle origini Amazon S3. Le configurazioni di origine S3 ignoreranno queste impostazioni.

`keepAliveTimeout`Indica per quanto tempo CloudFront deve cercare di mantenere la connessione all'origine dopo aver ricevuto l'ultimo pacchetto della risposta. Il timeout minimo è di 1 secondo e quello massimo è di 120 secondi. Per ulteriori informazioni, consulta Timeout keep-alive (solo origini personalizzate e VPC).

connectionTimeout (facoltativo)

Il numero di secondi che CloudFront attendono quando si tenta di stabilire una connessione all'origine. Il timeout minimo è di 1 secondo e quello massimo è di 10 secondi. Per ulteriori informazioni, consulta Timeout di connessione.

customOriginConfig (facoltativo)

Utilizza `customOriginConfig` per specificare le impostazioni di connessione per origini che non sono un bucket Amazon S3. C'è un'eccezione: puoi specificare queste impostazioni se il bucket S3 è configurato con hosting di siti web statici. Altri tipi di configurazioni di bucket S3 ignoreranno queste impostazioni. Se `customOriginConfig` non viene fornito, vengono utilizzate le impostazioni dell'origine assegnata.

port (obbligatorio)

La porta HTTP CloudFront utilizzata per connettersi all'origine. La porta HTTP sulla quale l'origine è in ascolto.

protocol (obbligatorio)

Speciifica il protocollo (HTTP o HTTPS) CloudFront utilizzato per connettersi all'origine. I valori validi sono:

- `http`— utilizza CloudFront sempre HTTP per connettersi all'origine
- `https`— utilizza CloudFront sempre HTTPS per connettersi all'origine

sslProtocols (obbligatorio)

Un elenco che specifica il SSL/TLS protocollo minimo da CloudFront utilizzare per la connessione all'origine tramite HTTPS. I valori validi includono `SSLv3`, `TLSv1`, `TLSv1.1` e `TLSv1.2`. Per ulteriori informazioni, consulta Protocollo SSL di origine minimo.

ipAddressType (facoltativo)

Speciifica il tipo di indirizzo IP CloudFront utilizzato per la connessione all'origine. I valori validi includono `ipv4`, `ipv6` e `dualstack`. La modifica di `ipAddressType` è supportata solo quando viene modificata anche la proprietà `domainName`.

sni (opzionale, per origini personalizzate non S3)

La Server Name Indication (SNI) è un'estensione del protocollo Transport Layer Security (TLS) con cui un client indica a quale nome host sta tentando di connettersi all'inizio del processo di handshake TLS. Questo valore deve corrispondere a un nome comune su un certificato TLS sul server di origine. In caso contrario, il server di origine potrebbe generare un errore.

Se questo non viene fornito, viene utilizzato il valore del `hostHeader` parametro. Se l'intestazione dell'host non viene fornita, viene utilizzato il valore del `domainName` parametro.

Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'SNI non può includere i due punti (`:`) e non può essere un indirizzo IP. Il codice SNI può contenere fino a 253 caratteri.

allowedCertificateNames (opzionale, per origini personalizzate non S3)

È possibile includere un elenco di nomi di certificati validi da utilizzare per CloudFront convalidare la corrispondenza del dominio con il certificato TLS del server di origine durante l'handshake TLS con il server di origine. Questo campo prevede una matrice di nomi di dominio validi e può includere domini wildcard, come. `*.example.com`

È possibile specificare fino a 20 nomi di certificato consentiti. Ogni nome di certificato può contenere fino a 64 caratteri.

Example — Aggiornamento dell'origine richiesta Amazon S3

Nell'esempio seguente viene modificata l'origine della richiesta visualizzatore in un bucket S3, abilitato OAC e ripristinate le intestazioni personalizzate inviate all'origine.

```
cf.updateRequestOrigin({
    "domainName" : "amzn-s3-demo-bucket-in-us-east-1.s3.us-east-1.amazonaws.com",
    "originAccessControlConfig": {
        "enabled": true,
        "signingBehavior": "always",
        "signingProtocol": "sigv4",
        "originType": "s3"
    },
    // Empty object resets any header configured on the assigned origin
    "customHeaders": {}
});
```

Example — Aggiornamento dell'origine richiesta di Application Load Balancer

Nell'esempio seguente viene modificata l'origine della richiesta visualizzatore in un'origine Application Load Balancer e impostata un'intestazione e timeout personalizzati.

```
cf.updateRequestOrigin({
```

```
    "domainName" : "example-1234567890.us-east-1.elb.amazonaws.com",
    "timeouts": {
        "readTimeout": 30,
        "connectionTimeout": 5
    },
    "customHeaders": {
        "x-stage": "production",
        "x-region": "us-east-1"
    }
});
```

Example — Aggiornamento dell'origine con Origin Shield abilitato

Nell'esempio seguente, Origin Shield è abilitato nell'origine della distribuzione. Il codice funzione aggiorna solo il nome di dominio utilizzato per l'origine e omette tutti gli altri parametri opzionali. In questo caso, Origin Shield continuerà a essere utilizzato con il nome di dominio di origine modificato poiché i parametri di Origin Shield non sono stati aggiornati.

```
cf.updateRequestOrigin({
    "domainName" : "www.example.com"
});
```

Example — Aggiorna l'intestazione dell'host, l'SNI e i nomi dei certificati consentiti

> **Warning**
>
> Nella maggior parte dei casi d'uso, non è necessario utilizzare questo tipo di modifica per le richieste che arrivano all'origine. Questi parametri non devono essere utilizzati a meno che non si comprenda l'impatto della modifica di questi valori.

L'esempio seguente modifica il nome di dominio, l'intestazione dell'host, l'SNI e i certificati consentiti dalla richiesta all'origine.

```
cf.updateRequestOrigin({
    "domainName": "www.example.com",
    "hostHeader": "test.example.com",
    "sni": "test.example.net",
    "allowedCertificateNames": ["*.example.com", "*.example.net"],
});
```

selectRequestOriginByIdmetodo ()

Utilizza `selectRequestOriginById()` per aggiornare un'origine esistente selezionando un'origine diversa già configurata nella distribuzione. Questo metodo utilizza tutte le stesse impostazioni definite dall'origine aggiornata.

Questo metodo accetta solo origini già definite nella stessa distribuzione utilizzata durante l'esecuzione della funzione. Le origini sono identificate dall'ID origine, ovvero il nome origine definito durante la configurazione dell'origine.

Se nella distribuzione è configurata un'origine VPC, puoi utilizzare questo metodo per aggiornare l'origine all'origine VPC. Per ulteriori informazioni, consulta Limitazione dell'accesso con VPC Origins.

Richiesta

```
cf.selectRequestOriginById(origin_id, {origin_overrides})
```

Nell'esempio precedente, `origin_id` è una stringa che punta al nome di origine di un'origine nella distribuzione che esegue la funzione. Il `origin_overrides` parametro può contenere quanto segue:

HostHeader (opzionale, per origini personalizzate non S3)

L'intestazione host da utilizzare quando si effettua la richiesta all'origine. Se non viene fornito, viene utilizzato il valore del `domainName` parametro.

Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'intestazione host non può includere i due punti (`:`) e non può essere un indirizzo IP. L'intestazione host può contenere fino a 253 caratteri.

sni (opzionale, per origini personalizzate non S3)

La Server Name Indication (SNI) è un'estensione del protocollo Transport Layer Security (TLS) con cui un client indica a quale nome host sta tentando di connettersi all'inizio del processo di handshake TLS. Questo valore deve corrispondere a un nome comune su un certificato TLS sul server di origine. In caso contrario, il server di origine potrebbe generare un errore.

Se questo non viene fornito, viene utilizzato il valore del `hostHeader` parametro. Se l'intestazione dell'host non viene fornita, viene utilizzato il valore del `domainName` parametro.

Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'SNI non può includere i due punti (`:`) e non può essere un indirizzo IP. Il codice SNI può contenere fino a 253 caratteri.

allowedCertificateNames (opzionale, per origini personalizzate non S3)

È possibile includere un elenco di nomi di certificati validi da utilizzare per CloudFront convalidare la corrispondenza del dominio con il certificato TLS del server di origine durante l'handshake TLS con il server di origine. Questo campo prevede una matrice di nomi di dominio validi e può includere domini wildcard, come. `*.example.com`

È possibile specificare fino a 20 nomi di certificato consentiti. Ogni nome di certificato può contenere fino a 64 caratteri.

Richiesta

```
selectRequestOriginById(origin_id)
```

Nell'esempio precedente, `origin_id` è una stringa che punta al nome dell'origine nella distribuzione che esegue la funzione.

Example — Selezione dell'origine della richiesta Amazon S3

Nell'esempio seguente viene selezionata l'origine denominata `amzn-s3-demo-bucket-in-us-east-1` dall'elenco delle origini associate alla distribuzione e applicate le impostazioni di configurazione dell'origine `amzn-s3-demo-bucket-in-us-east-1` alla richiesta.

```
cf.selectRequestOriginById("amzn-s3-demo-bucket-in-us-east-1");
```

Example — Selezione dell'origine della richiesta Application Load Balancer

Nell'esempio seguente viene selezionata un'origine Application Load Balancer denominata `myALB-prod` dall'elenco delle origini associate alla distribuzione e applicate le impostazioni di configurazione di `myALB-prod` alla richiesta.

```
cf.selectRequestOriginById("myALB-prod");
```

Example — Seleziona l'origine della richiesta Application Load Balancer e sovrascrivi l'intestazione dell'host

Come nell'esempio precedente, l'esempio seguente seleziona un'origine Application Load Balancer `myALB-prod` denominata dall'elenco di origini associate alla distribuzione e applica le impostazioni `myALB-prod` di configurazione di alla richiesta. Tuttavia, questo esempio sostituisce il valore dell'intestazione dell'host utilizzando. `origin_overrides`

```
cf.overrideRequestOrigin("myALB-prod",{
        "hostHeader" : "test.example.com"
});
```

createRequestOriginMetodo Group ()

Utilizza `createRequestOriginGroup()` per definire due origini da utilizzare come gruppo di origine per il failover in scenari che richiedono un'elevata disponibilità.

Un gruppo di origine include due origini (una primaria e una secondaria) e un criterio di failover specificato. Si crea un gruppo di origine per supportare il failover di origine in CloudFront. Quando si crea o si aggiorna un gruppo di origine utilizzando questo metodo, è possibile specificare il gruppo di origine anziché una singola origine. CloudFront eseguirà il failover dall'origine primaria all'origine secondaria, utilizzando i criteri di failover.

Se nella distribuzione è configurata un'origine VPC, puoi utilizzare questo metodo per creare un gruppo di origini utilizzando un'origine VPC. Per ulteriori informazioni, consulta Limitazione dell'accesso con VPC Origins.

Richiesta

```
createRequestOriginGroup({origin_group_properties})
```

Nell'esempio precedente, `origin_group_properties` può contenere quanto segue:

originIds (obbligatorio)

Array di `origin_ids`, dove `origin_id` è una stringa che punta al nome di origine di un'origine nella distribuzione che esegue la funzione. È necessario fornire due origini come parte dell'array. La prima origine nell'elenco è l'origine primaria, mentre la seconda funge da origine secondaria per il failover.

OriginOverrides (opzionale)

È possibile sovrascrivere alcune impostazioni avanzate utilizzando il parametro. `{origin_overrides}` Le `origin overrides` possono contenere i seguenti valori:

HostHeader (opzionale, per origini personalizzate non S3)

L'intestazione host da utilizzare quando si effettua la richiesta all'origine. Se non viene fornito, viene utilizzato il valore del `domainName` parametro.

Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'intestazione host non può includere i due punti (`:`) e non può essere un indirizzo IP. L'intestazione host può contenere fino a 253 caratteri.

sni (opzionale, per origini personalizzate non S3)

La Server Name Indication (SNI) è un'estensione del protocollo Transport Layer Security (TLS) con cui un client indica a quale nome host sta tentando di connettersi all'inizio del processo di handshake TLS. Questo valore deve corrispondere a un nome comune su un certificato TLS sul server di origine, altrimenti il server di origine potrebbe generare un errore.

Se questo non viene fornito, viene utilizzato il valore del `hostHeader` parametro. Se l'intestazione dell'host non viene fornita, viene utilizzato il valore del `domainName` parametro.

Se non vengono forniti né l'intestazione host né il parametro del nome di dominio, viene utilizzato il nome di dominio dell'origine assegnata o l'intestazione host della richiesta in entrata se la politica di inoltro all'origine (FTO) include l'host. L'SNI non può includere i due punti (`:`) e non può essere un indirizzo IP. Il codice SNI può contenere fino a 253 caratteri.

allowedCertificateNames (opzionale, per origini personalizzate non S3)

È possibile includere un elenco di nomi di certificati validi da utilizzare per CloudFront convalidare la corrispondenza del dominio con il certificato TLS del server di origine durante l'handshake TLS con il server di origine. Questo campo prevede una matrice di nomi di dominio validi e può includere domini wildcard, come. `*.example.com`

È possibile specificare fino a 20 nomi di certificato consentiti. Ogni nome di certificato può contenere fino a 64 caratteri.

selectionCriteria (facoltativo)

Scegli se utilizzare i criteri di failover di origine `default` o la logica di failover basata su `media-quality-score`. I valori validi sono:

- `default` utilizza i criteri di failover, in base ai codici di stato specificati in `failoverCriteria`. Se non si imposta `selectionCriteria` nella funzione, verrà utilizzato `default`.
- `media-quality-score` viene utilizzato quando è attiva la funzionalità di instradamento sensibile ai contenuti multimediali.

failoverCriteria (obbligatorio)

Una serie di codici di stato che, se restituiti dall'origine principale, attivano CloudFront il failover sull'origine secondaria. Se si sovrascrive un gruppo di origine esistente, questo array sovrascriverà tutti i codici di stato di failover impostati nella configurazione originale del gruppo di origine.

Quando lo utilizzi `media-quality-scoreselectionCriteria`, CloudFront tenterà di indirizzare le richieste in base al punteggio di qualità multimediale. Se l'origine selezionata restituisce un codice di errore impostato in questo array, CloudFront eseguirà il failover sull'altra origine.

Example — Creazione del gruppo di origini della richiesta

L'esempio seguente crea un gruppo di origine per una richiesta utilizzando l'origine IDs. Queste origini IDs provengono dalla configurazione del gruppo di origine per la distribuzione utilizzata per eseguire questa funzione.

Facoltativamente, è possibile utilizzare `originOverrides` per sovrascrivere le configurazioni del gruppo di origine per`sni`, `hostHeader` e. `allowedCertificateNames`

```
import cf from 'cloudfront';

function handler(event) {
    cf.createRequestOriginGroup({
        "originIds": [
            {
                "originId": "origin-1",
                "originOverrides": {
                    "hostHeader": "hostHeader.example.com",
```

```
                    "sni": "sni.example.com",
                    "allowedCertificateNames": ["cert1.example.com",
 "cert2.example.com", "cert3.example.com"]
                }
            },
            {
                "originId": "origin-2",
                "originOverrides": {
                    "hostHeader": "hostHeader2.example.com",
                    "sni": "sni2.example.com",
                    "allowedCertificateNames": ["cert4.example.com",
 "cert5.example.com"]
                }
            }
        ],
        "failoverCriteria": {
            "statusCodes": [500]
        }
    });

    event.request.headers['x-hookx'] = { value: 'origin-overrides' };
    return event.request;
}
```

Metodi di supporto per le proprietà di CloudFront SaaS Manager

Utilizza le seguenti funzioni di supporto per CloudFront SaaS Manager per recuperare i valori per le distribuzioni multi-tenant nella funzione che crei. Per utilizzare gli esempi in questa pagina, è necessario innanzitutto creare una CloudFront funzione utilizzando runtime 2.0. JavaScript Per ulteriori informazioni, consulta, Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront.

Argomenti

- Gruppi di connessioni
- Tenant di distribuzione

Gruppi di connessioni

Il gruppo di connessioni associato ai tenant di distribuzione dispone di un nome di dominio.

Per ottenere questo valore, utilizza il campo `endpoint` dell'oggetto secondario `context` dell'oggetto evento.

Richiesta

```
const value = event.context.endpoint;
```

Risposta

La risposta è una `string` che contiene il nome di dominio del gruppo di connessioni, ad esempio d111111abcdef8.cloudfront.net. Il campo `endpoint` viene visualizzato solo quando la funzione viene invocata per una distribuzione multi-tenant con un gruppo di connessioni associato. Per ulteriori informazioni, consulta Oggetto Context.

Tenant di distribuzione

CloudFront Functions dispone di un modulo che fornisce l'accesso a valori specifici del tenant di distribuzione.

Per utilizzare questo modulo, includi la seguente istruzione nella prima riga del codice funzione:

```
import cf from 'cloudfront';
```

Puoi utilizzare i seguenti esempi solo nella funzione `handler`, direttamente o tramite qualsiasi funzione di chiamata nidificata.

Campo **`distributionTenant.id`**

Utilizza questo campo per ottenere il valore dell'ID del tenant di distribuzione.

Richiesta

```
const value = cf.distributionTenant.id;
```

Risposta

La risposta è una `string` che contiene l'ID del tenant di distribuzione, ad esempio `dt_1a2b3c4d5e6f7`.

Gestione errori

Se la funzione viene invocata per una distribuzione standard, specificando il campo `distributionTenant.id` verrà restituito l'errore di tipo `distributionTenant module is not available`. Per gestire questo caso d'uso, puoi aggiungere un blocco `catch` e `try` al codice.

Metodo **`distributionTenant.parameters.get()`**

Utilizza questo metodo per restituire il valore dei nomi dei parametri tenant di distribuzione specificati.

```
distributionTenant.parameters.get("key");
```

`key`: il nome del parametro tenant di distribuzione di cui desideri recuperare il valore.

Richiesta

```
const value = distributionTenant.parameters.get("key");
```

Risposta

La risposta è una `string` che contiene il valore per il parametro tenant di distribuzione. Ad esempio, se il nome della chiave è `TenantPath`, il valore di questo parametro potrebbe essere `tenant1`.

Gestione errori

Potrebbero verificarsi i seguenti errori:

- Se la funzione viene invocata per una distribuzione standard, il metodo `distributionTenant.parameters.get()` restituirà l'errore di tipo `distributionTenant module is not available`.
- L'errore `DistributionTenantParameterKeyNotFound` viene restituito quando il parametro tenant di distribuzione specificato non esiste.

Per gestire questi casi d'uso, puoi aggiungere un blocco `try` e `catch` al codice.

Uso di async e await

CloudFront Le funzioni JavaScript di runtime di Functions 2.0 forniscono una `async await` sintassi per gestire `Promise` gli oggetti. Le promesse rappresentano risultati con ritardo a cui è possibile accedere tramite la parola chiave `await` nelle funzioni contrassegnate come `async`. Diverse nuove WebCrypto funzioni utilizzano Promises.

Per ulteriori informazioni sugli oggetti `Promise`, consulta Promessa.

> **Note**
>
> È necessario utilizzare JavaScript runtime 2.0 per i seguenti esempi di codice.

`await` può essere utilizzato solo all'interno delle funzioni `async`. Argomenti e chiusure `async` non sono supportati.

```
async function answer() {
    return 42;
}

// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.

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;
}
```

Il JavaScript codice di esempio seguente mostra come visualizzare le promesse con il metodo `then` chain. È possibile utilizzare `catch` per visualizzare gli errori.

Warning

L'uso dei combinatori di promesse (ad esempio, `Promise.all`, `Promise.any`) e dei metodi di catena di promesse (ad esempio, `then` e `catch`) può richiedere un elevato utilizzo della memoria delle funzioni. Se la funzione supera la quota massima di memoria delle funzioni, non verrà eseguita. Per evitare questo errore, ti consigliamo di utilizzare la sintassi `await` anziché i metodi `promise`.

```
async function answer() {
    return 42;
}

async function squared_answer() {
   return answer().then(value => value * value)
}
// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.
```

```
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;
}
```

Supporto CWT per le funzioni CloudFront

Questa sezione fornisce dettagli sul supporto per i token Web CBOR (CWT) nelle CloudFront funzioni, che consente l'autenticazione e l'autorizzazione sicure basate su token presso le edge location. CloudFront Questo supporto viene fornito come modulo, accessibile nella funzione. CloudFront

Per utilizzare questo modulo, create una CloudFront funzione utilizzando JavaScript runtime 2.0 e includete la seguente istruzione nella prima riga del codice della funzione:

```
import cf from 'cloudfront';
```

I metodi associati a questo modulo sono accessibili tramite (dove* è un jolly che rappresenta le diverse funzioni presenti nel modulo):

```
cf.cwt.*
```

Per ulteriori informazioni, consulta Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront.

Attualmente, il modulo supporta solo la struttura MAC0 con algoritmo HS256 (HMAC-SHA256) con un limite di 1 KB per la dimensione massima del token.

Struttura dei token

Questa sezione illustra la struttura dei token prevista dal modulo CWT. Il modulo si aspetta che il token sia etichettato e identificabile correttamente (ad esempio COSE MAC0). Inoltre, per quanto riguarda la struttura del token, il modulo segue gli standard stabiliti da CBOR Object Signing and Encryption (COSE) [RFC 8152].

```
( // CWT Tag (Tag value: 61) --- optional
    ( // COSE MAC0 Structure Tag (Tag value: 17) --- required
        [
            protectedHeaders,
```

```
            unprotectedHeaders,
            payload,
            tag,
        ]
    )
)
```

Example : CWT utilizza la struttura COSE MAC0

```
61( // CWT tag
    17( // COSE_MAC0 tag
        [
            { // Protected Headers
                1: 4  // algorithm : HMAC-256-64
            },
            { // Unprotected Headers
                4: h'53796d6d6574726963323536' // kid : Symmetric key id
            },
            { // Payload
                1: "https://iss.example.com", // iss
                2: "exampleUser", // sub
                3: "https://aud.example.com", // aud
                4: 1444064944, // exp
                5: 1443944944, // nbf
                6: 1443944944, // iat
            },
            h'093101ef6d789200' // tag
        ]
    )
)
```

> **Note**
>
> Il tag CWT è opzionale per la generazione di token. Tuttavia, il tag di struttura COSE è obbligatorio.

metodo validateToken ()

La funzione decodifica e convalida un token CWT utilizzando la chiave specificata. Se la convalida ha esito positivo, restituisce il token CWT decodificato. Altrimenti, genera un errore. Tieni presente che questa funzione non esegue alcuna convalida sul set di attestazioni.

Richiesta

```
cf.cwt.validateToken(token, handlerContext{key})
```

Parameters

token (richiesto)

Token codificato per la convalida. Questo deve essere un JavaScript buffer.

HandlerContext (obbligatorio)

Un JavaScript oggetto che memorizza il contesto per la chiamata validateToken. Al momento, è supportata solo la proprietà key.

chiave (obbligatoria)

Chiave segreta per il calcolo del message digest. Può essere fornita come stringa o JavaScript buffer.

Risposta

Quando il `validateToken()` metodo restituisce un token convalidato correttamente, la risposta della funzione è a `CWTObject` nel seguente formato. Una volta decodificate, tutte le chiavi di rivendicazione vengono rappresentate come stringhe.

```
CWTObject {
    protectedHeaders,
    unprotectedHeaders,
    payload
}
```

Esempio: convalida il token con kid inviato come parte del token

Questo esempio dimostra la convalida del token CWT, in cui il kid viene estratto dall'header. Il bambino viene quindi passato KeyValueStore a CloudFront Functions per recuperare la chiave segreta usata per convalidare il token.

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
```

```
   exp: 4
}

async function handler(event) {
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;

        // Retrieve the secret key from the kvs
        let secretKey = await cf.kvs().get(kid);

        // Now you can use the secretKey to decode & validate the token.
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtObj = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtObj[CwtClaims.exp] && cwtObj[CwtClaims.exp] < currentTime) {
                return {
                    statusCode: 401,
                    statusDescription: 'Token expired'
                };
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
```

```
}
```

metodo generateToken ()

Questa funzione genera un nuovo token CWT utilizzando il payload e le impostazioni di contesto fornite.

Richiesta

```
cf.cwt.generateToken(generatorContext, payload)
```

Parameters

GeneratorContext (obbligatorio)

Si tratta di un JavaScript oggetto che viene utilizzato come contesto per la generazione del token e contiene le seguenti coppie chiave-valore:

CwtTag (opzionale)

Questo valore è un booleano, che se lo `true` specifica deve essere aggiunto. `cwtTag`

CoseTag (obbligatorio)

Specifica il tipo di tag COSE. Attualmente supporta `MAC0` solo.

chiave (richiesta)

Chiave segreta per calcolare il message digest. Questo valore può essere una stringa o. JavaScript `Buffer`

payload (obbligatorio)

Payload di token per la codifica. Il payload deve essere in formato. `CWTObject`

Risposta

Restituisce un JavaScript Buffer contenente il token codificato.

Example : genera un token CWT

```
import cf from 'cloudfront';

const CwtClaims = {
    iss: 1,
```

```
    sub: 2,
    exp: 4
};

const CatClaims = {
    catu: 401,
    catnip: 402,
    catm: 403,
    catr: 404
};

const Catu = {
    host: 1,
    path: 2,
    ext: 3
};

const CatuMatchTypes = {
    prefix_match: 1,
    suffix_match: 2,
    exact_match: 3
};

const Catr = {
    renewal_method: 1,
    next_renewal_time: 2,
    max_uses: 3
};

async function handler(event) {
    try {
        const response = {
            statusCode: 200,
            statusDescription: 'OK',
            headers: {}
        };

        const commonAccessToken = {
            protected: {
                1: "5",
            },
            unprotected: {},
            payload: {
                [CwtClaims.iss]: "cloudfront-documentation",
```

```
            [CwtClaims.sub]: "cwt-support-on-cloudfront-functions",
            [CwtClaims.exp]: 1740000000,
            [CatClaims.catu]: {
                [Catu.host]: {
                    [CatuMatchTypes.suffix_match]: ".cloudfront.net"
                },
                [Catu.path]: {
                    [CatuMatchTypes.prefix_match]: "/media/live-stream/cf-4k/"
                },
                [Catu.ext]: {
                    [CatuMatchTypes.exact_match]: [
                        ".m3u8",
                        ".ts",
                        ".mpd"
                    ]
                }
            },
            [CatClaims.catnip]: [
                "[IP_ADDRESS]",
                "[IP_ADDRESS]"
            ],
            [CatClaims.catm]: [
                "GET",
                "HEAD"
            ],
            [CatClaims.catr]: {
                [Catr.renewal_method]: "header_renewal",
                [Catr.next_renewal_time]: 1750000000,
                [Catr.max_uses]: 5
            }
        }
    };

    if (!request.headers['x-cwt-kid']) {
        throw new Error('Missing x-cwt-kid header');
    }

    const kid = request.headers['x-cwt-kid'].value;
    const secretKey = await cf.kvs().get(kid);

    if (!secretKey) {
        throw new Error('Secret key not found for provided kid');
    }
```

```
        try {
            const genContext = {
                cwtTag: true,
                coseTag: "MAC0",
                key: secretKey
            };

            const tokenBuffer = cf.cwt.generateToken(commonAccessToken, genContext);
            response.headers['x-generated-cwt-token'] = { value:
 tokenBuffer.toString('base64url') };

            return response;
        } catch (tokenError) {
            return {
                statusCode: 401,
                statusDescription: 'Could not generate the token'
            };
        }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
    }
}
```

Example : Aggiorna il token in base a una logica

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
   exp: 4
}

async function handler(event) {
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;
        let secretKey = await cf.kvs().get(kid); // Retrieve the secret key from the
 kvs
```

```
        // Now you can use the secretKey to decode & validate the token.
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtJSON = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtJSON[CwtClaims.exp] && cwtJSON[CwtClaims.exp] < currentTime) {
                // We can regnerate the token and add 8 hours to the expiry time
                cwtJSON[CwtClaims.exp] = Math.floor(Date.now() / 1000) + (8 * 60 * 60);

                let genContext = {
                  coseTag: "MAC0",
                  key: secretKey
                }

                let newTokenBuffer = cf.cwt.generateToken(cwtJSON, genContext);
                 request.headers['x-cwt-regenerated-token'] =
 newTokenBuffer.toString('base64url');
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    }
    catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
}
```

Metodi generali di supporto

Questa pagina fornisce metodi di supporto aggiuntivi all'interno CloudFront di Functions. Per utilizzare questi metodi, create una CloudFront funzione utilizzando JavaScript runtime 2.0.

```
import cf from 'cloudfront';
```

Per ulteriori informazioni, consulta Funzionalità di runtime JavaScript 2.0 per Funzioni CloudFront.

`edgeLocation`metadati

Questo metodo richiede l'utilizzo del `cloudfront` modulo.

> **Note**
>
> È possibile utilizzare questo metodo solo per le funzioni di richiesta del visualizzatore. Per le funzioni di risposta del visualizzatore, questo metodo è vuoto.

Utilizzate questo JavaScript oggetto per ottenere il codice dell'aeroporto della edge location, la regione Regional Edge Cache prevista o l'indirizzo IP del CloudFront server utilizzato per gestire la richiesta. Questi metadati sono disponibili solo nel trigger dell'evento di richiesta del visualizzatore.

```
cf.edgeLocation = {
    name: SEA
    serverIp: 1.2.3.4
    region: us-west-2
}
```

L'`cf.edgeLocation`oggetto può contenere quanto segue:

nome

Il codice IATA a tre lettere dell'edge location che ha gestito la richiesta.

IP del server

L' IPv6 indirizzo IPv4 o del server che ha gestito la richiesta.

region

La CloudFront Regional Edge Cache (REC) che la richiesta dovrebbe utilizzare in caso di perdita della cache. Questo valore non viene aggiornato nel caso in cui il REC previsto non sia disponibile

e per la richiesta venga utilizzato un REC di backup. Questo non include la posizione Origin Shield utilizzata, tranne nei casi in cui il REC principale e l'Origin Shield si trovino nella stessa posizione.

> **Note**
>
> CloudFront Functions non viene richiamato una seconda volta quando CloudFront è configurato per utilizzare il failover di origine. Per ulteriori informazioni, consulta Ottimizzazione dell'elevata disponibilità con il failover di origine CloudFront.

Metodo **`rawQueryString()`**

Questo metodo non richiede il `cloudFront` modulo.

Utilizzate il `rawQueryString()` metodo per recuperare la stringa di query non analizzata e inalterata come stringa.

Richiesta

```
function handler(event) {
    var request = event.request;
    const qs = request.rawQueryString();
}
```

Risposta

Restituisce la stringa di query completa della richiesta in entrata come valore di stringa senza l'iniziale. ?

- Se non è presente una stringa di query, ma ? è presente, le funzioni restituiscono una stringa vuota.
- Se non è presente una stringa di query e ? non è presente, la funzione restituisce`undefined`.

Caso 1: restituita la stringa di query completa (senza interlinea**?**)

URL della richiesta in entrata: `https://example.com/page?name=John&age=25&city=Boston`

`rawQueryString()`restituisce: `"name=John&age=25&city=Boston"`

Caso 2: restituita una stringa vuota (quando **?** è presente ma senza parametri)

URL della richiesta in entrata: `https://example.com/page?`

`rawQueryString()`restituisce: `""`

Caso 3: **`undefined`** restituito (nessuna stringa di query e no**?**)

URL della richiesta in entrata: `https://example.com/page`

`rawQueryString()`restituisce: `undefined`

Creazione di funzioni

La creazione di una funzione avviene in due fasi:

1. Crea il codice della funzione come JavaScript. Puoi utilizzare l'esempio predefinito della console CloudFront o scriverne uno personalizzato. Per ulteriori informazioni, consulta i seguenti argomenti:
   - Scrittura del codice della funzione
   - the section called "Struttura degli eventi"
   - CloudFront Esempi di funzioni per CloudFront
2. Utilizza CloudFront per creare la funzione e includere il codice. Il codice è presente all'interno della funzione (non come riferimento).

Console

Per creare una funzione

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegli Crea funzione.
3. Immetti un nome di funzione univoco all'interno dell'Account AWS, scegli la versione di JavaScript e infine seleziona Continua. Viene visualizzata la pagina dei dettagli relativa alla nuova funzione.

> **Note**
>
> Per utilizzare coppie chiave-valore nella funzione, è necessario scegliere JavaScript runtime 2.0.

4. Nella sezione Codice funzione, scegli la scheda Compila e immetti il codice funzione. Il codice di esempio incluso nella scheda Compila illustra la sintassi di base del codice funzione.
5. Scegli Save changes (Salva modifiche).
6. Se il codice funzione utilizza coppie chiave-valore, è necessario associare un archivio di valori delle chiavi.

   Puoi associare l'archivio di valori delle chiavi al momento della creazione della funzione. In alternativa, puoi associarlo in un secondo momento aggiornando la funzione.

   Per associare subito un archivio di valori delle chiavi, procedi come segue:

   - Nella sezione Associa KeyValueStore, scegli Associa KeyValueStore esistente.
   - Seleziona l'archivio di valori delle chiavi contenente le coppie chiave-valore nella funzione, quindi scegli Associata KeyValueStore.

   CloudFront associa immediatamente l'archivio alla funzione. Non è necessario salvare la funzione.

CLI

Con la CLI, in genere si crea prima il codice funzione in un file e poi si crea la funzione con AWS CLI.

Per creare una funzione

1. Crea il codice funzione in un file e memorizzalo in una directory a cui il computer può connettersi.
2. Esegui il comando come mostrato nell'esempio. Questo esempio utilizza la notazione `fileb://` per passare il file. Include anche interruzioni di riga per rendere il comando più leggibile.

```
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
```

> **Note**
>
> - `Runtime`: la versione di JavaScript. Per utilizzare coppie chiave-valore nella funzione, è necessario specificare la versione 2.0.
> - `KeyValueStoreAssociations`: se la funzione utilizza coppie chiave-valore, puoi associare l'archivio dei valori delle chiavi al momento della creazione della funzione. In alternativa, puoi associarlo in un secondo momento utilizzando `update-function`. Il valore `Quantity` è sempre 1 perché a ogni funzione può essere associato un solo archivio di valori delle chiavi.

Se il comando viene eseguito correttamente, vedrai un output simile al seguente.

```
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 maggior parte delle informazioni viene ripetuta dalla richiesta. Altre informazioni vengono aggiunte da CloudFront.

> **Note**
>
> - `ETag`: questo valore cambia a ogni modifica dell'archivio di valori delle chiavi. Utilizza questo valore e il nome della funzione per fare riferimento alla funzione in futuro. Assicurati di utilizzare sempre l'`ETag` corrente.
> - `FunctionARN`: l'ARN per la funzione CloudFront.
> - 111122223333: l'Account AWS.
> - `Stage`: la fase della funzione (`LIVE` o `DEVELOPMENT`).
> - `Status`: lo stato della funzione (`PUBLISHED` o `UNPUBLISHED`).

Dopo aver creato la funzione, viene aggiunta alla fase `DEVELOPMENT`. Ti consigliamo di provare la funzione prima di pubblicarla. Dopo aver pubblicato la funzione, questa passa alla fase `LIVE`.

Test delle funzioni

Prima di distribuire la funzione nella fase live (produzione), puoi testarla per verificare che funzioni come previsto. Per testare una funzione, specifica un oggetto evento che rappresenta una richiesta HTTP o una risposta che la distribuzione CloudFront potrebbe ricevere in produzione.

CloudFront Functions esegue quanto riportato di seguito:

1. Esegue la funzione, utilizzando l'oggetto evento fornito come input.
2. Restituisce il risultato della funzione (l'oggetto evento modificato) insieme a tutti i registri delle funzioni o messaggi di errore e l'utilizzo del calcolo della funzione. Per ulteriori informazioni sull'utilizzo delle capacità di calcolo, consultare the section called "Informazioni sull'utilizzo del calcolo".

> **Note**
>
> Quando si esegue il test di una funzione, CloudFront verifica solo gli errori di esecuzione della funzione. CloudFront non verifica se la richiesta verrà elaborata correttamente una volta pubblicata. Ad esempio, se la funzione elimina un'intestazione obbligatoria, il test avrà esito

positivo perché non vi è alcun problema con il codice. Tuttavia, se pubblichi la funzione e la associ a una distribuzione, la funzione non funzionerà quando viene effettuata una richiesta tramite CloudFront.

Indice

Impostazione dell'oggetto evento

Prima di testare una funzione, è necessario impostare l'oggetto evento per testarlo. Sono disponibili diverse opzioni.

Opzione 1: impostazione di un oggetto evento senza salvarlo

Puoi impostare un oggetto evento nell'editor visivo della console CloudFront senza salvarlo.

Puoi utilizzare questo oggetto evento per testare la funzione dalla console CloudFront, anche se non è stato salvato.

Opzione 2: creazione di un oggetto evento nell'editor visuale

Puoi impostare un oggetto evento nell'editor visivo della console CloudFront senza salvarlo. È possibile creare 10 oggetti evento per ogni funzione, ad esempio per testare diversi input possibili.

L'oggetto evento creato in questo modo può essere utilizzato per testare la funzione nella console CloudFront. Non è possibile utilizzarlo per testare la funzione tramite un'API o un SDK AWS.

Opzione 3: creazione di un oggetto evento utilizzando un editor di testo

Puoi utilizzare un editor di testo per creare un oggetto evento in formato JSON. Per informazioni sulla struttura di un oggetto evento, consulta Struttura degli eventi.

Puoi utilizzare l'oggetto evento per testare la funzione utilizzando la CLI. Tuttavia, non puoi utilizzarlo per testare la funzione nella console CloudFront.

Come creare un oggetto evento (opzione 1 o 2)

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.

   Scegli la funzione che desideri testare.
2. Nella pagina dei dettagli della funzione, seleziona la scheda Test.
3. Per Tipo di evento, scegli una delle seguenti opzioni:

   - Se la funzione modifica una richiesta HTTP o genera una risposta in base alla richiesta, scegli Richiesta visualizzatore. Viene visualizzata la sezione Richiesta.
   - Scegli Risposta visualizzatore. Vengono visualizzate le sezioni Richiesta e Risposta.
4. Completa tutti i campi da includere nell'evento. Puoi scegliere Modifica JSON per visualizzare il JSON non elaborato.
5. (Facoltativo) Per salvare l'evento, scegli Salva e nel campo Salva evento di test, inserisci un nome, quindi scegli Salva.

   Puoi anche scegliere Modifica JSON per copiare il codice JSON non elaborato e salvarlo nel tuo file, all'esterno di CloudFront.

Come creare un oggetto evento (opzione 3)

Crea l'oggetto evento utilizzando un editor di testo. Archivia il file in una directory a cui il tuo computer può connettersi.

Verifica di aver seguito queste linee guida:

- Ometti i campi `distributionDomainName`, `distributionId` e `requestId`.
- I nomi delle intestazioni, dei cookie e delle stringhe di query devono essere in minuscolo.

Per creare un oggetto evento in questo modo è possibile creare un esempio utilizzando l'editor visuale. Hai così la certezza che l'esempio sia formattato correttamente. Puoi copiare il codice JSON non elaborato, incollarlo in un editor di testo e salvare il file.

Per ulteriori informazioni sulla struttura di un evento, consulta Struttura degli eventi.

Test della funzione

Puoi testare una funzione nella console CloudFront o con AWS Command Line Interface (AWS CLI).

Console

Per testare la funzione

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegli la funzione che desideri testare.
3. Seleziona la scheda Test.
4. Assicurati che venga visualizzato l'evento corretto. Per passare dall'evento attualmente visualizzato a un altro, scegli un altro evento nel campo Seleziona evento di test.
5. Scegli Testa la funzione. La console mostra l'output della funzione, inclusi i log delle funzioni e l'utilizzo del calcolo.

CLI

Puoi testare una funzione utilizzando il comando aws cloudfront test-function.

Per testare la funzione

1. Aprire una finestra a riga di comando.
2. Esegui il comando seguente dalla stessa directory che contiene il file specificato.

   Questo esempio utilizza la notazione `fileb://` per passare il file dell'evento oggetto. Include anche interruzioni di riga per rendere il comando più leggibile.

```
aws cloudfront test-function \
    --name MaxAge \
    --if-match ETVABCEXAMPLE \
    --event-object fileb://event-maxage-test01.json \
    --stage DEVELOPMENT
```

> **Note**
>
> - Fai riferimento alla funzione tramite i rispettivi nomi e ETag (nel parametro `if-match`). Fai riferimento all'oggetto evento in base alla sua posizione nel file system.
> - La fase può essere `DEVELOPMENT` o `LIVE`.

Se il comando viene eseguito correttamente, vedrai un output simile al seguente.

```
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
```

> **Note**
>
> - `FunctionExecutionLogs` contiene un elenco di righe di log che la funzione ha scritto nelle istruzioni `console.log()` (se presenti).

- `ComputeUtilization` contiene informazioni sull'esecuzione della funzione. Per informazioni, consulta the section called "Informazioni sull'utilizzo del calcolo".
- `FunctionOutput` contiene l'oggetto evento restituito dalla funzione.

Informazioni sull'utilizzo del calcolo

Compute utilization (Utilizzo del calcolo) è la quantità di tempo impiegata per l'esecuzione della funzione come percentuale del tempo massimo consentito. Ad esempio, un valore pari a 35 significa che la funzione è stata completata nel 35% del tempo massimo consentito.

Se una funzione supera continuamente il tempo massimo consentito, CloudFront limita la funzione. L'elenco seguente illustra la probabilità che una funzione venga limitata in base al valore di utilizzo del calcolo.

Valore di utilizzo del calcolo:

- 1 – 50 – Da 1 a 50: la funzione è comodamente al di sotto del tempo massimo consentito e dovrebbe funzionare senza limitazione (della larghezza di banda della rete).
- 51 – 70 – Da 51 a 70: la funzione si sta avvicinando al tempo massimo consentito. Prendere in considerazione l'ottimizzazione del codice della funzione.
- 71 – 100 – Da 71 a 100: la funzione è molto vicina o supera il tempo massimo consentito. È probabile che CloudFront limiti questa funzione se la si associa a una distribuzione.

Aggiornamento delle funzioni

Puoi aggiornare una funzione in qualsiasi momento. Le modifiche vengono apportate solo alla versione della funzione che si trova nella fase `DEVELOPMENT`. Per copiare gli aggiornamenti dalla fase `DEVELOPMENT` in `LIVE`, devi pubblicare la funzione.

Puoi aggiornare il codice di una funzione nella console CloudFront o tramite AWS Command Line Interface (AWS CLI).

Console

Come aggiornare il codice della funzione

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.

Scegliere la funzione da aggiornare.

2. Scegli Modifica e apporta le modifiche seguenti:

   - Aggiorna gli eventuali campi nella sezione Dettagli.
   - Modifica o rimuovi l'archivio di valori delle chiavi associato. Per ulteriori informazioni sugli archivi di valori delle chiavi, consulta the section called " KeyValueStore di CloudFront".
   - Modifica il codice funzione. Scegli la scheda Compila, apporta le modifiche, quindi seleziona Salva modifiche per salvare le modifiche al codice.

CLI

Per aggiornare il codice della funzione

1. Aprire una finestra a riga di comando.
2. Esegui il comando seguente.

   Questo esempio utilizza la notazione `fileb://` per passare il file. Include anche interruzioni di riga per rendere il comando più leggibile.

```
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
```

> **Note**
>
> - Puoi identificare la funzione tramite i rispettivi nomi ed ETag (nel parametro `if-match`). Assicurati di utilizzare l'ETag corrente. Puoi ottenere questo valore dall'operazione API DescribeFunction.

- È necessario includere `function-code`, anche se non intendi apportarvi modifiche.
- Fai attenzione con `function-config`. Devi passare tutto ciò che vuoi mantenere nella configurazione. In particolare, gestisci l'archivio di valori delle chiavi come segue:
  - Per mantenere l'associazione esistente con l'archivio di valori delle chiavi (se presente), specifica il nome dell'archivio esistente.
  - Per modificare l'associazione, specifica il nome del nuovo archivio di valori delle chiavi.
  - Per rimuovere l'associazione, ometti il parametro `KeyValueStoreAssociations`.

Se il comando viene eseguito correttamente, vedrai un output simile al seguente.

```
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 maggior parte delle informazioni viene ripetuta dalla richiesta. Altre informazioni vengono aggiunte da CloudFront.

Note

- `ETag`: questo valore cambia a ogni modifica dell'archivio di valori delle chiavi.
- `FunctionARN`: l'ARN per la funzione CloudFront.
- `Stage`: la fase della funzione (`LIVE` o `DEVELOPMENT`).
- `Status`: lo stato della funzione (`PUBLISHED` o `UNPUBLISHED`).

Pubblicazione di funzioni

Quando pubblichi la funzione, questa operazione copia la funzione dalla fase `DEVELOPMENT` alla fase `LIVE`.

Se alla funzione non sono associati comportamenti cache, la sua pubblicazione consente di associarla a un comportamento cache. Puoi associare i comportamenti della cache solo alle funzioni che si trovano nella fase `LIVE`.

Important

- Prima di pubblicare, ti consigliamo di provare la funzione.
- Dopo aver pubblicato la funzione, tutti i comportamenti cache associati a tale funzione iniziano automaticamente a utilizzare la copia appena pubblicata, non appena le distribuzioni completano l'implementazione.

Puoi pubblicare una funzione nella console CloudFront o con l'AWS CLI.

Console

Come pubblicare una funzione

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegliere la funzione da aggiornare.
3. Scegli la scheda Pubblica, quindi seleziona Pubblica. Se la funzione è già collegata a uno o più comportamenti cache, scegli Pubblica e aggiorna.

4. (Facoltativo) Per visualizzare le distribuzioni associate alla funzione, seleziona Distribuzioni CloudFront associate per espandere tale sezione.

In caso di esito positivo, nella parte superiore della pagina viene visualizzato un banner che indica il ***nome della funzione*** pubblicata correttamente. Puoi anche scegliere la scheda Genera e quindi Live per visualizzare la versione live del codice funzione.

CLI

Come pubblicare una funzione

1. Aprire una finestra a riga di comando.
2. Eseguire il seguente comando aws cloudfront publish-function. Nell'esempio vengono fornite interruzioni di riga per rendere l'esempio più leggibile.

```
aws cloudfront publish-function \
    --name MaxAge \
    --if-match ETVXYZEXAMPLE
```

Se il comando viene eseguito correttamente, vedrai un output simile al seguente.

```
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
```

Associazione delle funzioni alle distribuzioni

Per utilizzare una funzione con una distribuzione, è necessario associare la funzione a uno o più comportamenti cache nella distribuzione. Puoi associare una funzione a più comportamenti della cache in più distribuzioni.

Puoi associare una funzione con uno qualsiasi di questi elementi:

- Un comportamento cache esistente
- Un nuovo comportamento cache in una distribuzione esistente
- Un nuovo comportamento cache in una nuova distribuzione

Quando associ una funzione a un comportamento di cache, è necessario scegliere un tipo di evento. Il tipo di evento determina quando CloudFront esegue la funzione.

Puoi scegliere i seguenti tipi di evento:

- Richiesta visualizzatore: la funzione viene eseguita quando CloudFront riceve una richiesta da un visualizzatore.
- Risposta visualizzatore: la funzione viene eseguita prima che CloudFront restituisca una risposta al visualizzatore.

Non puoi utilizzare tipi di eventi rivolti all'origine (richiesta origine e risposta origine) con Funzioni CloudFront. Puoi invece usare Lambda@Edge. Per ulteriori informazioni, consulta CloudFront eventi che possono attivare una funzione Lambda @Edge.

> **Note**
>
> Prima di associare una funzione, è necessario pubblicarla nella fase `LIVE`.

Puoi associare una funzione a una distribuzione nella console CloudFront o tramite AWS Command Line Interface (AWS CLI). Nella procedura seguente viene illustrato come associare una funzione a un comportamento della cache esistente.

Console

Come associare una funzione a un comportamento cache esistente

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegli la funzione che desideri associare.
3. Nella pagina Funzioni, seleziona la scheda Pubblica.

4. Scegli Funzione Pubblica.
5. Scegliere Add Association (Aggiungi associazione). Nella finestra di dialogo che viene visualizzata, scegli una distribuzione, un tipo di evento e/o un comportamento cache.

   Per il tipo di evento, scegli quando eseguire questa funzione:

   - Richiesta visualizzatore: esegui la funzione ogni volta che CloudFront riceve una richiesta.
   - Risposta visualizzatore: esegui la funzione ogni volta che CloudFront restituisce una risposta.
6. Per salvare la configurazione, scegli Aggiungi associazione.

CloudFront associa la distribuzione alla funzione. Attendere alcuni minuti affinché la distribuzione associata finisca la distribuzione. Per controllare l'avanzamento, puoi scegliere Visualizza distribuzione nella pagina dei dettagli della funzione.

CLI

Come associare una funzione a un comportamento cache esistente

1. Aprire una finestra a riga di comando.
2. Inserisci il comando seguente per salvare la configurazione di distribuzione per la distribuzione di cui desideri associare il comportamento cache a una funzione. Questo comando salva la configurazione di distribuzione in un file denominato `dist-config.yaml`. Per utilizzare questo comando, effettua le seguenti operazioni:

   - Sostituisci *`DistributionID`* con l'ID della distribuzione.
   - Esegui il comando su una riga. Nell'esempio vengono fornite interruzioni di riga per rendere l'esempio più leggibile.

   ```
   aws cloudfront get-distribution-config \
       --id DistributionID \
       --output yaml > dist-config.yaml
   ```

   Se il comando viene eseguito correttamente, l'AWS CLI non restituisce alcun output.
3. Apri il file denominato `dist-config.yaml` creato. Modifica il file per apportare le modifiche seguenti.

a. Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

b. Nel comportamento della cache, trova l'oggetto denominato `FunctionAssociations`. Aggiorna questo oggetto per aggiungere un'associazione di funzioni. La sintassi YAML per un'associazione di funzioni è simile all'esempio seguente.

- L'esempio seguente mostra un oggetto evento Richiesta visualizzatore (trigger). Per utilizzare un tipo di evento Risposta del visualizzatore, sostituisci `viewer-request` con `viewer-response`.
- Sostituisci *`arn:aws:cloudfront::111122223333:function/ExampleFunction`* con il nome della risorsa Amazon (ARN) della funzione che stai associando a questo comportamento della cache. Per ottenere l'ARN della funzione, puoi utilizzare il comando aws cloudfront list-functions.

```
FunctionAssociations:
  Items:
    - EventType: viewer-request
      FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
  Quantity: 1
```

c. Dopo aver apportato queste modifiche, salva il file.

4. Utilizza il comando seguente per aggiornare la distribuzione, aggiungendo l'associazione di funzioni. Per utilizzare questo comando, effettua le seguenti operazioni:

- Sostituisci *`DistributionID`* con l'ID della distribuzione.
- Esegui il comando su una riga. Nell'esempio vengono fornite interruzioni di riga per rendere l'esempio più leggibile.

```
aws cloudfront update-distribution \
    --id DistributionID \
    --cli-input-yaml file://dist-config.yaml
```

Se il comando ha esito positivo, viene visualizzato un output simile al seguente che descrive la distribuzione appena aggiornata con l'associazione di funzioni. L'output di esempio seguente è stato troncato per una maggiore leggibilità.

```
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
```

Lo `Status` della distribuzione cambia in `InProgress` mentre la distribuzione viene ridistribuita. Quando la nuova configurazione di distribuzione raggiunge una posizione edge CloudFront, tale posizione edge inizia a utilizzare la funzione associata. Quando la distribuzione è completamente distribuita, `Status` torna a `Deployed`. Ciò indica che la funzione CloudFront associata è attiva in tutte le posizioni edge CloudFront in tutto il mondo. In genere sono necessari pochi minuti.

Amazon CloudFront KeyValueStore

KeyValueStore di CloudFront è un datastore di valori delle chiavi sicuro, globale e a bassa latenza che consente l'accesso in lettura dall'interno di Funzioni CloudFront, abilitando una logica personalizzabile avanzata nelle posizioni edge di CloudFront.

Con KeyValueStore di CloudFront, puoi aggiornare il codice della funzione e i dati associati a una funzione indipendentemente l'uno dall'altro. Questa separazione semplifica il codice della funzione e agevola l'aggiornamento dei dati senza la necessità di implementare modifiche al codice.

> **Note**
>
> Per utilizzare KeyValueStore di CloudFront, la funzione CloudFront deve utilizzare JavaScript runtime 2.0.

Di seguito è riportata la procedura generale per l'utilizzo delle coppie chiave-valore:

- Crea archivi di valori delle chiavi e compilali con un set di coppie chiave-valore. Puoi aggiungere archivi di valori delle chiavi a un bucket Amazon S3 o inserirli manualmente.
- Associa gli archivi di valori delle chiavi alla funzione CloudFront.
- All'interno del codice della funzione, utilizza il nome della chiave per recuperare il valore associato alla chiave stessa o stabilire se ne esiste una. Per ulteriori informazioni sull'utilizzo delle coppie chiave-valore nel codice della funzione e per informazioni sui metodi dell'assistente di gestione, consulta the section called "Metodi helper per archivi di valori delle chiavi".

Casi d'uso

Puoi utilizzare coppie chiave-valore per i seguenti esempi:

- Riscritture o reindirizzamenti degli URL: la coppia chiave-valore può contenere gli URL riscritti o gli URL di reindirizzamento.
- Flag di funzionalità e test A/B: puoi creare una funzione per eseguire esperimenti assegnando una percentuale di traffico a una versione specifica del sito web.
- Autorizzazione di accesso: puoi implementare il controllo degli accessi per consentire o rifiutare richieste in base ai criteri definiti e ai dati archiviati in un archivio di valori delle chiavi.

Formati supportati per i valori

Puoi archiviare il valore in una coppia chiave-valore in uno qualsiasi dei seguenti formati:

- Stringa
- Stringa con codifica in byte
- JSON

Sicurezza

La funzione CloudFront e tutti i dati degli archivi di valori delle chiavi vengono gestiti in modo sicuro, come descritto di seguito:

- CloudFront esegue la crittografia di ogni archivio di valori delle chiavi a riposo e in transito (durante la lettura o la scrittura negli archivi di valori delle chiavi) quando si chiamano le operazioni API di KeyValueStore di CloudFront.

- Quando si esegue la funzione, CloudFront procede con la decrittografia di ogni coppia chiave-valore in memoria nelle posizioni edge di CloudFront.

Per iniziare a utilizzare KeyValueStore di CloudFront, consulta gli argomenti seguenti.

Argomenti

- Utilizzo dell'archivio di valori delle chiavi
- Utilizzo dei dati dei valori delle chiavi

- Per ulteriori informazioni su come iniziare a usare KeyValueStore di CloudFront, consulta il post del blog AWS Introducing Amazon CloudFront KeyValueStore.

Utilizzo dell'archivio di valori delle chiavi

È necessario creare un archivio di valori delle chiavi per contenere le coppie chiave-valore da utilizzare in Funzioni CloudFront.

Dopo aver creato gli archivi di valori delle chiavi e aggiunto le coppie chiave-valore, puoi utilizzare i valori delle chiavi nel codice della funzione CloudFront.

Per iniziare, consulta i seguenti argomenti:

Argomenti

- Creazione di un archivio di valori delle chiavi
- Associazione di un archivio di valori delle chiavi a una funzione
- Aggiornamento di un archivio di valori delle chiavi
- Ottenere un riferimento a un archivio di valori delle chiavi
- Eliminazione di un archivio di valori delle chiavi
- Formato file per coppie chiave-valore

> **Note**
>
> Il runtime JavaScript 2.0 include alcuni metodi helper per lavorare con i valori delle chiavi nel codice della funzione. Per ulteriori informazioni, consulta the section called "Metodi helper per archivi di valori delle chiavi".

Creazione di un archivio di valori delle chiavi

Puoi creare contemporaneamente un archivio di valori delle chiavi e le rispettive coppie chiave-valore. Ora, puoi anche creare un archivio di valori delle chiavi vuoto e aggiungere le coppie chiave-valore in un secondo momento.

> **Note**
>
> Se specifichi l'origine dati da un bucket Amazon S3, devi disporre delle autorizzazioni `s3:GetObject` e `s3:GetBucketLocation` per tale bucket. Se non disponi di tali autorizzazioni, CloudFront non può creare correttamente l'archivio di valori delle chiavi.

Scegli se desideri aggiungere coppie chiave-valore contemporaneamente alla creazione dell'archivio di valori delle chiavi. Puoi importare le coppie chiave-valore utilizzando la console CloudFront, l'API CloudFront o gli SDK AWS. Tuttavia, puoi importare il file di coppie chiave-valore solo quando crei inizialmente l'archivio di valori delle chiavi.

Per creare un file di coppie chiave-valore, consulta Formato file per coppie chiave-valore.

Console

Come creare un archivio di valori delle chiavi

1. Accedi a Console di gestione AWS e apri la pagina Funzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Scegli la scheda KeyValueStores, quindi seleziona Crea KeyValueStore.
3. Immetti un nome e una descrizione facoltativa per l'archivio di valori delle chiavi.
4. Completa URI S3:
   - Se disponi di un file di coppie chiave-valore, inserisci il percorso del bucket Amazon S3 in cui hai archiviato il file.
   - Lascia vuoto questo campo se intendi inserire manualmente le coppie chiave-valore.
5. Seleziona Create (Crea). L'archivio di valori delle chiavi ora esiste.

   Viene visualizzata la pagina dei dettagli relativa al nuovo archivio di valori delle chiavi. Le informazioni sulla pagina includono l'ID e l'ARN dell'archivio di valori delle chiavi.

- L'ID è una stringa univoca e casuale di caratteri univoca nell'Account AWS.
- La sintassi dell'ARN è la seguente:

  ```
  Account AWS:key-value-store/the key value stores ID
  ```

6. Osserva la sezione Coppie chiave-valore. Se hai importato un file, in questa sezione vengono visualizzate alcune coppie chiave-valore. Puoi eseguire le operazioni indicate di seguito:

   - Se hai importato un file, puoi anche aggiungere altri valori manualmente.
   - Se non hai importato un file da un bucket Amazon S3 e vuoi aggiungere subito coppie chiave-valore, puoi completare la fase successiva.
   - Puoi ignorare questa fase e aggiungere le coppie chiave-valore in un secondo momento.

7. Per aggiungere subito le coppie:

   a. Scegli Aggiungi coppie chiave-valore.

   b. Scegli Aggiungi coppia e inserisci un nome e un valore. Ripeti questa fase per aggiungere altre coppie.

   c. Al termine, scegli Salva modifiche per salvare tutte le coppie chiave-valore nell'archivio di valori delle chiavi. Nella finestra di dialogo visualizzata, scegli Fatto.

8. Per associare subito l'archivio di valori delle chiavi a una funzione, completa la sezione Funzioni associate. Per ulteriori informazioni, consulta ??? o ???.

   Puoi associare la funzione in un secondo momento, dalla pagina dei dettagli di questo archivio di valori delle chiavi o dalla pagina dei dettagli della funzione.

AWS CLI

Come creare un archivio di valori delle chiavi

- Esegui il comando seguente per creare un archivio di valori delle chiavi e importare le coppie chiave-valore da un bucket Amazon S3.

```
aws cloudfront create-key-value-store \
    --name=keyvaluestore1 \
    --comment="This is my key value store file" \
    --import-source=SourceType=S3,SourceARN=arn:aws:s3:::amzn-s3-demo-
bucket1/kvs-input.json
```

Risposta

```
{
    "ETag": "ETVABCEXAMPLE",
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/key-value-store/
arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-
example",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is my key value store file",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "PROVISIONING",
        "LastModifiedTime": "2024-08-06T22:19:10.813000+00:00"
    }
}
```

API

Come creare un archivio di valori delle chiavi

1. Utilizza l'operazione CreateKeyValueStore di CloudFront. L'operazione richiede diversi parametri:
   - un `name` dell'archivio di valori delle chiavi;
   - un parametro `comment` che includa un commento;
   - un parametro `import-source` che consenta di importare coppie chiave-valore da un file archiviato in un bucket Amazon S3. Puoi importare da un file solo la prima volta che crei l'archivio di valori delle chiavi. Per informazioni sulla struttura dei file, consulta the section called "Formato file per coppie chiave-valore".

La risposta dell'operazione include le informazioni seguenti:

- i valori trasmessi nella richiesta, incluso il nome assegnato;
- dati come l'ora di creazione;

- un `ETag` (ad esempio, `ETVABCEXAMPLE`), l'ARN che include il nome dell'archivio di valori delle chiavi (ad esempio, `arn:aws:cloudfront::123456789012:key-value-store/keyvaluestore1`).

  Per utilizzare l'archivio di valori delle chiavi a livello di codice, utilizzerai una combinazione di `ETag`, ARN e nome.

Stati dell'archivio di valori delle chiavi

Quando crei un archivio di valori delle chiavi, i valori di stato del datastore possono essere i seguenti.

Valore	Descrizione
Provisioning	L'archivio di valori delle chiavi è stato creato e CloudFront sta elaborando l'origine dati specificata.
Pronto	L'archivio di valori delle chiavi è stato creato e CloudFront ha correttamente elaborato l'origine dati specificata.
Importazione non riuscita	CloudFront non è stato in grado di elaborare l'origine dati specificata. Questo stato può essere visualizzato se il formato file non è valido o se supera il limite di dimensioni. Per ulteriori informazioni, consulta Formato file per coppie chiave-valore.

Associazione di un archivio di valori delle chiavi a una funzione

Dopo aver creato l'archivio di valori delle chiavi, puoi aggiornare la funzione per associarla all'archivio di valori delle chiavi. Questa associazione è necessaria per utilizzare le coppie chiave-valore di tale archivio nella funzione. Si applicano le regole seguenti:

- Una funzione può avere un solo archivio di valori delle chiavi
- Puoi associare lo stesso archivio di valori delle chiavi a più funzioni

Console

Come associare un archivio di valori delle chiavi a una funzione

1. Accedi alla console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegli il nome della funzione.
3. Nella sezione Associa KeyValueStore, scegli Associa KeyValueStore esistente.
4. Seleziona l'archivio di valori delle chiavi contenente le coppie chiave-valore nella funzione, quindi scegli Associata KeyValueStore.

   CloudFront associa immediatamente l'archivio alla funzione. Non è necessario salvare la funzione.
5. Per specificare un archivio di valori delle chiavi diverso, scegli Aggiorna KeyValueStore associato, seleziona il nome di un altro archivio di valori delle chiavi e scegli Associa KeyValueStore.

Per ulteriori informazioni, consulta the section called "Aggiornamento delle funzioni".

AWS CLI

Come associare un archivio di valori delle chiavi a una funzione

- Esegui il comando seguente per aggiornare la funzione *MaxAge* e associare una risorsa dell'archivio di valori delle chiavi.

```
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::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example"}]}}' \
    --function-code fileb://function-max-age-v1.js \
    --if-match ETVABCEXAMPLE
```

- Per associare un archivio di valori delle chiavi a una funzione, specifica il parametro `KeyValueStoreAssociations` e l'ARN dell'archivio di valori delle chiavi.
- Per modificare l'associazione, specifica un altro ARN dell'archivio di valori delle chiavi.

- Per rimuovere l'associazione, rimuovi il parametro `KeyValueStoreAssociations`.

Per ulteriori informazioni, consulta the section called "Aggiornamento delle funzioni".

API

Come associare un archivio di valori delle chiavi a una funzione

- Utilizza l'operazione API UpdateFunction. Per ulteriori informazioni, consulta the section called "Aggiornamento delle funzioni".

> **Note**
>
> - Se modifichi un archivio di valori delle chiavi senza cambiare le coppie chiave-valore, o se modifichi solo le coppie chiave-valore nell'archivio di valori delle chiavi, non devi associare nuovamente l'archivio di valori delle chiavi. Inoltre, non è necessario ripubblicare la funzione.
>
> Tuttavia, ti consigliamo di testare la funzione per verificare che funzioni nel modo previsto. Per ulteriori informazioni, consulta Test delle funzioni.
> - Puoi visualizzare tutte le funzioni che utilizzano un archivio di valori delle chiavi specifico. Nella console CloudFront, scegli la pagina dei dettagli dell'archivio di valori delle chiavi.

Aggiornamento di un archivio di valori delle chiavi

Quando aggiorni un archivio di valori delle chiavi, puoi modificare le coppie chiave-valore o modificare l'associazione tra l'archivio di valori delle chiavi e la funzione.

Console

Come aggiornare un archivio di valori delle chiavi

1. Accedi a Console di gestione AWS e apri la pagina Funzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Scegli la scheda KeyValueStores.
3. Seleziona l'archivio dei valori delle chiavi che desideri aggiornare.

- Per aggiornare le coppie chiave-valore, scegli Modifica nella sezione Coppie chiave-valore. Puoi aggiungere o eliminare qualsiasi coppia chiave-valore. Puoi anche modificare il valore di una coppia chiave-valore esistente. Al termine, scegli Salva le modifiche.
- Per aggiornare l'associazione per questo archivio di valori delle chiavi, scegli Vai alle funzioni. Per ulteriori informazioni, consulta the section called "Associazione di un archivio di valori delle chiavi a una funzione".

AWS CLI

Come aggiornare un archivio di valori delle chiavi

1. Modificare le coppie chiave-valore: puoi aggiungere altre coppie chiave-valore, eliminare una o più coppie chiave-valore, nonché modificare il valore di una coppia chiave-valore esistente. Per ulteriori informazioni, consulta Utilizzo dei dati dei valori delle chiavi.
2. Modificare l'associazione della funzione per l'archivio di valori delle chiavi: per aggiornare l'associazione della funzione per l'archivio di valori delle chiavi, consulta Associazione di un archivio di valori delle chiavi a una funzione.

> **Tip**
>
> Avrai bisogno dell'ARN dell'archivio di valori delle chiavi. Per ulteriori informazioni, consulta the section called "Ottenere un riferimento a un archivio di valori delle chiavi".

API

Come aggiornare un archivio di valori delle chiavi

1. Modificare le coppie chiave-valore: puoi aggiungere altre coppie chiave-valore, eliminare una o più coppie chiave-valore, nonché modificare il valore di una coppia chiave-valore esistente. Per ulteriori informazioni, consulta Utilizzo dei dati dei valori delle chiavi.
2. Modificare l'associazione della funzione per l'archivio di valori delle chiavi: per aggiornare l'associazione della funzione per l'archivio di valori delle chiavi, utilizza l'operazione API UpdateFunction. Per ulteriori informazioni, consulta the section called "Aggiornamento delle funzioni".

> **Tip**
>
> Avrai bisogno dell'ARN dell'archivio di valori delle chiavi. Per ulteriori informazioni, consulta the section called “Ottenere un riferimento a un archivio di valori delle chiavi”.

Ottenere un riferimento a un archivio di valori delle chiavi

Per utilizzare gli archivi di valori delle chiavi a livello di codice, sono necessari l’`ETag` e il nome dell’archivio di valori delle chiavi.

Per ottenere entrambi i valori, puoi utilizzare AWS Command Line Interface (AWS CLI) o l’API CloudFront.

AWS CLI

Come ottenere il riferimento all’archivio di valori delle chiavi

1. Per restituire un elenco di archivi di valori delle chiavi, il seguente comando trova il nome dell’archivio di valori delle chiavi da modificare.

```
aws cloudfront list-key-value-stores
```

2. Dalla risposta, trova il nome dell’archivio di valori delle chiavi desiderato.

   Risposta

```
{
    "KeyValueStoreList": {
        "Items": [
            {
                "Name": "keyvaluestore3",
                "Id": "37435e19-c205-4271-9e5c-example3",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/37435e19-c205-4271-9e5c-example3",
                "Status": "READY",
                "LastModifiedTime": "2024-05-08T14:50:18.876000+00:00"
            },
            {
                "Name": "keyvaluestore2",
```

```
                "Id": "47970d59-6408-474d-b850-example2",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/47970d59-6408-474d-b850-example2",
                "Status": "READY",
                "LastModifiedTime": "2024-05-30T21:06:22.113000+00:00"
            },
            {
                "Name": "keyvaluestore1",
                "Id": "8aa76c93-3198-462c-aaf6-example",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
                "Status": "READY",
                "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
            }
        ]
    }
}
```

3. Esegui il comando seguente per restituire l'ETag per l'archivio di valori delle chiavi specificato.

```
aws cloudfront describe-key-value-store \
    --name=keyvaluestore1
```

Risposta

```
{
    "ETag": "E3UN6WX5RRO2AG",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is an example KVS",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "READY",
        "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
    }
}
```

API

Come ottenere il riferimento all'archivio di valori delle chiavi

1. Utilizza l'operazione API CloudFront ListKeyValueStores per restituire un elenco di archivi di valori delle chiavi. Trova il nome dell'archivio di valori delle chiavi da modificare.
2. Utilizza l'operazione API CloudFront DescribeKeyValueStore e specifica il nome dell'archivio di valori delle chiavi restituito dalla fase precedente.

La risposta include un UUID, nonché l'ARN e l'`ETag` dell'archivio di valori delle chiavi.

- Un `ETag`, ad esempio `E3UN6WX5RRO2AG`
- L'UUID è a 128 bit, ad esempio `8aa76c93-3198-462c-aaf6-example`
- L'ARN include il numero di Account AWS, la costante `key-value-store` e l'UUID, come nell'esempio seguente:

  ```
  arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-example
  ```

Per ulteriori informazioni sull'operazione `DescribeKeyValueStore`, consulta the section called "Informazioni su KeyValueStore di CloudFront".

Eliminazione di un archivio di valori delle chiavi

Puoi eliminare l'archivio di valori delle chiavi utilizzando la console Amazon CloudFront o l'API.

Console

Come eliminare un archivio di valori delle chiavi

1. Accedi a Console di gestione AWS e apri la pagina Funzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Scegli il nome della funzione.
3. Nella sezione KeyValueStore associato, verifica se un archivio di valori delle chiavi è associato alla funzione. In tal caso, rimuovi l'associazione scegliendo Annulla associazione KeyValueStore, quindi scegli Rimuovi associazione.
4. Nel riquadro di navigazione, scegli la pagina Funzioni, quindi seleziona la scheda KeyValueStores.

5. Seleziona l'archivio di valori delle chiavi da eliminare, quindi scegli Elimina.

AWS CLI

Come eliminare un archivio di valori delle chiavi

1. Ottieni l'`ETag` e il nome dell'archivio di valori delle chiavi. Per ulteriori informazioni, consulta the section called "Ottenere un riferimento a un archivio di valori delle chiavi".
2. Verifica se l'archivio di valori delle chiavi è associato a una funzione. Se lo è, rimuovi l'associazione. Per ulteriori informazioni su questi due passaggi, consulta ???.
3. Dopo aver ottenuto il nome e l'`ETag` dell'archivio di valori delle chiavi e dopo che questo non è più associato a una funzione, puoi eliminarlo.

   Esegui il comando seguente per eliminare l'l'archivio di valori delle chiavi specificato.

```
aws cloudfront delete-key-value-store \
    --name=keyvaluestore1 \
    --if-match=E3UN6WX5RRO2AG
```

API

Come eliminare un archivio di valori delle chiavi

1. Ottieni l'`ETag` e il nome dell'archivio di valori delle chiavi. Per ulteriori informazioni, consulta the section called "Ottenere un riferimento a un archivio di valori delle chiavi".
2. Verifica se l'archivio di valori delle chiavi è associato a una funzione. Se lo è, rimuovi l'associazione. Per ulteriori informazioni su questi due passaggi, consulta ???.
3. Per eliminare l'archivio di valori delle chiavi, utilizza l'operazione API DeleteKeyValueStore di CloudFront.

Formato file per coppie chiave-valore

Quando crei un file con codifica UTF-8, utilizza il seguente formato JSON:

```
{
  "data":[
    {
      "key":"key1",
```

```
      "value":"value"
    },
    {
      "key":"key2",
      "value":"value"
    }
  ]
}
```

Il file non può includere chiavi duplicate. Se hai specificato un file non valido nel bucket Amazon S3, puoi aggiornare il file per rimuovere eventuali duplicati e quindi provare a creare nuovamente l'archivio di valori delle chiavi.

Per ulteriori informazioni, consulta Creazione di un archivio di valori delle chiavi.

> **Note**
>
> Il file per l'origine dati e le relative coppie chiave-valore hanno i seguenti limiti:
>
> - Dimensione del file: 5 MB
> - Dimensione della chiave: 512 caratteri
> - Dimensione del valore: 1024 caratteri

Utilizzo dei dati dei valori delle chiavi

In questa sezione viene descritto come aggiungere coppie chiave-valore a un archivio di valori delle chiavi esistente. Per includere coppie chiave-valore durante la creazione iniziale degli archivi di valori delle chiavi, consulta the section called "Creazione di un archivio di valori delle chiavi".

Argomenti

- Utilizzo di coppie chiave-valore (console)
- Informazioni su KeyValueStore di CloudFront
- Utilizzo di coppie chiave-valore (AWS CLI)
- Utilizzo di coppie chiave-valore (API)

Utilizzo di coppie chiave-valore (console)

Puoi utilizzare la console CloudFront per utilizzare le coppie chiave-valore.

Come utilizzare coppie chiave-valore

1. Accedi a Console di gestione AWS e apri la pagina Funzioni nella console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Scegli la scheda KeyValueStores.
3. Seleziona l'archivio dei valori delle chiavi da modificare.
4. Nella sezione Coppie chiave-valore, scegli Modifica.
5. Puoi aggiungere una coppia chiave-valore, eliminarla o modificare il valore di una coppia esistente.
6. Al termine, scegli Salva le modifiche.

Informazioni su KeyValueStore di CloudFront

> **Tip**
>
> L'API KeyValueStore di CloudFront è un servizio globale che utilizza Signature Version 4A (SigV4A) per l'autenticazione. L'utilizzo di credenziali temporanee con SigV4A richiede i token sessione versione 2. Per ulteriori informazioni, consulta Utilizzo di credenziali temporanee con l'API KeyValueStore di CloudFront.

Se utilizzi AWS Command Line Interface (AWS CLI) o il tuo codice per chiamare l'API KeyValueStore di CloudFront, consulta le seguenti sezioni.

Quando utilizzi un archivio di valori delle chiavi e le relative coppie chiave-valore, il servizio che chiami dipende dal tuo caso d'uso:

- Per utilizzare le coppie chiave-valore in un archivio di valori delle chiavi esistente, utilizza il servizio KeyValueStore di CloudFront.
- Per includere coppie chiave-valore nell'archivio chiave-valore quando lo crei inizialmente, utilizza il servizio CloudFront.

Sia l'API di CloudFront che l'API di KeyValueStore di CloudFront dispongono di un'operazione `DescribeKeyValueStore`. Vengono chiamate per diversi motivi. Per comprendere le differenze, consulta la tabella seguente.

	API DescribeKeyValueStore di CloudFront	API DescribeKeyValueStore di KeyValueStore di CloudFront
Dati relativi all'archivio di valori delle chiavi	Restituisce dati quali lo stato e la data dell'ultima modifica dell'archivio di valori delle chiavi.	Restituisce dati relativi ai contenuti della risorsa di archiviazione: le coppie chiave-valore nell'archivio e le dimensioni del contenuto.
Dati che identificano l'archivio di valori delle chiavi	Restituisce un `ETag`, l'UUID e l'ARN dell'archivio di valori delle chiavi.	Restituisce un `ETag` e l'ARN dell'archivio di valori delle chiavi.

Note

- Ogni operazione DescribeKeyValueStore restituisce un diverso `ETag`. Gli `ETags` non sono intercambiabili.
- Quando chiami un'operazione API per completare un'azione, devi specificare l'`ETag` dall'API appropriata. Ad esempio, nell'operazione DeleteKey di KeyValueStore di CloudFront, si specifica l'`ETag` restituito dall'operazione DescribeKeyValueStore di KeyValueStore di CloudFront.
- Quando invochi le Funzioni CloudFront utilizzando KeyValueStore di CloudFront, i valori nell'archivio di valori delle chiavi non vengono aggiornati o modificati durante l'invocazione della funzione. Gli aggiornamenti vengono elaborati tra le invocazioni di una funzione.

Utilizzo di coppie chiave-valore (AWS CLI)

Puoi eseguire i comandi AWS Command Line Interface seguenti per KeyValueStore di CloudFront.

Indice

- Descrizione di un archivio di valori delle chiavi
- Creazione di una coppia chiave-valore
- Eliminazione di una coppia chiave-valore
- Aggiornamento di coppie chiave-valore

Elencare coppie chiave/valore

Per elencare coppie chiave-valore nell'archivio di valori delle chiavi, esegui il comando seguente.

```
aws cloudfront-keyvaluestore list-keys \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Risposta

```
{
    "Items": [
        {
            "Key": "key1",
            "Value": "value1"
        }
    ]
}
```

Ottenere coppie chiave/valore

Per ottenere una coppia chiave-valore nell'archivio di valori delle chiavi, esegui il comando seguente.

```
aws cloudfront-keyvaluestore get-key \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Risposta

```
{
    "Key": "key1",
    "Value": "value1",
    "ItemCount": 1,
    "TotalSizeInBytes": 11
```

```
}
```

Descrizione di un archivio di valori delle chiavi

Per descrivere un archivio di valori delle chiavi, esegui il comando seguente.

```
aws cloudfront-keyvaluestore describe-key-value-store \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Risposta

```
{
    "ETag": "KV1F83G8C2ARO7P",
    "ItemCount": 1,
    "TotalSizeInBytes": 11,
    "KvsARN": "arn:aws:cloudfront::123456789012:key-value-store/37435e19-
c205-4271-9e5c-example",
    "Created": "2024-05-08T07:48:45.381000-07:00",
    "LastModified": "2024-08-05T13:50:58.843000-07:00",
    "Status": "READY"
}
```

Creazione di una coppia chiave-valore

Per creare una coppia chiave-valore nell'archivio di valori delle chiavi, esegui il comando seguente.

```
aws cloudfront-keyvaluestore put-key \
    --if-match=KV1PA6795UKMFR9 \
    --key=key2 \
    --value=value2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Risposta

```
{
    "ETag": "KV13V1IB3VIYZZH",
    "ItemCount": 3,
    "TotalSizeInBytes": 31
}
```

Eliminazione di una coppia chiave-valore

Per eliminare una coppia chiave-valore, esegui il comando seguente.

```
aws cloudfront-keyvaluestore delete-key \
    --if-match=KV13V1IB3VIYZZH \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Output

```
{
    "ETag": "KV1VC38T7YXB528",
    "ItemCount": 2,
    "TotalSizeInBytes": 22
}
```

Aggiornamento di coppie chiave-valore

Puoi utilizzare il comando `update-keys` per aggiornare più coppie chiave-valore. Ad esempio, per eliminare una coppia chiave-valore esistente e crearne un'altra, esegui il comando seguente.

```
aws cloudfront-keyvaluestore update-keys \
    --if-match=KV2EUQ1WTGCTBG2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example \
    --deletes '[{"Key":"key2"}]' \
    --puts '[{"Key":"key3","Value":"value3"}]'
```

Risposta

```
{
    "ETag": "KV3AEGXETSR30VB",
    "ItemCount": 3,
    "TotalSizeInBytes": 28
}
```

Utilizzo di coppie chiave-valore (API)

Segui questa sezione per utilizzare le coppie chiave-valore a livello di codice.

Indice

Ottenere un riferimento a un archivio di valori delle chiavi

Quando utilizzi l'API KeyValueStore di CloudFront per chiamare un'operazione di scrittura, devi specificare l'ARN e l'`ETag` dell'archivio di valori delle chiavi. Per ottenere questi dati, procedi come descritto di seguito:

Come ottenere un riferimento a un archivio di valori delle chiavi

1. Utilizza l'operazione API CloudFront ListKeyValueStores per ottenere un elenco di archivi di valori delle chiavi. Trova l'archivio di valori delle chiavi da modificare.
2. Utilizza l'operazione API CloudFrontKeyValueStore DescribeKeyValueStore e specifica l'archivio di valori delle chiavi della fase precedente.

   La risposta include l'ARN e l'`ETag` dell'archivio di valori delle chiavi.

   - L'ARN include il numero di Account AWS, la costante `key-value-store` e l'UUID, come nell'esempio seguente:

     ```
     arn:aws:cloudfront::123456789012:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
     ```

   - Un `ETag` il cui aspetto è simile a quello dell'esempio seguente:

     ```
     ETVABCEXAMPLE2
     ```

Modifica delle coppie chiave-valore in un archivio di valori delle chiavi

Puoi specificare l'archivio di valori delle chiavi che contiene la coppia chiave-valore che desideri aggiornare.

Consulta le seguenti operazioni API di KeyValueStore di CloudFront:

- CloudFrontKeyValueStore DeleteKey: elimina una coppia chiave-valore
- CloudFrontKeyValueStore GetKey: restituisce una coppia chiave-valore

- CloudFrontKeyValueStore ListKeys: restituisce un elenco di coppie chiave-valore
- CloudFrontKeyValueStore PutKey: puoi eseguire le seguenti attività:
  - Creare una coppia chiave-valore in un unico archivio di valori delle chiavi specificando un nuovo nome e valore della chiave.
  - Impostare un valore diverso in una coppia chiave-valore esistente specificando un nome chiave esistente e un nuovo valore della chiave.
- CloudFrontKeyValueStore UpdateKeys: puoi eseguire una o più delle seguenti azioni in un'unica operazione "tutto o niente":
  - Eliminare una o più coppie chiave-valore
  - Creare una o più nuove coppie chiave-valore
  - Impostare un valore diverso in una o più coppie chiave-valore esistenti

Codice di esempio per KeyValueStore di CloudFront

Example

Il codice seguente mostra come chiamare l'operazione API `DescribeKeyValueStore` per un archivio di valori delle chiavi.

```
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);
  }
})();
```

Personalizza con le funzioni di CloudFront connessione

CloudFront Le funzioni di connessione consentono di scrivere JavaScript funzioni leggere per la convalida dei certificati MTL e la logica di autenticazione personalizzata. Le funzioni di connessione vengono eseguite durante la creazione della connessione MTL per convalidare i certificati client, implementare regole di autenticazione specifiche del dispositivo e gestire scenari di revoca dei certificati. L'ambiente di runtime Connection Functions offre tempi di avvio inferiori al millisecondo, è immediatamente scalabile per gestire milioni di connessioni al secondo ed è estremamente sicuro. Le funzioni di connessione sono una funzionalità nativa di CloudFront, il che significa che puoi creare, testare e distribuire il codice interamente all'interno. CloudFront

Quando associate una funzione di connessione a una CloudFront distribuzione abilitata per MTLS, CloudFront intercetta le richieste di connessione TLS nelle postazioni CloudFront periferiche e trasmette le informazioni sul certificato alla funzione. È possibile richiamare Connection Functions quando si verifica il seguente evento:

- Durante la creazione della connessione TLS (richiesta di connessione), per connessioni TLS (mTLS) reciproche

Per ulteriori informazioni sulle funzioni di connessione, vedere i seguenti argomenti.

Argomenti

- Panoramica e flusso di lavoro
- Configurazione e limiti
- Crea funzioni di CloudFront connessione per la convalida reciproca del TLS (viewer)
- Scrivi il codice della funzione di CloudFront connessione per la convalida reciproca del TLS (viewer)
- Verifica le funzioni di CloudFront connessione prima della distribuzione
- Associa le funzioni di connessione alle distribuzioni
- Implementa la revoca dei certificati per Mutual TLS (viewer) con funzioni e CloudFront KeyValueStore

Panoramica e flusso di lavoro

CloudFront Le funzioni di connessione sono un tipo specializzato di CloudFront funzioni che vengono eseguite durante l'handshake TLS quando un client tenta di stabilire una connessione mTLS. La funzione di connessione può accedere alle informazioni sul certificato del client, ai parametri di configurazione MTLS, ai risultati del controllo della revoca del certificato e all'indirizzo IP del client.

Le funzioni di connessione vengono richiamate dopo aver CloudFront eseguito la convalida standard dei certificati (catena di fiducia, scadenza, verifica della firma), ma possono essere eseguite anche se i controlli di revoca dei certificati falliscono. Ciò consente di implementare una logica personalizzata per la gestione dei certificati revocati o l'aggiunta di criteri di convalida aggiuntivi.

Dopo aver creato e pubblicato una funzione di connessione, assicuratevi di aggiungere un'associazione per il tipo di evento di richiesta di connessione con una distribuzione abilitata per MTLS. In questo modo la funzione viene eseguita ogni volta che un client tenta di stabilire una connessione MTLS con. CloudFront

CloudFront Le funzioni di connessione seguono un ciclo di vita in due fasi che consente di sviluppare e testare le funzioni prima di implementarle in produzione. Questo flusso di lavoro garantisce il corretto funzionamento delle funzioni di connessione prima che influiscano sul traffico in tempo reale.

Argomenti

Fasi della funzione

Le funzioni di connessione esistono in una delle due fasi seguenti:

- SVILUPPO — Le funzioni in questa fase possono essere modificate, testate e aggiornate. Utilizzate questa fase per scrivere ed eseguire il debug del codice della funzione.
- LIVE: le funzioni in questa fase sono di sola lettura e gestiscono il traffico di produzione. Non è possibile modificare direttamente le funzioni nella fase LIVE.

Quando si crea una nuova funzione di connessione, questa inizia nella fase DI SVILUPPO. Dopo il test e la convalida, pubblicate la funzione per spostarla nella fase LIVE.

Flusso di lavoro di sviluppo

Segui questo flusso di lavoro per sviluppare e implementare le funzioni di connessione:

1. Crea: crea una nuova funzione di connessione nella fase di SVILUPPO con il codice e la configurazione iniziali.
2. Test: utilizza la funzionalità di test per convalidare la funzione con eventi di connessione di esempio prima della distribuzione.
3. Aggiornamento: modifica il codice e la configurazione della funzione secondo necessità in base ai risultati del test.
4. Pubblicazione: quando è pronta per la produzione, pubblica la funzione per spostarla dalla fase DI SVILUPPO alla fase LIVE.
5. Associa: associa la funzione pubblicata alla tua distribuzione abilitata per MTLS per gestire le connessioni live.

Per apportare modifiche a una funzione LIVE, è necessario aggiornare la versione DEVELOPMENT e pubblicarla nuovamente. Questo crea una nuova versione nella fase LIVE.

Differenze rispetto ad altri tipi di funzioni

Le funzioni di connessione differiscono dalle funzioni di richiesta e risposta del visualizzatore in diversi modi importanti:

- Le funzioni di connessione vengono eseguite dopo l'handshake MTLS, prima che avvenga qualsiasi elaborazione HTTP
- Le funzioni di connessione hanno accesso alle informazioni del certificato TLS anziché ai dati HTTP request/response
- Le funzioni di connessione possono solo consentire o negare la connessione, non modificare i dati HTTP
- Le funzioni di connessione vengono richiamate solo per nuove connessioni TLS, non per il riutilizzo della connessione
- La ripresa della sessione TLS non è supportata con MTLS per garantire che la convalida del certificato avvenga su ogni connessione
- Le funzioni di connessione vengono eseguite in aggiunta alle funzioni standard di richiesta e risposta del visualizzatore

- Le funzioni di connessione vengono associate a livello di distribuzione, anziché a livello di comportamento della cache.
- Le funzioni di connessione supportano solo il JavaScript runtime 2.0.

Configurazione e limiti

CloudFront Le funzioni di connessione hanno requisiti di configurazione e limiti di servizio specifici a causa del loro ruolo specializzato nella convalida delle connessioni TLS e dei requisiti prestazionali dell'edge computing.

Argomenti

Requisiti del codice funzionale

Le funzioni di connessione richiedono un JavaScript codice che elabora gli eventi di connessione TLS. Il codice della funzione deve:

- Essere scritto in JavaScript
- Elabora gli eventi di connessione e allow/deny prendi decisioni
- Esecuzione completa entro i limiti di tempo
- Gestisci la logica di convalida dei certificati e delle connessioni

Limiti del servizio

Le funzioni di connessione sono soggette ai seguenti limiti:

- Dimensione della funzione: il codice e la configurazione della funzione hanno dimensioni limitate
- Tempo di esecuzione: le funzioni hanno limiti di tempo di esecuzione rigorosi per l'elaborazione delle connessioni TLS
- Limiti di associazione: a ciascuna distribuzione può essere associata una sola funzione di connessione

- Restrizioni sullo stage: solo le funzioni dello stage LIVE possono essere associate alle distribuzioni

Opzioni di filtraggio delle funzioni

Quando si elencano le funzioni di connessione, è possibile utilizzare i seguenti filtri:

- Filtro Stage: filtra per fase DEVELOPMENT o LIVE
- Filtro di associazione: filtra per ID di distribuzione o associazioni di ID di archivio chiave-valore

Questi filtri consentono di organizzare e gestire le funzioni di connessione in diversi ambienti e casi d'uso.

Crea funzioni di CloudFront connessione per la convalida reciproca del TLS (viewer)

È possibile creare una funzione di CloudFront connessione in due fasi:

1. Crea il codice della funzione come JavaScript. Puoi usare l'esempio predefinito dalla CloudFront console o scriverne uno tuo. Per ulteriori informazioni, consulta i seguenti argomenti:
   - Scrivi il codice della funzione di CloudFront connessione per la convalida di MTL
   - CloudFront Struttura degli eventi e formato di risposta di Connection Function
   - Esempi di codice della funzione di connessione
2. CloudFront Utilizzatela per creare la funzione di connessione e includere il codice. Il codice è presente all'interno della funzione (non come riferimento).

Argomenti

- CloudFront console
- AWS CLI

CloudFront console

Per creare una funzione di connessione

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.

2. Scegli Crea funzione.
3. Inserisci un nome di funzione univoco all'interno di Account AWS, scegli Funzione di connessione come tipo di funzione, quindi scegli Continua.
4. Viene visualizzata la pagina dei dettagli della nuova funzione di connessione.

> **Note**
>
> Le funzioni di connessione supportano solo il JavaScript runtime 2.0. Per utilizzare l' KeyValueStore integrazione della funzione di CloudFront connessione nella funzione, è necessario utilizzare questa versione di runtime.

5. Nella sezione Codice funzione, scegli la scheda Build e inserisci il codice della funzione di connessione. Il codice di esempio incluso nella scheda Build illustra la sintassi di base del codice Connection Function.
6. Scegli Save changes (Salva modifiche).
7. Se il codice della funzione di connessione viene utilizzato KeyValueStore per il controllo della revoca dei certificati o la convalida del dispositivo, è necessario associare un. KeyValueStore

   È possibile associare la prima KeyValueStore volta che si crea la funzione. In alternativa, è possibile associarla in un secondo momento, associando Connection Functions.

   Per associare un KeyValueStore adesso, segui questi passaggi:

   - Vai alla KeyValueStore sezione Associa e scegli Associa esistente KeyValueStore.
   - Seleziona KeyValueStore quello che contiene i dati del certificato per la tua funzione di connessione, quindi scegli Associa KeyValueStore.

   CloudFront associa immediatamente lo store alla funzione. Non è necessario salvare la funzione.

AWS CLI

Se si utilizza il AWS CLI, in genere si crea prima il codice della funzione di connessione in un file, quindi si crea la funzione con. AWS CLI

Per creare una funzione di connessione

1. Create il codice della funzione di connessione in un file e memorizzatelo in una directory a cui il computer possa connettersi.
2. Esegui il comando come mostrato nell'esempio. Questo esempio utilizza la notazione `fileb://` per passare il file. Include anche interruzioni di riga per rendere il comando più leggibile.

```
aws cloudfront create-connection-function \
    --name CertificateValidator \
    --connection-function-config '{
        "Comment":"Device certificate validation",
        "Runtime":"cloudfront-js-2.0",
        "KeyValueStoreAssociations":{
            "Quantity":1,
            "Items":[{
                "KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }]
        }
    }' \
    --connection-function-code fileb://certificate-validator.js
```

> **Note**
>
> - Runtime: le funzioni di connessione supportano solo il JavaScript runtime 2.0 (cloudfront-js-2.0).
> - KeyValueStoreAssociations— Se la funzione di connessione utilizza la funzione KeyValueStore per la convalida dei certificati, è possibile associarla quando si crea la funzione per la KeyValueStore prima volta. In alternativa, puoi associarlo in un secondo momento utilizzando update-connection-function. La quantità è sempre 1 perché a ciascuna funzione di connessione può essere KeyValueStore associata una sola.

3. Se il comando viene eseguito correttamente, vedrai un output simile al seguente.

```
ETag: ETVABCEXAMPLE
ConnectionFunctionSummary:
  ConnectionFunctionConfig:
    Comment: Device certificate validation
```

```
    Runtime: cloudfront-js-2.0
    KeyValueStoreAssociations:
      Quantity: 1
      Items:
        - KeyValueStoreARN: arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
  ConnectionFunctionMetadata:
    CreatedTime: '2024-09-04T16:32:54.292000+00:00'
    ConnectionFunctionARN: arn:aws:cloudfront::111122223333:connection-function/
CertificateValidator
    LastModifiedTime: '2024-09-04T16:32:54.292000+00:00'
    Stage: DEVELOPMENT
  Name: CertificateValidator
  Status: UNPUBLISHED
Location: https://cloudfront.amazonaws.com/2020-05-31/connection-function/
arn:aws:cloudfront:::connection-function/CertificateValidator
```

La maggior parte delle informazioni viene ripetuta dalla richiesta. Altre informazioni vengono aggiunte da CloudFront.

> **Note**
>
> - ETag— Questo valore cambia ogni volta che si modifica la funzione di connessione. È necessario questo valore per aggiornare o pubblicare la funzione.
> - Fase: le nuove funzioni di connessione iniziano nella fase DI SVILUPPO. È necessario pubblicare la funzione per spostarla nella fase LIVE prima di associarla a una distribuzione.
> - Stato: lo stato della funzione è INEDITO finché non la pubblicate sullo stage LIVE.

Scrivi il codice della funzione di CloudFront connessione per la convalida reciproca del TLS (viewer)

CloudFront Le funzioni di connessione consentono di scrivere JavaScript funzioni leggere per la convalida dei certificati MTL e la logica di autenticazione personalizzata. Il codice Connection Function può convalidare i certificati client, implementare regole di autenticazione specifiche del dispositivo, gestire scenari di revoca dei certificati e allow/deny prendere decisioni per le connessioni TLS nelle edge location di tutto il mondo. CloudFront

Le funzioni di connessione offrono un modo efficace per estendere la convalida CloudFront dei certificati integrata con la propria logica aziendale. A differenza delle funzioni di richiesta e risposta del visualizzatore che elaborano i dati HTTP, le funzioni di connessione operano a livello TLS e hanno accesso alle informazioni sui certificati, agli indirizzi IP dei client e ai dettagli della connessione TLS. Ciò le rende ideali per implementare modelli di sicurezza zero-trust, sistemi di autenticazione dei dispositivi e politiche di convalida dei certificati personalizzate che vanno oltre la convalida PKI standard.

Il codice della funzione di connessione viene eseguito in un ambiente sicuro e isolato con tempi di avvio inferiori al millisecondo ed è scalabile per gestire milioni di connessioni al secondo. Il runtime è ottimizzato per i carichi di lavoro di convalida dei certificati e offre un'integrazione integrata CloudFront KeyValueStore per le operazioni di ricerca dei dati in tempo reale, abilitando scenari di autenticazione sofisticati come il controllo degli elenchi di revoca dei certificati e la convalida delle liste consentite dei dispositivi.

Per aiutarti a scrivere un codice efficace per le funzioni di connessione, consulta i seguenti argomenti. Per esempi di codice e step-by-step tutorial completi, consulta le sezioni del tutorial di questa guida ed esplora gli esempi di Connection Function disponibili nella CloudFront console.

Argomenti

CloudFront Casi d'uso e scopi della funzione di connessione

Prima di scrivere la funzione di CloudFront connessione, stabilite attentamente il tipo di convalida dei certificati o la logica di autenticazione che dovete implementare. Le funzioni di connessione sono progettate per casi d'uso specifici che richiedono una convalida personalizzata oltre al controllo standard dei certificati PKI. La comprensione del caso d'uso consente di progettare codice efficiente che soddisfi i requisiti di sicurezza mantenendo al contempo prestazioni ottimali.

I casi d'uso di Common Connection Function includono:

- Gestione della revoca dei certificati: implementa politiche personalizzate per la gestione dei certificati revocati, inclusi periodi di grazia per la rotazione dei certificati, eccezioni di rete affidabili per i dispositivi interni o scenari di accesso di emergenza in cui i certificati revocati potrebbero richiedere un accesso temporaneo.
- Supporto MTL opzionale: gestisci connessioni MTL e non MTLS con politiche di autenticazione diverse, in modo da fornire una maggiore sicurezza ai client che supportano i certificati mantenendo la compatibilità con i client legacy.
- Autenticazione basata su IP: combina la convalida dei certificati con il controllo degli indirizzi IP dei client per una maggiore sicurezza, ad esempio limitando l'accesso da aree geografiche specifiche, reti aziendali o intervalli IP dannosi noti.
- Convalida dei certificati multi-tenant: implementa regole di convalida specifiche del tenant in cui si applicano autorità di certificazione o criteri di convalida diversi in base all'emittente del certificato client o agli attributi del soggetto.
- Controllo degli accessi basato sul tempo: applica restrizioni temporali in cui i certificati sono validi solo in orari, finestre di manutenzione o periodi lavorativi specifici, anche se il certificato stesso non è scaduto.

Le funzioni di connessione vengono CloudFront eseguite dopo aver eseguito la convalida standard dei certificati (verifica della catena di fiducia, controlli di scadenza e convalida delle firme) ma prima che venga stabilita la connessione TLS. Questa tempistica offre la flessibilità necessaria per aggiungere criteri di convalida personalizzati, beneficiando al contempo della convalida dei certificati integrata. CloudFront La tua funzione riceve i risultati della convalida standard e può prendere decisioni informate sull'opportunità di consentire o negare la connessione in base a criteri standard e personalizzati.

Durante la progettazione della funzione di connessione, considerate le implicazioni prestazionali della logica di convalida. Le funzioni hanno un limite di esecuzione di 5 millisecondi, quindi le operazioni complesse devono essere ottimizzate in termini di velocità. KeyValueStore Utilizzatele per ricerche rapide dei dati anziché calcoli complessi e strutturate la logica di convalida in modo che fallisca rapidamente per i certificati non validi.

CloudFront Funzione di connessione, struttura degli eventi e formato di risposta.

CloudFront Le funzioni di connessione ricevono una struttura degli eventi diversa rispetto alle funzioni di richiesta e risposta del visualizzatore. Invece dei request/response dati HTTP, le funzioni di connessione ricevono informazioni sul certificato e sulla connessione che è possibile utilizzare per prendere decisioni di autenticazione.

Argomenti

Struttura degli eventi per le funzioni di connessione

Le funzioni di connessione ricevono un oggetto evento che contiene informazioni sul certificato e sulla connessione. La struttura degli eventi della funzione è illustrata di seguito:

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "string",
        "issuer": "string",
        "subject": "string",
        "validity": {
          "notBefore": "string",
          "notAfter": "string",
        },
        "sha256Fingerprint": "string"
      }
    }
  },
  "clientIp": "string",
  "endpoint": "string",
  "distributionId": "string",
  "connectionId": "string"
}
```

Di seguito è riportato un esempio della struttura degli oggetti dell'evento:

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "00:9e:2a:af:16:56:e5:47:25:7d:2e:38:c3:f9:9d:57:fa",
        "issuer": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "subject": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "validity": {
          "notBefore": "2025-09-10T23:43:10Z",
```

```
          "notAfter": "2055-09-11T00:43:02Z"
        },
        "sha256Fingerprint": "_w6bJ7aOAlGOj7NUhJxTfsfee-ONg_xop3_PTgTJpqs="
      }
    }
  },
  "clientIp": "127.0.0.1",
  "endpoint": "d3lch071jze0cb.cloudfront.net",
  "distributionId": "E1NXS4MQZH501R",
  "connectionId": "NpvTe1925xfj24a67sPQr7ae42BIq03FGhJJKfrQYWZcWZFp96SIIg=="
}
```

Formato di risposta di Connection Functions

La funzione di connessione deve restituire un oggetto di risposta che indichi se consentire o negare la connessione. Usa i metodi di supporto per prendere decisioni sulla connessione:

```
function connectionHandler(connection) {
    // Helper methods to allow or deny connections
    if (/* some logic to determine if function should allow connection */) {
        connection.allow();
    } else {
        connection.deny();
    }
}
```

A differenza delle funzioni di richiesta e risposta del visualizzatore, Connection Functions non può modificare le richieste o le risposte HTTP. Possono solo consentire o negare la connessione TLS.

CloudFront Funzioni di runtime di Connection Functions JavaScript

CloudFront Connection Functions utilizza CloudFront Functions JavaScript runtime 2.0, che fornisce un ambiente sicuro e ad alte prestazioni ottimizzato specificamente per i carichi di lavoro di convalida dei certificati. Il runtime è progettato per iniziare in meno di millisecondi e gestire milioni di esecuzioni simultanee sulla rete edge globale. CloudFront

L'ambiente di runtime include un supporto linguistico completo: JavaScript

- ECMAScript Supporto 2020 (ES11): JavaScript funzionalità moderne tra cui il concatenamento opzionale (?.) , coalescenza nulla (??) e BigInt per gestire numeri di serie di certificati di grandi dimensioni
- Oggetti integrati: JavaScript oggetti standard come Object, Array, JSON, Math e Date

- Registrazione da console: utilizzate console.log () per il debug e il monitoraggio delle decisioni di convalida dei certificati. I log sono disponibili in tempo reale durante i test e possono aiutare a risolvere i problemi della logica di convalida durante lo sviluppo
- KeyValueStore integrazione: accesso nativo a CloudFront KeyValueStore operazioni di ricerca dei dati ultraveloci, che consente il controllo in tempo reale della revoca dei certificati, la convalida delle liste consentite dei dispositivi e il recupero della configurazione specifica del tenant

Le funzioni di connessione sono ottimizzate per garantire prestazioni elevate negli scenari di convalida dei certificati. Il runtime gestisce automaticamente la gestione della memoria, la raccolta dei rifiuti e la pulizia delle risorse per garantire prestazioni costanti su milioni di connessioni simultanee. Tutte le operazioni sono progettate per essere deterministiche e veloci, con il completamento delle KeyValueStore ricerche in genere in microsecondi.

L'ambiente di runtime è completamente isolato tra le esecuzioni delle funzioni, garantendo che non vi siano perdite di dati tra le diverse connessioni client. Ogni esecuzione di funzione inizia con uno stato pulito e non ha accesso ai risultati di esecuzione precedenti o ai dati dei client provenienti da altre connessioni.

CloudFront Metodi di supporto per Connection Function e APIs

CloudFront Connection Functions fornisce metodi di supporto specializzati progettati per semplificare le decisioni di convalida dei certificati e migliorare l'osservabilità. Questi metodi sono ottimizzati per il flusso di lavoro di convalida delle connessioni e si integrano perfettamente con i sistemi CloudFront di registrazione e monitoraggio delle connessioni.

- connection.allow (): consente alla connessione TLS di procedere. Questo metodo segnala CloudFront di completare l'handshake TLS e consente al client di stabilire la connessione. Usalo quando la convalida del certificato ha esito positivo e qualsiasi logica di autenticazione personalizzata è soddisfatta
- connection.deny () — Nega la connessione TLS e termina l'handshake. Questo metodo chiude immediatamente la connessione e impedisce il flusso di traffico HTTP. Il client riceverà un errore di connessione TLS. Utilizzalo per certificati non validi, autenticazione non riuscita o violazioni delle politiche
- connessione. logCustomData() — Aggiunge dati personalizzati ai registri delle connessioni (fino a 800 byte di testo UTF-8). Questo metodo consente di includere risultati di convalida, dettagli del certificato o motivazioni decisionali nei log di CloudFront connessione per il monitoraggio della sicurezza, il controllo della conformità e la risoluzione dei problemi

Questi metodi forniscono un'interfaccia chiara e dichiarativa per prendere decisioni sulla connessione e registrare le informazioni pertinenti per il monitoraggio e il debug. Lo allow/deny schema assicura che l'intento della funzione sia chiaro e che CloudFront possa ottimizzare la gestione della connessione in base alla decisione presa dall'utente. I dati di registrazione personalizzati sono immediatamente disponibili nei registri di CloudFront connessione e possono essere utilizzati con strumenti di analisi dei log per il monitoraggio della sicurezza e informazioni operative.

Chiama sempre connection.allow () o connection.deny () prima del completamento della funzione. Se non viene chiamato nessuno dei due metodi, CloudFront negherà la connessione per impostazione predefinita come precauzione di sicurezza.

CloudFront Integrazione della funzione di connessione KeyValueStore

CloudFront Le funzioni di connessione possono essere utilizzate CloudFront KeyValueStore per eseguire ricerche di dati ultraveloci per scenari di convalida dei certificati. KeyValueStore è particolarmente potente per Connection Functions perché fornisce un accesso ai dati globale e alla fine coerente con tempi di ricerca in microsecondi in tutte le edge location. CloudFront Ciò lo rende ideale per mantenere elenchi di revoca dei certificati, elenchi di dispositivi consentiti, configurazioni dei tenant e altri dati di convalida che devono essere accessibili durante gli handshake TLS.

KeyValueStore l'integrazione è progettata specificamente per flussi di lavoro di convalida delle connessioni ad alte prestazioni:

- KVSHandle.exists (key) — Controlla se esiste una chiave in senza recuperare il valore. KeyValueStore Questo è il metodo più efficiente per scenari di convalida binaria come il controllo della revoca dei certificati, in cui è sufficiente sapere se il numero di serie di un certificato è presente in un elenco di revoche
- KVSHandle.get (key) — Recupera un valore da scenari di convalida più complessi. KeyValueStore Usalo quando devi accedere ai dati di configurazione, alle regole di convalida o ai metadati associati a un certificato o a un identificatore di dispositivo

KeyValueStore le operazioni sono asincrone e devono essere utilizzate con la sintassi async/await. KeyValueStore Ha un limite di dimensione totale di 10 MB e supporta fino a 10 milioni di coppie chiave-valore. KeyValueStore i dati alla fine sono coerenti in tutte le edge location, con gli aggiornamenti che in genere si propagano in pochi secondi.

Per prestazioni ottimali, strutturate le KeyValueStore chiavi in modo da ridurre al minimo le operazioni di ricerca. Utilizza i numeri di serie dei certificati come chiavi per un semplice controllo delle revoce

oppure crea chiavi composite che combinano l'hash dell'emittente e il numero di serie per ambienti con più CA. Considera i compromessi tra complessità e KeyValueStore capacità delle chiavi durante la progettazione della struttura dei dati.

Usa async e await

Le funzioni di connessione supportano le operazioni asincrone utilizzando la async/await sintassi, essenziale quando si lavora con operazioni o altre attività asincrone. KeyValueStore Lo async/await schema assicura che la funzione attenda il completamento delle KeyValueStore ricerche prima di prendere decisioni sulla connessione, mantenendo al contempo le caratteristiche ad alte prestazioni richieste per l'elaborazione dell'handshake TLS.

async/await L'uso corretto è fondamentale per Connection Functions perché le KeyValueStore operazioni, sebbene molto veloci, sono comunque operazioni di rete che richiedono il coordinamento dell'infrastruttura distribuita. CloudFront Il runtime gestisce automaticamente la risoluzione delle promesse e garantisce il completamento della funzione entro il limite di esecuzione di 5 millisecondi.

Example : Funzione di connessione asincrona con KeyValueStore

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Async operation to check KeyValueStore for certificate revocation
    const isRevoked = await
 kvsHandle.exists(connection.clientCertificate.certificates.leaf.serialNumber);

    if (isRevoked) {
        // Log the revocation decision with certificate details
        connection.logCustomData(`REVOKED_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}:
${connection.clientCertificate.certificates.leaf.issuer}`);
        console.log(`Denying connection for revoked certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
        return connection.deny();
    }

    // Log successful validation for monitoring
    connection.logCustomData(`VALID_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}`);
```

```
    console.log(`Allowing connection for valid certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
    return connection.allow();
}
```

Da utilizzare sempre async/await quando si chiamano KeyValueStore metodi o altre operazioni asincrone. Il runtime Connection Function gestisce automaticamente la risoluzione delle promesse e garantisce il corretto flusso di esecuzione entro i rigorosi vincoli temporali dell'elaborazione dell'handshake TLS. Evita di usare .then () o pattern di callback, poiché async/await offre una gestione degli errori più pulita e prestazioni migliori nell'ambiente Connection Function.

Quando progettate funzioni di connessione asincrone, strutturate il codice in modo da ridurre al minimo il numero di KeyValueStore operazioni ed eseguitele il prima possibile nella logica di convalida. Ciò garantisce le massime prestazioni e riduce il rischio di problemi di timeout durante i periodi di traffico intenso. Prendi in considerazione la possibilità di raggruppare i controlli di convalida correlati e di utilizzare il KeyValueStore metodo più efficiente (exists () vs get ()) per il tuo caso d'uso.

Esempi di codice delle funzioni di connessione

Gli esempi seguenti mostrano modelli comuni di Connection Function per diversi scenari di convalida. Utilizzate questi esempi come punti di partenza per le vostre implementazioni di Connection Function.

Example : convalida del certificato del dispositivo

Questo esempio convalida i numeri di serie dei dispositivi e i campi relativi all'oggetto del certificato per dispositivi IoT, console di gioco e altri scenari di autenticazione client:

```
async function connectionHandler(connection) {
    // Custom validation: check device serial number format
    const serialNumber = connection.clientCertificate.certificates.leaf.serialNumber;
    if (!serialNumber.startsWith("DEV")) {
        connection.logCustomData(`INVALID_SERIAL:${serialNumber}`);
        return connection.deny();
    }

    // Validate certificate subject contains required organizational unit
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("OU=AuthorizedDevices")) {
        connection.logCustomData(`INVALID_OU:${subject}`);
        return connection.deny();
    }
```

```
    // Allow connection for valid devices
    connection.logCustomData(`VALID_DEVICE:${serialNumber}`);
    return connection.allow();
}
```

Questa funzione esegue più controlli di convalida oltre alla convalida dei certificati standard, tra cui il formato del numero di serie del dispositivo e la verifica delle unità organizzative.

Example : MTL opzionali con autenticazione mista

Questo esempio gestisce connessioni MTL e non MTLS con politiche di autenticazione diverse:

```
async function connectionHandler(connection) {
    if (connection.clientCertificate) {
        // mTLS connection - enhanced validation for certificate holders
        const subject = connection.clientCertificate.certificates.leaf.subject;
        connection.logCustomData(`MTLS_SUCCESS:${subject}:${connection.clientIp}`);
        console.log(`mTLS connection from: ${subject}`);
        return connection.allow();
    } else {
        // Non-mTLS connection - apply IP-based restrictions
        const clientIp = connection.clientIp;

        // Only allow non-mTLS from specific IP ranges
        if (clientIp.startsWith("203.0.113.") || clientIp.startsWith("198.51.100.")) {
            connection.logCustomData(`NON_MTLS_ALLOWED:${clientIp}`);
            console.log(`Non-mTLS connection allowed from: ${clientIp}`);
            return connection.allow();
        }

        connection.logCustomData(`NON_MTLS_DENIED:${clientIp}`);
        return connection.deny();
    }
}
```

Questa funzione offre una maggiore sicurezza per i client con certificati, mantenendo al contempo la compatibilità con i client legacy di intervalli IP affidabili.

Verifica le funzioni di CloudFront connessione prima della distribuzione

È possibile testare le funzioni di CloudFront connessione nella fase DI SVILUPPO utilizzando l'operazione TestConnectionFunction API. Il test consente di convalidare la logica della funzione con esempi di eventi di connessione prima della pubblicazione nella fase LIVE.

Argomenti

Processo di test

Per testare una funzione di connessione:

1. Crea una funzione di connessione nella fase di SVILUPPO
2. Preparare un oggetto di connessione di prova che rappresenti l'evento di connessione TLS
3. Usa l'operazione TestConnectionFunction API per eseguire la tua funzione con i dati di test
4. Esamina i risultati del test, inclusi l'output della funzione, i registri di esecuzione e gli eventuali messaggi di errore
5. Aggiorna il codice della funzione secondo necessità e ripeti il processo di test

Risultati del test

Quando testate una funzione di connessione, i risultati includono:

- Riepilogo della funzione: metadati relativi alla funzione testata
- Utilizzo del calcolo: metriche delle prestazioni che mostrano l'utilizzo delle risorse
- Registri di esecuzione: output della funzione sulla console, incluse eventuali istruzioni di registrazione
- Uscita della funzione: il risultato restituito dalla funzione
- Messaggi di errore: eventuali errori o eccezioni di runtime verificatisi durante l'esecuzione

Oggetto di test di connessione

L'oggetto di test di connessione è un blob binario (fino a 40 KB) che rappresenta l'evento di connessione TLS che la funzione elaborerà. Questo oggetto contiene il certificato e le informazioni di connessione utilizzate dalla funzione per prendere decisioni di autenticazione.

> **Note**
>
> La struttura e il formato specifici dell'oggetto di test di connessione sono definiti dal runtime CloudFront Connection Functions. CloudFront Consultate la documentazione sulle funzioni o contattateci Supporto AWS per i dettagli sulla creazione di oggetti di test appropriati per il vostro caso d'uso.

Dopo aver creato la funzione di connessione, puoi:

- Verifica la funzione: utilizza la funzionalità di test nella console o nella CLI per convalidare la funzione con eventi di connessione di esempio. Per ulteriori informazioni, consulta Test della funzione di connessione.
- Aggiorna la funzione: modifica il codice e la configurazione della funzione in base alle esigenze. Le funzioni di connessione in fase di SVILUPPO possono essere aggiornate in qualsiasi momento.
- Pubblica la funzione: quando sei pronta per la produzione, pubblica la funzione per spostarla dalla fase DI SVILUPPO alla fase LIVE. Per ulteriori informazioni, vedete Associazione delle funzioni di connessione.
- Associa a una distribuzione: associa la funzione pubblicata a una distribuzione abilitata per MTLS per gestire le connessioni live. Per ulteriori informazioni, vedete Associazione delle funzioni di connessione.

Associa le funzioni di connessione alle distribuzioni

Dopo aver pubblicato una funzione di connessione nella fase LIVE, è necessario associarla a una distribuzione abilitata per MTLS per gestire le connessioni live. Le funzioni di connessione sono associate a livello di distribuzione, a differenza delle funzioni di richiesta e risposta del visualizzatore che sono associate ai comportamenti della cache.

Argomenti

Requisiti di associazione

Per associare una funzione di connessione a una distribuzione:

- La funzione deve essere nella fase LIVE
- La distribuzione deve avere MTL abilitati
- La distribuzione deve avere un trust store valido configurato
- È possibile associare solo una funzione di connessione per distribuzione

Organizzazione delle funzioni con filtri

CloudFront offre funzionalità di filtraggio per aiutarti a organizzare e gestire le funzioni di connessione:

- Filtro ID di distribuzione: trova le funzioni associate a distribuzioni specifiche
- Filtro dell'archivio chiave-valore: trova le funzioni che utilizzano archivi chiave-valore specifici per la ricerca dei dati
- Filtro Stage: elenca le funzioni nella fase DEVELOPMENT o LIVE

Utilizza questi filtri per gestire più funzioni di connessione in diverse distribuzioni o ambienti di sviluppo.

Considerazioni sull'implementazione

Considerate questi fattori quando implementate Connection Functions:

- Implementazione globale: le funzioni di connessione vengono distribuite in tutte le CloudFront edge location del mondo, operazione che può richiedere diversi minuti
- Gestione delle versioni: ogni versione pubblicata crea una nuova funzione LIVE che sostituisce la versione precedente
- Strategia di rollback: pianifica il rollback mantenendo le versioni funzionanti precedenti del codice della funzione

- Test in produzione: valuta la possibilità di utilizzare distribuzioni separate per gli ambienti di gestione temporanea e di produzione

Implementa la revoca dei certificati per Mutual TLS (viewer) con funzioni e CloudFront KeyValueStore

È possibile utilizzare CloudFront Connection Functions con KeyValueStore per implementare il controllo della revoca dei certificati. Ciò consente di mantenere un elenco di numeri di serie dei certificati revocati e di confrontare i certificati client con questo elenco durante l'handshake TLS.

Per implementare la revoca dei certificati, sono necessari questi componenti:

- Una distribuzione configurata con Viewer MTL
- A KeyValueStore contenente i numeri di serie dei certificati revocati
- Una funzione di connessione che interroga KeyValueStore per verificare lo stato del certificato

Quando un client si connette, CloudFront convalida il certificato confrontandolo con il trust store, quindi esegue la funzione di connessione. La tua funzione confronta il numero di serie del certificato con il KeyValueStore e consente o nega la connessione.

Argomenti

Passaggio 1: creare un file KeyValueStore per i certificati revocati

Crea un file KeyValueStore per memorizzare i numeri di serie dei certificati revocati che la Funzione di connessione può controllare durante le connessioni MTL.

Per prima cosa, prepara i numeri di serie dei certificati revocati in formato JSON:

```
{
  "data": [
```

```
    {
      "key": "ABC123DEF456",
      "value": ""
    },
    {
      "key": "789XYZ012GHI",
      "value": ""
    }
  ]
}
```

Carica questo file JSON in un bucket S3, quindi crea: KeyValueStore

```
aws s3 cp revoked-serials.json s3://your-bucket-name/revoked-serials.json
aws cloudfront create-key-value-store \
  --name revoked-serials-kvs \
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::your-bucket-name/revoked-serials.json"
  }'
```

Attendi il completamento del KeyValueStore provisioning. Verifica lo stato con:

```
aws cloudfront get-key-value-store --name "revoked-serials-kvs"
```

Fase 2: Creare la funzione di connessione di revoca

Crea una funzione di connessione che controlli i numeri di serie dei certificati rispetto a quelli KeyValueStore per determinare se i certificati sono stati revocati.

Crea una funzione di connessione che controlli i numeri di serie dei certificati rispetto a: KeyValueStore

```
aws cloudfront create-connection-function \
  --name "revocation-control" \
  --connection-function-config file://connection-function-config.json \
  --connection-function-code file://connection-function-code.txt
```

Il file di configurazione specifica l' KeyValueStore associazione:

```
{
```

```
  "Runtime": "cloudfront-js-2.0",
  "Comment": "A function that implements revocation control via KVS",
  "KeyValueStoreAssociations": {
    "Quantity": 1,
    "Items": [
      {
        "KeyValueStoreArn": "arn:aws:cloudfront::account-id:key-value-store/kvs-id"
      }
    ]
  }
}
```

Il codice della funzione di connessione verifica la presenza KeyValueStore di certificati revocati:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get parsed client serial number from client certificate
    const clientSerialNumber = connection.clientCertInfo.serialNumber;

    // Check KVS to see if serial number exists as a key
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    // Deny connection if serial number exists in KVS
    if (serialNumberExistsInKvs) {
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Allow connections that don't exist in kvs
    console.log("Connection allowed");
    return connection.allow();
}
```

Fase 3: Verifica la tua funzione di revoca

Usa la CloudFront console per testare la tua funzione di connessione con certificati di esempio. Vai alla funzione di connessione nella console e usa la scheda Test.

Esegui il test con certificati di esempio

1. Incolla un certificato di esempio in formato PEM nell'interfaccia di test
2. Specificare facoltativamente un indirizzo IP del client per testare la logica basata su IP
3. Scegli la funzione Test per vedere i risultati dell'esecuzione
4. Esamina i registri di esecuzione per verificare la logica della funzione

Esegui test con certificati validi e revocati per assicurarti che la funzione gestisca correttamente entrambi gli scenari. I log di esecuzione mostrano l'output di console.log e tutti gli errori che si verificano durante l'esecuzione della funzione.

Fase 4: Associate la funzione alla vostra distribuzione

Una volta pubblicata la Connection Function, associala alla distribuzione abilitata per MTLS per attivare il controllo della revoca dei certificati.

È possibile associare la funzione dalla pagina delle impostazioni di distribuzione o dalla tabella delle distribuzioni associate alla funzione di connessione. Passa alle impostazioni di distribuzione, scorri fino alla sezione Viewer Mutual Authentication (mTLS), seleziona la funzione di connessione e salva le modifiche.

Scenari di revoca avanzati

Per requisiti di revoca dei certificati più complessi, considera queste configurazioni aggiuntive:

Argomenti

- Converti gli elenchi di revoca dei certificati (CRL) in formato KeyValueStore
- Gestisci più autorità di certificazione
- Aggiungere dati personalizzati ai registri di connessione
- Gestisci gli aggiornamenti CRL
- Pianifica la capacità KeyValueStore

Converti gli elenchi di revoca dei certificati (CRL) in formato KeyValueStore

Se disponi di un file CRL (Certificate Revocation List), puoi convertirlo in formato KeyValueStore JSON utilizzando OpenSSL e jq:

Converti CRL in formato KeyValueStore

Estrai i numeri di serie dal file CRL:

```
openssl crl -text -noout -in rfc5280_CRL.crl | \
  awk '/Serial Number:/ {print $3}' | \
  cut -d'=' -f2 | \
  sed 's/../&:/g;s/:$//' >> serialnumbers.txt
```

Converti i numeri di serie in formato KeyValueStore JSON:

```
jq -R -s 'split("\n") | map(select(length > 0)) | {data: map({"key": ., "value": ""})}'
 \
  serialnumbers.txt >> serialnumbers_kvs.json
```

Carica il file formattato su S3 e crealo KeyValueStore come descritto nel passaggio 1.

Gestisci più autorità di certificazione

Se disponi TrustStore di più autorità di certificazione (CAs), includi le informazioni sull'emittente nelle KeyValueStore chiavi per evitare conflitti tra certificati diversi CAs che potrebbero avere lo stesso numero di serie.

Per scenari con più CA, utilizzate come chiave una combinazione dell' SHA1 hash dell'emittente e del numero di serie:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientCert = connection.clientCertInfo;

    // Create composite key with issuer hash and serial number
    const issuer = clientCert.issuer.replace(/[^a-zA-Z0-9]/g, '').substring(0, 20);
    const serialno = clientCert.serialNumber;
    const compositeKey = `${issuer}_${serialno}`;

    const cert_revoked = await kvsHandle.exists(compositeKey);

    if (cert_revoked) {
        console.log(`Blocking revoked cert: ${serialno} from issuer: ${issuer}`);
        connection.deny();
    } else {
        connection.allow();
    }
```

```
}
```

> **Note**
>
> L'utilizzo dell'identificatore emittente + del numero di serie crea chiavi più lunghe, che possono ridurre il numero totale di voci che è possibile memorizzare in. KeyValueStore

Aggiungere dati personalizzati ai registri di connessione

Le funzioni di connessione possono aggiungere dati personalizzati ai registri di CloudFront connessione utilizzando il logCustomData metodo. Ciò consente di includere i risultati del controllo di revoca, le informazioni sul certificato o altri dati pertinenti nei registri.

```
async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientSerialNumber = connection.clientCertInfo.serialNumber;
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    if (serialNumberExistsInKvs) {
        // Log revocation details to connection logs
        connection.logCustomData(`REVOKED:${clientSerialNumber}:DENIED`);
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Log successful validation
    connection.logCustomData(`VALID:${clientSerialNumber}:ALLOWED`);
    console.log("Connection allowed");
    return connection.allow();
}
```

I dati personalizzati sono limitati a 800 byte di testo UTF-8 valido. Se superi questo limite, CloudFront tronca i dati fino al limite UTF-8 valido più vicino.

> **Note**
>
> La registrazione dei dati personalizzata funziona solo quando i registri di connessione sono abilitati per la distribuzione. Se i log di connessione non sono configurati, il logCustomData metodo non è operativo.

Gestisci gli aggiornamenti CRL

Le autorità di certificazione possono emettere due tipi di CRLs:

- Completo CRLs: contiene un elenco completo di tutti i certificati revocati
- Delta CRLs: elenca solo i certificati revocati dall'ultimo CRL completo

Per gli aggiornamenti CRL completi, creane uno nuovo KeyValueStore con i dati aggiornati e reindirizza l'associazione Connection Function al nuovo. KeyValueStore Questo approccio è più semplice rispetto al calcolo delle differenze e all'esecuzione di aggiornamenti incrementali.

Per gli aggiornamenti delta CRL, usa il comando update-keys per aggiungere nuovi certificati revocati a quelli esistenti: KeyValueStore

```
aws cloudfront update-key-value-store \
  --name "revoked-serials-kvs" \
  --if-match "current-etag" \
  --put file://delta-revoked-serials.json
```

Pianifica la capacità KeyValueStore

KeyValueStore ha un limite di dimensione di 5 MB e supporta fino a 10 milioni di coppie chiave-valore. Pianifica la capacità dell'elenco di revoca in base al formato della chiave e alla dimensione dei dati:

- Solo numero di serie: archiviazione efficiente per un semplice controllo delle revoche
- Identificatore dell'emittente + numero di serie: chiavi più lunghe per ambienti con più CA

Per elenchi di revoche di grandi dimensioni, prendi in considerazione l'implementazione di un approccio a più livelli in cui mantieni la separazione KeyValueStores per diverse categorie di certificati o periodi di tempo.

Personalizzazione al livello di edge con Lambda@Edge

Lambda @Edge è un'estensione di. AWS Lambda Lambda @Edge è un servizio di elaborazione che consente di eseguire funzioni che personalizzano i contenuti forniti da Amazon. CloudFront Puoi creare funzioni Node.js o Python nella console Lambda in una Regione AWS, Stati Uniti orientali (Virginia settentrionale).

Dopo aver creato la funzione, puoi aggiungere i trigger utilizzando la console CloudFront o la console Lambda in modo che le funzioni vengano eseguite AWS in posizioni più vicine al visualizzatore, senza effettuare il provisioning o gestire i server. Facoltativamente, puoi utilizzare le operazioni Lambda CloudFront e API per configurare funzioni e trigger a livello di codice.

Lambda@Edge è in grado di adattare automaticamente la capacità, da alcune richieste al giorno fino a migliaia di richieste al secondo. L'elaborazione delle richieste in AWS posizioni più vicine al visualizzatore anziché sui server di origine riduce significativamente la latenza e migliora l'esperienza dell'utente.

> **Note**
>
> Lambda@Edge non è supportata con le richieste gRPC. Per ulteriori informazioni, consulta Usare gRPC con le distribuzioni CloudFront .

Argomenti

Come funziona Lambda@Edge con richieste e risposte

Quando associ una CloudFront distribuzione a una funzione Lambda @Edge, CloudFront intercetta le richieste e le risposte nelle edge location. CloudFront È possibile eseguire funzioni Lambda quando si verificano i seguenti CloudFront eventi:

- Quando CloudFront riceve una richiesta da un visualizzatore (richiesta del visualizzatore)
- Prima CloudFront inoltra una richiesta all'origine (richiesta di origine)
- Quando CloudFront riceve una risposta dall'origine (origin response)
- Before CloudFront restituisce la risposta allo spettatore (risposta del visualizzatore)

Se si utilizza AWS WAF, la richiesta del visualizzatore Lambda @Edge viene eseguita dopo l'applicazione di qualsiasi AWS WAF regola.

Per ulteriori informazioni, consultare Utilizzo di richieste e risposte e Struttura dell'evento Lambda@Edge.

Modi per usare Lambda@Edge

L'elaborazione di Lambda @Edge con la tua CloudFront distribuzione Amazon può essere utilizzata in molti modi, come i seguenti esempi:

- Una funzione Lambda può ispezionare i cookie e riscriverli URLs in modo che gli utenti visualizzino diverse versioni di un sito per i test. A/B
- CloudFront può restituire oggetti diversi agli spettatori in base al dispositivo che stanno utilizzando controllando l'`User-Agent`intestazione, che include informazioni sui dispositivi. Ad esempio, CloudFront possono restituire immagini diverse in base alle dimensioni dello schermo del dispositivo. Allo stesso modo, la funzione potrebbe considerare il valore dell'`Referer`intestazione e CloudFront far sì che le immagini vengano restituite ai bot con la risoluzione più bassa disponibile.
- In alternativa, puoi controllare i cookie per altri criteri. Ad esempio, su un sito web di vendita al dettaglio che vende abbigliamento, se si utilizzano i cookie per indicare il colore scelto dall'utente per una giacca, una funzione Lambda può modificare la richiesta in CloudFront modo da restituire l'immagine di una giacca nel colore selezionato.
- Una funzione Lambda può generare risposte HTTP quando si verificano eventi di richiesta del CloudFront visualizzatore o di richiesta di origine.
- Una funzione può controllare le intestazioni o i token di autorizzazione e inserire un'intestazione per controllare l'accesso ai contenuti prima di CloudFront inoltrare la richiesta all'origine.
- Una funzione Lambda può anche effettuare chiamate di rete a risorse esterne per verificare le credenziali utente o recuperare ulteriore contenuto per personalizzare una risposta.

Per ulteriori informazioni, incluso codice di esempio, consulta Esempi di funzioni Lambda@Edge.

Per ulteriori informazioni sulla configurazione di Lambda@Edge nella console, consulta Tutorial: creazione di una funzione Lambda@Edge di base (console).

Nozioni di base sulle funzioni Lambda@Edge (console)

Con Lambda @Edge, puoi usare i CloudFront trigger per richiamare una funzione Lambda. Quando associ una CloudFront distribuzione a una funzione Lambda, CloudFront intercetta le richieste e le risposte nelle posizioni CloudFront periferiche ed esegue la funzione. Le funzioni Lambda possono migliorare la sicurezza o personalizzare le informazioni vicine ai visualizzatori per migliorare le prestazioni.

L'elenco seguente fornisce una panoramica di base su come creare e utilizzare le funzioni Lambda con. CloudFront

Panoramica: creazione e utilizzo di funzioni Lambda con CloudFront

1. Crea una funzione Lambda nella regione Stati Uniti orientali (Virginia settentrionale).
2. Salvare e pubblicare una versione numerata della funzione.

   Per apportare modifiche alla funzione è necessario modificare la versione $LATEST della funzione nella regione Stati Uniti orientali (N. Virginia). Quindi, prima di configurarlo per funzionare CloudFront, pubblicate una nuova versione numerata.
3. Associate la funzione a un comportamento CloudFront di distribuzione e cache. Specificate quindi uno o più CloudFront eventi (trigger) che causano l'esecuzione della funzione. Ad esempio, è possibile creare un trigger per l'esecuzione della funzione quando si CloudFront riceve una richiesta da un visualizzatore.
4. Quando si crea un trigger, Lambda crea repliche della funzione nelle posizioni AWS in tutto il mondo.

> **Tip**
>
> Per ulteriori informazioni, consultate la creazione e l'aggiornamento delle funzioni, la struttura degli eventi e l'aggiunta di CloudFront trigger. Puoi inoltre trovare ulteriori idee e ottenere esempi di codice in Esempi di funzioni Lambda@Edge.

Per un step-by-step tutorial, consultate il seguente argomento:

Argomenti

Tutorial: creazione di una funzione Lambda@Edge di base (console)

Questo tutorial mostra come iniziare a usare Lambda @Edge creando e configurando una funzione Node.js di esempio che viene eseguita in. CloudFront Questo esempio aggiunge intestazioni di sicurezza HTTP a una risposta quando CloudFront recupera un file. Questo può migliorare la sicurezza e la privacy di un sito web.

Per questo tutorial non è necessario avere un proprio sito web. Tuttavia, quando scegli di creare una soluzione Lambda@Edge, segui passaggi simili e scegli tra le stesse opzioni.

Argomenti

Fase 1: registrazione ad un Account AWS

Se non l'hai ancora fatto, registrati per ottenere un Account AWS. Per ulteriori informazioni, consulta Registrati per un Account AWS.

Fase 2: creare una distribuzione CloudFront

Prima di creare la funzione di esempio Lambda @Edge, è necessario disporre di un CloudFront ambiente con cui lavorare che includa un'origine da cui distribuire il contenuto.

Per questo esempio, crei una CloudFront distribuzione che utilizza un bucket Amazon S3 come origine per la distribuzione. Se disponi già di un ambiente da utilizzare, puoi saltare questa fase.

Per creare una CloudFront distribuzione con un'origine Amazon S3

1. Crea un bucket Amazon S3 con un file o due, ad esempio file di immagini, come contenuti di esempio. Se hai bisogno di aiuto, puoi procedere come descritto in Caricamento dei contenuti su Amazon S3. Assicurati di impostare le autorizzazioni per assegnare l'accesso pubblico in lettura agli oggetti nel bucket.
2. Crea una CloudFront distribuzione e aggiungi il tuo bucket S3 come origine, seguendo i passaggi in Creare una CloudFront distribuzione web. Se disponi già di una distribuzione, puoi aggiungere il bucket come origine di quella distribuzione.

> **Tip**
>
> Annota l'ID della tua distribuzione. Più avanti in questo tutorial, quando aggiungi un CloudFront trigger per la tua funzione, devi scegliere l'ID per la tua distribuzione in un elenco a discesa, ad esempio. `E653W22221KDDL`

Fase 3: creare la tua funzione

In questa fase, devi creare una funzione Lambda, a partire da un modello blueprint nella console Lambda. La funzione aggiunge il codice per aggiornare le intestazioni di sicurezza nella tua distribuzione CloudFront.

Come creare una funzione Lambda

1. Accedi a Console di gestione AWS e apri la console all' AWS Lambda indirizzo. https://console.aws.amazon.com/lambda/

> **Important**
>
> Assicurati di trovarti negli Stati Uniti orientali 1 (Virginia settentrionale) (Regione AWS us-east-1). È necessario essere in questa regione per creare funzioni Lambda@Edge.

2. Selezionare Create function (Crea funzione).
3. Nella pagina Crea funzione, scegli Usa un blueprint, quindi filtra i blueprint inserendoli nel campo di CloudFront ricerca. **`cloudfront`**

> **Note**
>
> CloudFront i blueprint sono disponibili solo nella regione US-east-1 (Virginia settentrionale) (us-east-1).

4. Scegli il blueprint Modifica intestazione risposta HTTP come modello per la funzione.
5. Immettere le seguenti informazioni sulla funzione:
   - Nome funzione: immetti un nome per la funzione.
   - Ruolo di esecuzione: scegli come impostare le autorizzazioni per la funzione. Per utilizzare il modello di policy di autorizzazione di base consigliato da Lambda @Edge, scegli Crea un nuovo ruolo dai AWS modelli di policy.
   - Nome ruolo: immetti un nome per il ruolo creato dal modello di policy.
   - Modelli di policy: Lambda aggiunge automaticamente i permessi del modello di policy Basic Lambda @Edge perché hai scelto un CloudFront blueprint come base per la tua funzione. Questo modello di policy aggiunge le autorizzazioni per i ruoli di esecuzione che consentono di CloudFront eseguire la funzione Lambda per te CloudFront in diverse località del mondo. Per ulteriori informazioni, consulta Configurazione di ruoli e autorizzazioni IAM per Lambda@Edge.
6. Scegli Crea funzione nella parte inferiore della pagina.
7. Nel riquadro Implementa in Lambda@Edge visualizzato, scegli Annulla. Per questo tutorial, devi modificare il codice della funzione prima di implementarla in Lambda@Edge.
8. Scorri fino alla sezione Origine del codice della pagina.
9. Sostituire il codice modello con una funzione che modifica le intestazioni di sicurezza restituite dall'origine. Ad esempio, puoi usare un codice simile a quanto segue:

```
'use strict';
export const handler = (event, context, callback) => {

    //Get contents of response
    const response = event.Records[0].cf.response;
    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. Scegli File, Salva per salvare il codice aggiornato.
11. Seleziona Implementa.

Passa alla sezione successiva per aggiungere un CloudFront trigger per eseguire la funzione.

Fase 4: Aggiungere un CloudFront trigger per eseguire la funzione

Ora che hai una funzione Lambda per aggiornare le intestazioni di sicurezza, configura il CloudFront trigger per eseguire la funzione per aggiungere le intestazioni in qualsiasi risposta CloudFront ricevuta dall'origine per la tua distribuzione.

Per configurare il CloudFront trigger per la tua funzione

1. Nella console Lambda, nella pagina Panoramica della funzione relativa alla funzione desiderata, scegli Aggiungi trigger.
2. Per la configurazione di Trigger, scegli CloudFront.
3. Scegli Implementa in Lambda@Edge.
4. Nel riquadro Deploy to Lambda @Edge, in CloudFront Configura trigger, inserisci le seguenti informazioni:

   - Distribuzione: l'ID di CloudFront distribuzione da associare alla funzione. Nell’elenco a discesa, scegli l’ID della distribuzione.
   - Comportamento cache: il comportamento cache da utilizzare con il trigger. Per questo esempio, lascia il valore impostato su *, che applica a tutte le richieste il comportamento cache predefinito della distribuzione. Per ulteriori informazioni, consulta Cache Behavior

Settings (Impostazioni del comportamento della cache) nell'argomento Riferimento a tutte le impostazioni di distribuzione.

- CloudFront evento: il trigger che specifica quando viene eseguita la funzione. Vogliamo che la funzione security headers venga eseguita ogni volta che CloudFront restituisce una risposta dall'origine. Nell'elenco a discesa, scegli Risposta origine. Per ulteriori informazioni, consulta Aggiunta di trigger per una funzione Lambda@Edge.

5. Seleziona la casella di controllo Conferma implementazione in Lambda@Edge.
6. Scegli Deploy per aggiungere il trigger e replicare la funzione in sedi in tutto il mondo. AWS
7. Attendi che la funzione venga replicata. Questo richiede in genere diversi minuti.

   È possibile controllare se la replica è terminata accedendo alla console CloudFront e visualizzando la distribuzione: Attendi che lo stato di distribuzione cambi da Implementazione in corso a una data e un'ora, il che significa che la funzione è stata replicata. Quindi segui la procedura nella sezione successiva per verificare che la funzione sia attiva.

Fase 5: verificare che la funzione venga eseguita

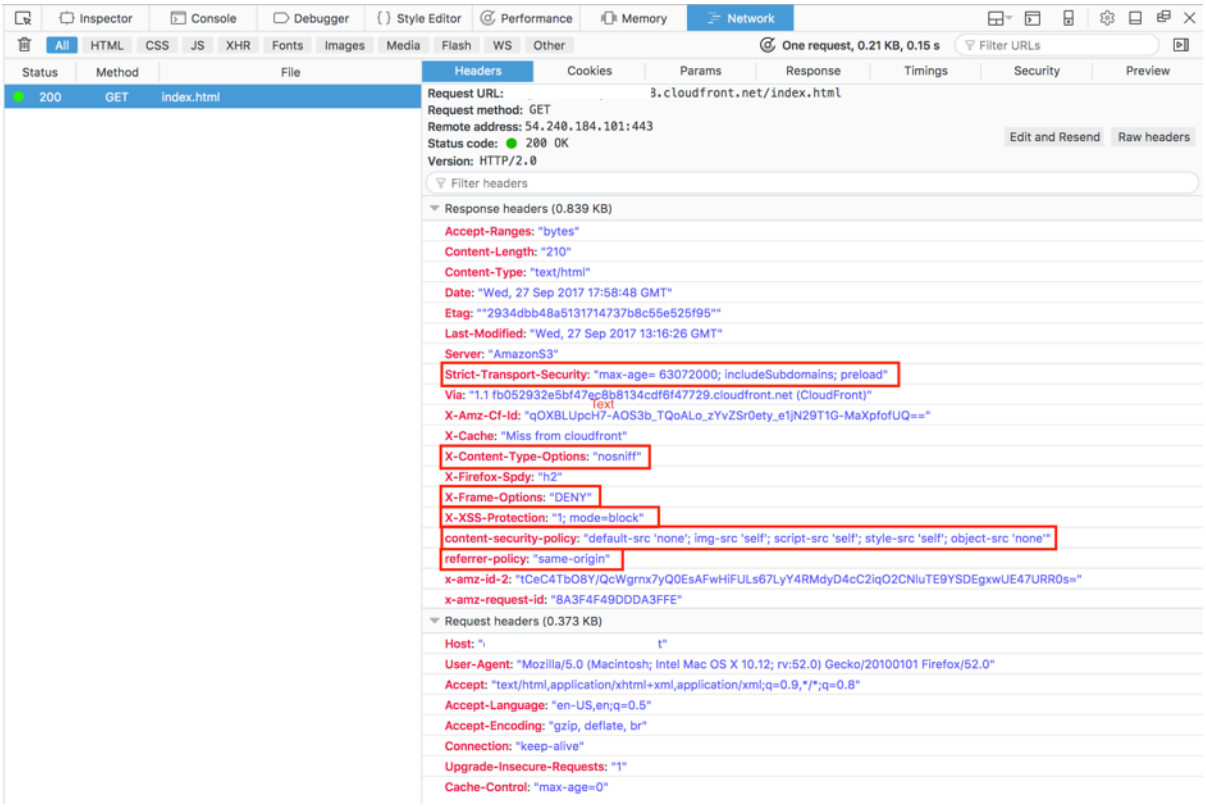
Ora che hai creato la funzione Lambda e configurato un trigger per eseguirla per una CloudFront distribuzione, assicurati che la funzione stia ottenendo ciò che ti aspetti. In questo esempio, controlliamo le intestazioni HTTP restituite da CloudFront, per assicurarci che vengano aggiunte le intestazioni di sicurezza.

Per verificare che la funzione Lambda@Edge aggiunga le intestazioni di sicurezza

1. In un browser, digita l'URL di un file del tuo S3 bucket. Ad esempio, puoi usare un URL simile a `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Per ulteriori informazioni sul nome di CloudFront dominio da utilizzare nell'URL del file, consulta. Personalizzazione del formato URL per i file in CloudFront
2. Apri la barra degli strumenti per sviluppatori del tuo browser Web. Ad esempio, nella finestra del browser in Chrome, apri il menu contestuale (pulsante destro del mouse) e scegli Inspect (Ispeziona).
3. Scegliere la scheda Network (Rete).
4. Ricarica la pagina per visualizzare l'immagine e quindi scegli una richiesta HTTP nel riquadro a sinistra. Vedrai le intestazioni HTTP visualizzate in un riquadro separato.

5. Scorri l'elenco delle intestazioni HTTP per verificare che le intestazioni di sicurezza previste vi siano incluse. Ad esempio, potresti vedere intestazioni simili a quelle mostrate nella schermata seguente:



Se le intestazioni di sicurezza sono incluse nel tuo elenco di intestazioni, è perfetto: hai creato la tua prima funzione Lambda@Edge. Se CloudFront restituisce errori o se ci sono altri problemi, continua con il passaggio successivo per risolverli.

Fase 6: risolvere i problemi

Se CloudFront restituisce errori o non aggiunge le intestazioni di sicurezza come previsto, puoi esaminare l'esecuzione della funzione esaminando Logs. CloudWatch Assicurati di utilizzare i log archiviati nella posizione più vicina alla AWS posizione in cui viene eseguita la funzione.

Ad esempio, se visualizzi il file da Londra, prova a cambiare la regione nella CloudWatch console in Europa (Londra).

Per esaminare i log CloudWatch per la funzione Lambda@Edge

1. Accedi a Console di gestione AWS e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.

2. Cambia regione nella posizione visualizzata quando visualizzi il file nel browser. Questo è dove la funzione è in esecuzione.
3. Nel riquadro sinistro, scegli Logs (Log) per visualizzare i log per la tua distribuzione.

Per ulteriori informazioni, consulta Monitoraggio delle metriche CloudFront con Amazon CloudWatch.

Fase 7: eliminare le risorse di esempio

Se hai creato un bucket Amazon S3 e una CloudFront distribuzione solo per questo tutorial, elimina le AWS risorse che hai allocato in modo da non addebitare più costi. Dopo aver eliminato le AWS risorse, i contenuti che hai aggiunto non sono più disponibili.

Attività

- Elimina il bucket S3
- Eliminazione della funzione Lambda
- Elimina la distribuzione CloudFront

Elimina il bucket S3

Prima di eliminare il bucket Amazon S3 in uso, accertarsi che le attività di registrazione siano disattivate per quel bucket. Altrimenti, AWS continua a scrivere i log nel bucket mentre lo elimini.

Per disattivare il log per un bucket

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il bucket, quindi Proprietà.
3. Da Properties (Proprietà), selezionare Log.
4. Deseleziona la casella Attivato.
5. Scegliere Save (Salva).

È possibile ora eliminare il bucket. Per ulteriori informazioni, consulta Eliminazione di un bucket nella Guida per l'utente della console di Amazon Simple Storage Service.

Eliminazione della funzione Lambda

Per istruzioni su come eliminare l’associazione della funzione Lambda e, facoltativamente, la funzione stessa, consulta Eliminazione delle funzioni e delle repliche Lambda@Edge.

Elimina la distribuzione CloudFront

Prima di eliminare una CloudFront distribuzione, è necessario disattivarla. Una distribuzione disattivata non è più funzionante e non accumula addebiti. Puoi attivare una distribuzione disattivata in qualsiasi momento. Una volta eliminata una distribuzione disattivata, non è più disponibile.

Per disabilitare ed eliminare una CloudFront distribuzione

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Selezionare la distribuzione che si vuole disattivare e scegliere Disable (Disattiva).
3. Quando viene richiesta la conferma, seleziona Sì, disattiva.
4. Selezionare la distribuzione disattivata e scegliere Delete (Elimina).
5. Quando viene richiesta la conferma, seleziona Sì, elimina.

Informazioni correlate

Ora che hai un'idea di come operano le funzioni Lambda@Edge, puoi approfondire i concetti consultando queste risorse:

- Esempi di funzioni Lambda@Edge
- Best practice di progettazione Lambda @Edge
- Ridurre la latenza e spostare l'elaborazione verso l'edge con Lambda @Edge

Configurazione di ruoli e autorizzazioni IAM per Lambda@Edge

Per configurare Lambda@Edge, devi disporre delle seguenti autorizzazioni e ruoli IAM per AWS Lambda:

- Autorizzazioni IAM: queste autorizzazioni ti consentono di creare la tua funzione Lambda e associarla alla tua distribuzione. CloudFront
- Un ruolo di esecuzione della funzione Lambda (ruolo IAM): i principali del servizio Lambda assumono questo ruolo per eseguire la funzione.
- Ruoli collegati ai servizi per Lambda @Edge: i ruoli collegati ai servizi consentono a specifiche funzioni Lambda di Servizi AWS replicare e abilitare l'utilizzo di file di registro. Regioni AWS CloudWatch CloudFront

Autorizzazioni IAM necessarie per associare le funzioni Lambda @Edge alle distribuzioni CloudFront

Oltre alle autorizzazioni IAM necessarie per Lambda, sono necessarie le seguenti autorizzazioni per associare le funzioni Lambda alle distribuzioni: CloudFront

- `lambda:GetFunction`: concede l'autorizzazione per ottenere informazioni di configurazione relative alla funzione Lambda e un URL pre-firmato per scaricare un file `.zip` contenente la funzione.
- `lambda:EnableReplication*`: concede l'autorizzazione alla policy delle risorse in modo che il servizio di replica Lambda possa ottenere il codice e la configurazione della funzione.
- `lambda:DisableReplication*`: concede l'autorizzazione alla policy delle risorse in modo che il servizio di replica Lambda possa eliminare la funzione.

  > **Important**
  >
  > È necessario aggiungere l'asterisco (*) alla fine delle azioni `lambda:EnableReplication*` e `lambda:DisableReplication*`.

- Per la risorsa, specificate l'ARN della versione della funzione che desiderate eseguire quando si verifica un CloudFront evento, come nell'esempio seguente:

  `arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2`

- `iam:CreateServiceLinkedRole`— Concede l'autorizzazione a creare un ruolo collegato al servizio che Lambda @Edge utilizza per replicare le funzioni Lambda. CloudFront Dopo aver configurato Lambda@Edge per la prima volta, il ruolo collegato al servizio viene creato automaticamente. Non è necessario aggiungere questa autorizzazione ad altre distribuzioni che utilizzano Lambda@Edge.

- `cloudfront:UpdateDistribution` o `cloudfront:CreateDistribution`: concede l'autorizzazione per aggiornare o creare una distribuzione.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Identity and Access Management per Amazon CloudFront
- Autorizzazioni di accesso alle risorse Lambda nella Guida per gli sviluppatori di AWS Lambda

Ruolo di esecuzione della funzione per i principali del servizio

È necessario creare un ruolo IAM che può essere assunto dai principali servizi `lambda.amazonaws.com` e `edgelambda.amazonaws.com` quando eseguono la funzione.

> **Tip**
>
> Quando crei la tua funzione nella console Lambda, puoi scegliere di creare un nuovo ruolo di esecuzione utilizzando un modello di AWS policy. Questa fase aggiunge automaticamente le autorizzazioni Lambda@Edge richieste per eseguire la funzione. Consulta Fase 5 del tutorial: creazione di una semplice funzione Lambda@Edge.

Per ulteriori informazioni sulla creazione manuale di un ruolo IAM, consulta Creazione di ruoli e collegamento di policy (console) nella Guida per l'utente IAM.

Example Esempio: policy di attendibilità del ruolo

Puoi aggiungere questo ruolo nella scheda Relazioni di attendibilità nella console IAM. Non aggiungere questa policy nella scheda Autorizzazioni.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "lambda.amazonaws.com",
               "edgelambda.amazonaws.com"
            ]
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```

Per ulteriori informazioni sulle autorizzazioni da concedere al ruolo di esecuzione, consulta Autorizzazioni di accesso alle risorse Lambda nella Guida per gli sviluppatori di AWS Lambda .

> **Note**
>
> - Per impostazione predefinita, ogni volta che un CloudFront evento attiva una funzione Lambda, i dati vengono scritti CloudWatch nei log. Se si desidera utilizzare questi registri, il ruolo di esecuzione richiede l'autorizzazione per scrivere dati nei registri. CloudWatch Puoi utilizzare il ruolo AWSLambdaBasicExecutionRole predefinito per concedere l'autorizzazione al ruolo di esecuzione.
>
>   Per ulteriori informazioni sui CloudWatch registri, vedere. the section called "Registri delle funzioni Edge"
> - Se il codice della funzione Lambda accede ad altre AWS risorse, ad esempio la lettura di un oggetto da un bucket S3, il ruolo di esecuzione necessita dell'autorizzazione per eseguire tale azione.

Ruoli collegati ai servizi per Lambda@Edge

Lambda@Edge usa un ruolo collegato al servizio IAM. Un ruolo collegato ai servizi è un tipo univoco di ruolo IAM collegato direttamente a un servizio. I ruoli collegati ai servizi sono definiti automaticamente dal servizio stesso e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Lambda@Edge usa i seguenti ruoli collegati al servizio IAM:

- AWSServiceRoleForLambdaReplicator: Lambda@Edge utilizza questo ruolo per consentire a Lambda@Edge di replicare funzioni su Regioni AWS.

  Quando aggiungi per la prima volta un trigger Lambda @Edge CloudFront, AWSServiceRoleForLambdaReplicator viene creato automaticamente un ruolo denominato per consentire a Lambda @Edge di replicare le funzioni. Regioni AWS Tale ruolo è obbligatorio per utilizzare le funzioni Lambda@Edge. L'aspetto dell'ARN per il ruolo AWSServiceRoleForLambdaReplicator è simile a quello dell'esempio seguente:

  ```
  arn:aws:iam::123456789012:role/aws-service-role/
  replicator.lambda.amazonaws.com/AWSServiceRoleForLambdaReplicator
  ```

- AWSServiceRoleForCloudFrontLogger— CloudFront utilizza questo ruolo per inviare file di registro in. CloudWatch Puoi utilizzare i file di log per eseguire il debug degli errori di convalida di Lambda@Edge.

  Il AWSServiceRoleForCloudFrontLogger ruolo viene creato automaticamente quando si aggiunge l'associazione di funzioni Lambda @Edge per consentire di inviare i file di CloudFront registro degli errori Lambda @Edge a. CloudWatch L'ARN per il ruolo AWSServiceRoleForCloudFrontLogger avrà il seguente aspetto:

  ```
  arn:aws:iam::account_number:role/aws-service-role/
  logger.cloudfront.amazonaws.com/AWSServiceRoleForCloudFrontLogger
  ```

Un ruolo collegato ai servizi semplifica la configurazione e l'utilizzo di Lambda@Edge perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Lambda@Edge definisce le autorizzazioni dei relativi ruoli associati ai servizi e solo Lambda@Edge potrà assumere i propri ruoli. Le autorizzazioni definite includono policy di trust e di autorizzazioni. Le policy di autorizzazioni non possono essere attribuite a nessun'altra entità IAM.

È necessario rimuovere tutte le risorse associate CloudFront o Lambda @Edge prima di poter eliminare un ruolo collegato al servizio. Questo aiuta a proteggere le risorse Lambda@Edge in modo da non rimuovere un ruolo collegato al servizio che è ancora necessario per accedere alle risorse attive.

Per ulteriori informazioni sui ruoli collegati al servizio, consulta Ruoli collegati ai servizi per CloudFront.

Autorizzazioni del ruolo collegato ai servizi per Lambda@Edge

Lambda@Edge usa due ruoli collegati ai servizi denominati AWSServiceRoleForLambdaReplicator e AWSServiceRoleForCloudFrontLogger. Nelle sezioni seguenti vengono descritte le autorizzazioni per ognuno di questi ruoli.

Indice

Autorizzazioni del ruolo collegato ai servizi per Lambda Replicator

Questo ruolo collegato al servizio consente a Lambda di replicare le funzioni Lambda@Edge su Regioni AWS.

Ai fini dell'assunzione del ruolo AWSServiceRoleForLambdaReplicator, il ruolo collegato ai servizi `replicator.lambda.amazonaws.com`considera attendibile il servizio.

La policy delle autorizzazioni del ruolo consente a Lambda@Edge di eseguire le seguenti operazioni sulle risorse specificate:

- `lambda:CreateFunction` - `arn:aws:lambda:*:*:function:*`
- `lambda:DeleteFunction` - `arn:aws:lambda:*:*:function:*`
- `lambda:DisableReplication` - `arn:aws:lambda:*:*:function:*`
- `iam:PassRole` - `all AWS resources`
- `cloudfront:ListDistributionsByLambdaFunction` - `all AWS resources`

Autorizzazioni relative ai ruoli collegati ai servizi per logger CloudFront

Questo ruolo collegato al servizio consente di CloudFront inviare file di registro in CloudWatch modo da poter eseguire il debug degli errori di convalida Lambda @Edge.

Ai fini dell'assunzione del ruolo AWSServiceRoleForCloudFrontLogger, il ruolo collegato ai servizi `logger.cloudfront.amazonaws.com`considera attendibile il servizio.

La policy delle autorizzazioni del ruolo consente a Lambda@Edge di eseguire le seguenti azioni sulla risorsa `arn:aws:logs:*:*:log-group:/aws/cloudfront/*` specificata:

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di eliminare ruoli Lambda@Edge collegati ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente IAM.

Creazione di ruoli collegati ai servizi per Lambda@Edge

In genere non si creano manualmente i ruoli collegati ai servizi per Lambda@Edge. Il servizio crea i ruoli automaticamente nei seguenti casi:

- Quando si crea un trigger per la prima volta, il servizio crea il ruolo AWSServiceRoleForLambdaReplicator (se non esiste già). Questo ruolo consente a Lambda di replicare le funzioni Lambda@Edge su Regioni AWS.

  Se lo elimini, il ruolo collegato ai servizi verrà creato nuovamente quando aggiungi un nuovo trigger per Lambda@Edge in una distribuzione.
- Quando aggiorni o crei una CloudFront distribuzione con un'associazione Lambda @Edge, il servizio crea il AWSServiceRoleForCloudFrontLogger ruolo (se il ruolo non esiste già). Questo ruolo consente di CloudFront inviare i file di registro a CloudWatch.

  Se elimini il ruolo collegato al servizio, il ruolo verrà creato nuovamente quando aggiorni o crei una CloudFront distribuzione con un'associazione Lambda @Edge.

Per creare manualmente questi ruoli collegati ai servizi, puoi eseguire i seguenti comandi (): AWS Command Line Interface AWS CLI

Per creare il ruolo AWSServiceRoleForLambdaReplicator

- Esegui il comando seguente.

```
aws iam create-service-linked-role --aws-service-name
 replicator.lambda.amazonaws.com
```

Per creare il ruolo AWSServiceRoleForCloudFrontLogger

- Esegui il comando seguente.

```
aws iam create-service-linked-role --aws-service-name
 logger.cloudfront.amazonaws.com
```

Modifica dei ruoli Lambda@Edge collegati ai servizi

Lambda@Edge non consente di modificare i ruoli collegati al servizio AWSServiceRoleForLambdaReplicator o AWSServiceRoleForCloudFrontLogger. Dopo che è stato creato un ruolo collegato al servizio, non puoi modificare il nome del ruolo perché varie entità possono farvi riferimento. Puoi tuttavia utilizzare IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Supportato Regioni AWS per i ruoli collegati ai servizi Lambda @Edge

CloudFront supporta l'utilizzo di ruoli collegati ai servizi per Lambda @Edge nei seguenti casi: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale) – `us-east-1`
- Stati Uniti orientali (Ohio) – `us-east-2`
- Stati Uniti occidentali (California settentrionale) – `us-west-1`
- Stati Uniti occidentali (Oregon) – `us-west-2`
- Asia Pacifico (Mumbai) – `ap-south-1`
- Asia Pacifico (Seul) - `ap-northeast-2`
- Asia Pacifico (Singapore) – `ap-southeast-1`
- Asia Pacifico (Sydney) - `ap-southeast-2`
- Asia Pacifico (Tokyo) - `ap-northeast-1`
- Europe (Francoforte) – `eu-central-1`
- Europa (Irlanda) – `eu-west-1`
- Europe (Londra) – `eu-west-2`
- Sud America (San Paolo) – `sa-east-1`

Scrivere e creare una funzione Lambda@Edge

Per usare Lambda@Edge, scrivi il codice per la funzione AWS Lambda . Per aiutarti a scrivere funzioni Lambda@Edge, consulta le seguenti risorse:

- Struttura dell'evento Lambda@Edge: comprendere la struttura degli eventi da utilizzare con Lambda@Edge.

- Esempi di funzioni Lambda@Edge— Funzioni di esempio, come il A/B test e la generazione di un reindirizzamento HTTP.

Il modello di programmazione per l'utilizzo di Node.js o Python con Lambda@Edge corrisponde a quello relativo all'utilizzo di Lambda in una Regione AWS. Per ulteriori informazioni, consulta Creazione di funzioni Lambda con Node.js o Creazione di funzioni Lambda con Python nella Guida per gli sviluppatori di AWS Lambda .

Nella funzione Lambda@Edge, includi il parametro `callback` e restituisci l'oggetto applicabile per gli eventi di richiesta o di risposta:

- Eventi di richiesta - È necessario includere l'oggetto `cf.request` nella risposta.

  Se si sta generando una risposta, includere l'oggetto `cf.response` nella risposta. Per ulteriori informazioni, consulta Generazione di risposte HTTP in trigger di richiesta.
- Eventi di risposta - È necessario includere l'oggetto `cf.response` nella risposta.

Dopo aver scritto il codice personalizzato o aver utilizzato uno degli esempi, crea la funzione in Lambda. Per creare una funzione o modificarne una esistente, consulta i seguenti argomenti:

Argomenti

- Creazione di una funzione Lambda@Edge
- Modifica di una funzione Lambda

Dopo aver creato la funzione in Lambda, configuri Lambda per eseguire la funzione in base a CloudFront eventi specifici, chiamati trigger. Per ulteriori informazioni, consulta Aggiunta di trigger per una funzione Lambda@Edge.

Creazione di una funzione Lambda@Edge

AWS Lambda Per configurare l'esecuzione di funzioni Lambda basate su CloudFront eventi, segui questa procedura.

Per creare una funzione Lambda@Edge

1. Accedi a Console di gestione AWS e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Se si dispone già di una o più funzioni Lambda, selezionare Create function (Crea funzione).

Se non si dispone di funzioni, selezionare Get Started Now (Inizia subito).

3. Nell'elenco Regione nella parte superiore della pagina, scegliere Stati Uniti orientali (Virginia settentrionale).
4. Creare una funzione utilizzando il proprio codice o creare una funzione iniziando con un piano CloudFront .

   - Per creare una funzione utilizzando il proprio codice, selezionare Author from scratch (Crea da zero).
   - Per visualizzare un elenco di progetti per CloudFront, inserisci cloudfront nel campo del filtro, quindi scegli Invio.

     Se si individua un piano che si desidera utilizzare, scegliere il nome del piano.
5. Nella sezione Basic information (Informazioni di base), specificare i seguenti valori:

   a. Nome: immetti un nome per la funzione.

   b. Ruolo: per iniziare rapidamente, scegli Crea nuovo ruolo dai modelli. Puoi anche scegliere Scegli un ruolo esistente o Crea un ruolo personalizzato, quindi segui i prompt per completare le informazioni di questa sezione.

   c. Nome ruolo: immetti un nome per il ruolo.

   d. Modelli di policy: scegli le autorizzazioni Lambda Edge di base.
6. Se nella fase 4 si è scelto Author from scratch (Crea da zero), passare alla fase 7.

   Se hai scelto un blueprint nel passaggio 4, la sezione cloudfront ti consente di creare un trigger, che associa questa funzione a una cache in una distribuzione e in un evento. CloudFront CloudFront A questo punto è consigliabile selezionare Remove (Rimuovi) in modo che non sia disponibile un trigger per la funzione al momento della creazione. È possibile aggiungere trigger in un secondo momento.

   > **Tip**
   >
   > Prima di aggiungere trigger, ti consigliamo di eseguire il test e il debugging della funzione. Se aggiungi ora un trigger, la funzione verrà eseguita non appena creerai la funzione e terminerà la replica in diverse AWS località del mondo e verrà distribuita la distribuzione corrispondente.
7. Selezionare Create function (Crea funzione).

Lambda crea due versioni della funzione: $LATEST e Version 1 (Versione 1). È possibile modificare solo la versione $LATEST, ma inizialmente nella console viene visualizzata l'opzione Version 1 (Versione 1).

8. Per modificare la funzione, selezionare Version 1 (Versione 1) vicino alla parte superiore della pagina, sotto l'ARN per la funzione. Quindi, nella scheda Versions (Versioni), selezionare $LATEST. Se si torna alla funzione in un secondo momento, l'etichetta del pulsante è Qualifiers (Qualificatori).
9. Nella scheda Configuration (Configurazione), selezionare l'opzione di Code entry type (Tipo di immissione codice) applicabile. Quindi, seguire le istruzioni per modificare o caricare il codice.
10. Per Runtime, scegliere il valore in base al codice della funzione.
11. Nella sezione Tags (Tag), aggiungere gli eventuali tag applicabili.
12. Selezionare Actions (Operazioni), quindi Publish new version (Pubblica nuova versione).
13. Immetti una descrizione per la nuova versione della funzione.
14. Seleziona Publish (Pubblica).
15. Eseguire il test e il debugging della funzione. Per ulteriori informazioni sul test nella console Lambda, consulta Invocare una funzione Lambda utilizzando la console nella Guida per gli sviluppatori di AWS Lambda .
16. Quando sei pronto per l'esecuzione della funzione per CloudFront gli eventi, pubblica un'altra versione e modifica la funzione per aggiungere trigger. Per ulteriori informazioni, consulta Aggiunta di trigger per una funzione Lambda@Edge.

Modifica di una funzione Lambda

Dopo aver creato una funzione Lambda@Edge, puoi utilizzare la console Lambda per modificarla.

> **Note**
>
> - La versione originale è contrassegnata con l'etichetta $LATEST.
> - È possibile modificare solo la versione $LATEST.
> - Ogni volta che si modifica la versione $LATEST, è necessario pubblicare una nuova versione numerata.
> - Non è possibile creare trigger per $LATEST.

- Quando si pubblica una nuova versione di una funzione, Lambda non copia automaticamente i trigger dalla versione precedente in quella nuova. È necessario riprodurre i trigger per la nuova versione.
- Quando aggiungi un trigger per un CloudFront evento a una funzione, se esiste già un trigger per la stessa distribuzione, lo stesso comportamento della cache e lo stesso evento per una versione precedente della stessa funzione, Lambda elimina il trigger dalla versione precedente.
- Dopo aver apportato aggiornamenti a una CloudFront distribuzione, ad esempio aggiungendo i trigger, è necessario attendere che le modifiche si propaghino nelle posizioni periferiche prima che le funzioni specificate nei trigger funzionino.

Come modificare una funzione Lambda

1. Accedi Console di gestione AWS e apri la console all'indirizzo. AWS Lambda https://console.aws.amazon.com/lambda/
2. Nell'elenco Regione nella parte superiore della pagina, scegliere Stati Uniti orientali (Virginia settentrionale).
3. Nell’elenco di funzioni, scegli il nome della funzione.

   Per default, nella console viene visualizzata la versione $LATEST. È possibile visualizzare le versioni precedenti selezionando Qualifiers (Qualificatori), ma è possibile modificare solo la versione $LATEST.
4. Nella scheda Code (Codice), per Code entry type (Tipo di immissione codice), scegliere di modificare il codice nel browser, caricare un file .zip o un file da Amazon S3.
5. Selezionare Save (Salva) o Save and test (Salva ed esegui test).
6. Selezionare Actions (Operazioni), quindi Publish new version (Pubblica nuova versione).
7. Nella finestra di dialogo Publish new version from $LATEST (Pubblica nuova versione da $LATEST), immettere una descrizione della nuova versione. Questa descrizione viene visualizzata nell'elenco di versioni, insieme a un numero di versione generato automaticamente.
8. Seleziona Publish (Pubblica).

   La nuova versione diventa automaticamente la versione più recente. Il numero di versione viene visualizzato sulla Versione nell’angolo in alto a sinistra della pagina.

> **Note**
>
> Se non hai ancora aggiunto trigger per la funzione, consulta Aggiunta di trigger per una funzione Lambda@Edge.

9. Selezionare la scheda Triggers (Trigger).
10. Selezionare Add trigger (Aggiungi trigger).
11. Nella finestra di dialogo Add trigger (Aggiungi trigger), selezionare la casella punteggiata, quindi CloudFront.

> **Note**
>
> Se hai già creato uno o più trigger per una funzione, CloudFront è il servizio predefinito.

12. Specificare i seguenti valori per indicare quando si desidera che la funzione Lambda venga eseguita.
    a. ID distribuzione: scegli l'ID della distribuzione a cui aggiungere il trigger.
    b. Comportamento cache: scegli il comportamento cache che specifica gli oggetti sui quali eseguire la funzione.
    c. CloudFront evento: scegli l' CloudFront evento che causa l'esecuzione della funzione.
    d. Attiva trigger e replica: seleziona questa casella di controllo per fare in modo che Lambda replichi la funzione nelle Regioni AWS a livello globale.
13. Seleziona Invia.
14. Per aggiungere più trigger per questa funzione, ripetere le fasi da 10 a 13.

Per ulteriori informazioni sul test e il debug della funzione nella console Lambda, consulta Invocare una funzione Lambda utilizzando la console nella Guida per gli sviluppatori di AWS Lambda .

Quando sei pronto per l'esecuzione della funzione per CloudFront gli eventi, pubblica un'altra versione e modifica la funzione per aggiungere trigger. Per ulteriori informazioni, consulta Aggiunta di trigger per una funzione Lambda@Edge.

Aggiunta di trigger per una funzione Lambda@Edge

Un trigger Lambda @Edge è una combinazione di CloudFront distribuzione, comportamento della cache ed evento che causa l'esecuzione di una funzione. Ad esempio, puoi creare un trigger che causa l'esecuzione della funzione quando ricevi una richiesta CloudFront da un visualizzatore per uno specifico comportamento della cache che hai impostato per la tua distribuzione. È possibile specificare uno o più CloudFront trigger.

> **Tip**
>
> Quando si crea una CloudFront distribuzione, si specificano le impostazioni che indicano CloudFront come rispondere quando riceve richieste diverse. Per impostazioni predefinite si intende il comportamento cache predefinito per la distribuzione. È possibile impostare comportamenti aggiuntivi della cache che definiscono la modalità di CloudFront risposta in circostanze specifiche, ad esempio quando riceve una richiesta per un tipo di file specifico. Per ulteriori informazioni, consulta Cache Behavior Settings (Impostazioni del comportamento della cache).

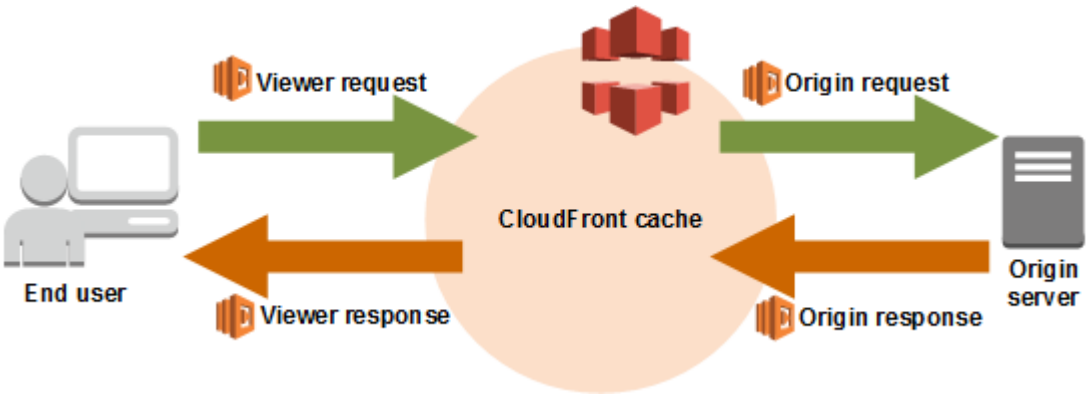
Quando crei una funzione Lambda per la prima volta, puoi specificare un solo trigger. Puoi aggiungere altri trigger alla stessa funzione in un secondo momento utilizzando la console Lambda o modificando la distribuzione nella CloudFront console.

- La console Lambda funziona bene se desideri aggiungere più trigger a una funzione per la stessa distribuzione. CloudFront
- La CloudFront console può essere migliore se desideri aggiungere trigger per più distribuzioni, perché è più facile trovare la distribuzione che desideri aggiornare. Puoi anche aggiornare altre CloudFront impostazioni contemporaneamente.

Argomenti

CloudFront eventi che possono attivare una funzione Lambda @Edge

Per ogni comportamento della cache in una CloudFront distribuzione Amazon, puoi aggiungere fino a quattro trigger (associazioni) che causano l'esecuzione di una funzione Lambda quando si verificano eventi CloudFront specifici. CloudFront i trigger possono essere basati su uno dei quattro CloudFront eventi, come mostrato nel diagramma seguente.



Gli CloudFront eventi che possono essere utilizzati per attivare le funzioni Lambda @Edge sono i seguenti:

Richiesta visualizzatore

La funzione viene eseguita quando CloudFront riceve una richiesta da un visualizzatore, prima di verificare se l'oggetto richiesto è nella CloudFront cache.

La funzione non viene eseguita nei seguenti casi:

- Quando si recupera una pagina di errore personalizzata.
- Quando reindirizza CloudFront automaticamente una richiesta HTTP a HTTPS (quando il valore di Viewer Protocol Policy (Policy protocollo visualizzatore) è Reindirizza HTTP a HTTPS).

Richiesta origine

La funzione viene eseguita solo quando CloudFront inoltra una richiesta all'origine. Quando l'oggetto richiesto è nella CloudFront cache, la funzione non viene eseguita.

Risposta origine

La funzione viene eseguita dopo aver CloudFront ricevuto una risposta dall'origine e prima di memorizzare nella cache l'oggetto nella risposta. La funzione verrà eseguita anche se l'origine restituisce un errore.

La funzione non viene eseguita nei seguenti casi:

- Quando il file richiesto è nella CloudFront cache e non è scaduto.
- Quando la risposta viene generata da una funzione che è stata attivata da un evento di richiesta origine

Risposta visualizzatore

La funzione viene eseguita prima di restituire il file richiesto al visualizzatore. Si noti che la funzione viene eseguita indipendentemente dal fatto che il file sia già presente nella CloudFront cache.

La funzione non viene eseguita nei seguenti casi:

- Quando l'origine restituisce un codice di stato HTTP 400 o superiore
- Quando viene restituita una pagina di errore personalizzata
- Quando la risposta viene generata da una funzione che è stata attivata da un evento di richiesta visualizzatore
- Quando reindirizza CloudFront automaticamente una richiesta HTTP a HTTPS (quando il valore di Viewer Protocol Policy (Policy protocollo visualizzatore) è Reindirizza HTTP a HTTPS).

Quando aggiungi più trigger allo stesso comportamento cache, puoi utilizzarli per eseguire la stessa funzione o eseguire funzioni differenti per ciascun trigger. Puoi anche associare la stessa funzione a più di una distribuzione.

> **Note**
>
> Quando un CloudFront evento attiva l'esecuzione di una funzione Lambda, la funzione deve terminare CloudFront prima di poter continuare.
> Ad esempio, se una funzione Lambda viene attivata da un evento di richiesta del CloudFront visualizzatore, CloudFront non restituirà una risposta al visualizzatore né inoltrerà la richiesta all'origine fino al termine dell'esecuzione della funzione Lambda.
> Ciò significa che ogni richiesta che attiva una funzione Lambda aumenta la latenza per la richiesta, pertanto è consigliabile che la funzione venga eseguita il più rapidamente possibile.

Scelta dell’evento per attivare la funzione

Quando decidi quale CloudFront evento utilizzare per attivare una funzione Lambda, considera quanto segue:

Voglio CloudFront memorizzare nella cache gli oggetti che vengono modificati da una funzione Lambda

Per memorizzare nella cache un oggetto che è stato modificato da una funzione Lambda in modo che CloudFront possa servire l'oggetto dall'edge location la prossima volta che viene richiesto, utilizzate l'evento origin request o origin response.

In questo modo, si riduce il carico sull'origine, la latenza per le richieste successive e il costo della richiamata di Lambda@Edge sulle richieste successive.

Ad esempio, se desideri aggiungere, rimuovere o modificare le intestazioni per gli oggetti restituiti dall'origine e desideri CloudFront inserire nella cache il risultato, utilizza l'evento origin response.

Desidero che la funzione venga eseguita per ogni richiesta

Per eseguire la funzione per ogni richiesta CloudFront ricevuta per la distribuzione, utilizzate gli eventi di richiesta del visualizzatore o di risposta del visualizzatore.

Gli eventi Origin request e origin response si verificano solo quando un oggetto richiesto non viene memorizzato nella cache in una edge location e CloudFront inoltra una richiesta all'origine.

Desidero che funzione modifichi la chiave della cache

Per modificare un valore utilizzato per il caching, utilizza l'evento di richiesta visualizzatore.

Ad esempio, se una funzione modifica l'URL per includere un abbreviazione di lingua nel percorso (ad esempio, perché l'utente ha scelto il linguaggio da un elenco a discesa), utilizza l'evento di richiesta visualizzatore:

- URL nella richiesta del visualizzatore: index.html https://example.com/en/
- URL se la richiesta proviene da un indirizzo IP in Germaniahttps://example.com/de/: index.html

Puoi anche utilizzare l'evento di richiesta visualizzatore se stai eseguendo il caching in base a cookie o intestazioni di richiesta.

> **Note**
>
> Se la funzione modifica i cookie o le intestazioni, configurate in modo CloudFront da inoltrare la parte pertinente della richiesta all'origine. Per ulteriori informazioni, consulta i seguenti argomenti:
>
> - Caching dei contenuti basati su cookie
> - Caching dei contenuti in base alle intestazioni di richiesta

La funzione influisce sulla risposta dall'origine

Per modificare la richiesta in un modo che influisca sulla risposta dall'origine, utilizza l'evento di richiesta origine.

In genere, la maggior parte degli eventi di richiesta del visualizzatore non viene inoltrata all'origine. CloudFront risponde a una richiesta con un oggetto già presente nella cache edge. Se la funzione modifica la richiesta in base a un evento di richiesta di origine, CloudFront memorizza nella cache la risposta alla richiesta di origine modificata.

Aggiunta di trigger a una funzione Lambda@Edge

Puoi usare la AWS Lambda console o la CloudFront console Amazon per aggiungere un trigger alla tua funzione Lambda @Edge.

> **Important**
>
> Puoi creare trigger solo per le versioni numerate della funzione (non per $LATEST).

Lambda console

Per aggiungere trigger per CloudFront eventi a una funzione Lambda @Edge

1. Accedi a Console di gestione AWS e apri la AWS Lambda console all'indirizzo. https://console.aws.amazon.com/lambda/
2. Nell'elenco Regione nella parte superiore della pagina, scegliere Stati Uniti orientali (Virginia settentrionale).
3. Nella pagina Functions (Funzioni), scegliere il nome della funzione per la quale si desidera aggiungere trigger.
4. Nella pagina Panoramica della funzione, scegli la scheda Versioni.
5. Selezionare la versione alla quale si desidera aggiungere trigger.

   Una volta selezionata la versione, il nome del pulsante viene modificato in Version: $LATEST (Versione: $LATEST) o Version: (Versione:) version number (numero della versione).
6. Selezionare la scheda Triggers (Trigger).
7. Selezionare Add trigger (Aggiungi trigger).

8. Per la configurazione di Trigger, scegli Seleziona una fonte**`cloudfront`**, inserisci, quindi scegli CloudFront.

   > **Note**
   >
   > Se hai già creato uno o più trigger, CloudFront è il servizio predefinito.

9. Specificare i seguenti valori per indicare quando si desidera che la funzione Lambda venga eseguita.

   a. Distribuzione: scegli la distribuzione a cui aggiungere il trigger.

   b. Comportamento cache: scegli il comportamento cache che specifica gli oggetti sui quali eseguire la funzione.

      > **Note**
      >
      > Se specifichi * per il comportamento cache, la funzione Lambda effettua la distribuzione al comportamento cache predefinito.

   c. CloudFront evento: scegli l'CloudFront evento che causa l'esecuzione della funzione.

   d. Includi corpo: seleziona questa casella di controllo per accedere al corpo della richiesta nella funzione.

   e. Conferma implementazione in Lambda@Edge: seleziona questa casella di controllo per fare in modo che AWS Lambda replichi la funzione nelle Regioni AWS a livello globale.

10. Scegliere Aggiungi.

    La funzione inizia a elaborare le richieste per gli CloudFront eventi specificati quando viene distribuita la CloudFront distribuzione aggiornata. Per determinare se una distribuzione viene distribuita, seleziona Distributions (Distribuzioni) nel riquadro di navigazione. Quando una distribuzione viene implementata, il valore della colonna Stato per la distribuzione cambia da Implementazione in corso alla data e ora dell'implementazione.

CloudFront console

Per aggiungere trigger per CloudFront eventi a una funzione Lambda @Edge

1. Ottieni l'ARN della funzione Lambda a cui desideri aggiungere dei trigger:

a. Accedi a Console di gestione AWS e apri la AWS Lambda console all'indirizzo. https://console.aws.amazon.com/lambda/

b. Nell'elenco delle regioni nella parte superiore della pagina, scegli US East (Virginia settentrionale).

c. Nell'elenco delle funzioni, scegli il nome della funzione a cui intendi aggiungere i trigger.

d. Nella pagina Panoramica della funzione, scegli la scheda Versioni e seleziona la versione numerata a cui aggiungere i trigger.

e. Scegli il pulsante Copia ARN per copiare l'ARN negli appunti. L'ARN per la funzione Lambda è simile a:

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2
```

Il numero alla fine (2 in questo esempio) è il numero di versione della funzione.

2. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
3. Nell'elenco delle distribuzioni, scegli l'ID della distribuzione a cui intendi aggiungere i trigger.
4. Scegli la scheda Behaviors (Comportamenti).
5. Seleziona il comportamento cache a cui aggiungere i trigger e scegli Modifica.
6. Per Associazioni funzione, nell'elenco Tipo di funzione, scegli Lambda@Edge per specificare quando eseguire la funzione: per richieste visualizzatore, risposte visualizzatore, richieste origine o risposte origine.

   Per ulteriori informazioni, consulta Scelta dell'evento per attivare la funzione.
7. Nella casella di testo ARN/Nome funzione, incolla l'ARN della funzione Lambda che desideri eseguire quando si verifica l'evento selezionato. Questo è il valore copiato dalla console Lambda.
8. Seleziona Includi corpo se desideri accedere al corpo della richiesta nella funzione.

   Si noti che non è necessario selezionare questa opzione se si desidera sostituire il corpo della richiesta.
9. Per eseguire la stessa funzione per più tipi di evento, ripeti le fasi 6 e 7.
10. Scegli Save changes (Salva modifiche).
11. Per aggiungere trigger a più comportamenti di cache per questa distribuzione, ripeti i passaggi da 5 a 10.

La funzione inizia a elaborare le richieste per gli CloudFront eventi specificati quando viene distribuita la CloudFront distribuzione aggiornata. Per determinare se una distribuzione viene distribuita, seleziona Distributions (Distribuzioni) nel riquadro di navigazione. Quando una distribuzione viene implementata, il valore della colonna Stato per la distribuzione cambia da Implementazione in corso alla data e ora dell'implementazione.

Test e debug delle funzioni Lambda@Edge

È importante testare il codice della funzione Lambda @Edge in modo indipendente, per assicurarsi che completi l'attività prevista, ed eseguire test di integrazione, per assicurarsi che la funzione funzioni correttamente. CloudFront

Durante i test di integrazione o dopo la distribuzione della funzione, potrebbe essere necessario eseguire il debug di CloudFront errori, come gli errori HTTP 5xx. Gli errori possono essere una risposta non valida restituita dalla funzione Lambda, gli errori di esecuzione quando la funzione è attivata, oppure gli errori dovuti al throttling di esecuzione da parte del servizio Lambda. Le sezioni in questo argomento condividono le strategie per determinare quale tipo di errore è il problema, e quindi quale procedura adottare per risolvere il problema.

> **Note**
>
> Quando esamini i file di CloudWatch registro o le metriche durante la risoluzione degli errori, tieni presente che vengono visualizzati o archiviati nella posizione Regione AWS più vicina alla posizione in cui è stata eseguita la funzione. Quindi, se hai un sito Web o un'applicazione Web con utenti nel Regno Unito e hai una funzione Lambda associata alla tua distribuzione, ad esempio, devi modificare la regione per visualizzare le CloudWatch metriche o i file di registro per Londra. Regione AWS Per ulteriori informazioni, consulta the section called "Determinazione della regione Lambda@Edge".

Argomenti

- Determinazione della regione Lambda@Edge
- Determina se il tuo account invia i log a CloudWatch

Test delle funzioni Lambda@Edge

Sono disponibili due fasi per il test della funzione Lambda: test autonomo e test di integrazione.

Test di funzionalità autonoma

Prima di aggiungere la funzione Lambda CloudFront, assicurati di testarla prima utilizzando le funzionalità di test nella console Lambda o utilizzando altri metodi. Per ulteriori informazioni sul test nella console Lambda, consulta Invocare una funzione Lambda utilizzando la console nella Guida per gli sviluppatori di AWS Lambda .

Verifica il funzionamento della tua funzione in CloudFront

È importante completare i test di integrazione, in cui la funzione è associata a una distribuzione ed è eseguita in base a un CloudFront evento. Verifica che la funzione sia attivata per l'evento corretto e restituisca una risposta valida e corretta per CloudFront. Ad esempio, verifica che la struttura dell'evento sia corretta, che siano incluse solo le intestazioni valide e così via.

Mentre esegui il test di integrazione con la tua funzione nella console Lambda, fai riferimento ai passaggi del tutorial Lambda @Edge mentre modifichi il codice o cambi il trigger che chiama CloudFront la tua funzione. Ad esempio, assicurati che si stia utilizzando una versione numerata della tua funzione, come descritto in questa fase del tutorial: Fase 4: Aggiungere un CloudFront trigger per eseguire la funzione.

Mentre apporti modifiche e le distribuisci, tieni presente che ci vorranno diversi minuti prima che la funzione e i CloudFront trigger aggiornati si replichino in tutte le regioni. Questa operazione di solito richiede alcuni minuti, in alcuni casi fino a 15.

Puoi verificare se la replica è terminata accedendo alla CloudFront console e visualizzando la distribuzione.

Come verificare se l'implementazione della replica è terminata

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli il nome della distribuzione.

3. Controlla che lo stato della distribuzione torni da In Progress (In corso) a Deployed (Implementato), il che significa che la funzione è stata replicata. Quindi segui la procedura nella sezione successiva per verificare che la funzione sia attiva.

Tieni presente che il test nella console convalida solo la logica della funzione e non applica quote di servizio (precedentemente note come limiti) specifiche di Lambda@Edge.

Identifica gli errori della funzione Lambda @Edge in CloudFront

Dopo aver verificato il corretto funzionamento della logica della funzione, potresti continuare a visualizzare errori HTTP 5xx durante l'esecuzione della funzione. CloudFront Gli errori HTTP 5xx possono essere restituiti per diversi motivi, tra cui errori della funzione Lambda o altri problemi in. CloudFront

- Se utilizzi le funzioni Lambda @Edge, puoi utilizzare i grafici nella CloudFront console per individuare la causa dell'errore e quindi lavorare per correggerlo. Ad esempio, puoi vedere se gli errori HTTP 5xx sono causati da CloudFront o da funzioni Lambda e quindi, per funzioni specifiche, puoi visualizzare i file di registro correlati per esaminare il problema.
- Per risolvere gli errori HTTP in generale in CloudFront, consulta la procedura di risoluzione dei problemi nel seguente argomento:. Risoluzione dei problemi relativi ai codici di stato della risposta agli errori in CloudFront

Cosa causa gli errori della funzione Lambda @Edge in CloudFront

Ci sono vari motivi per cui una funzione Lambda potrebbe causare un errore HTTP 5xx e i passaggi di risoluzione dei problemi da eseguire variano a seconda del tipo di errore. Gli errori possono essere classificati come riportato di seguito:

Un errore di esecuzione della funzione Lambda

Si verifica un errore di esecuzione quando CloudFront non riceve una risposta da Lambda perché ci sono eccezioni non gestite nella funzione o c'è un errore nel codice. Ad esempio, se il codice include callback (Error).

Viene restituita una risposta alla funzione Lambda non valida a CloudFront

Dopo l'esecuzione della funzione, CloudFront riceve una risposta da Lambda. Si verifica un errore nel caso in cui la struttura dell'oggetto della risposta non è conforme a Struttura dell'evento Lambda@Edge, oppure la risposta contiene le intestazioni non valide o altri campi non validi.

L'esecuzione in CloudFront è limitata a causa delle quote del servizio Lambda (precedentemente note come limiti)

Il servizio Lambda limita le esecuzioni in ciascuna regione e restituisce un errore se si supera la quota. Per ulteriori informazioni, consulta Quote di Lambda@Edge.

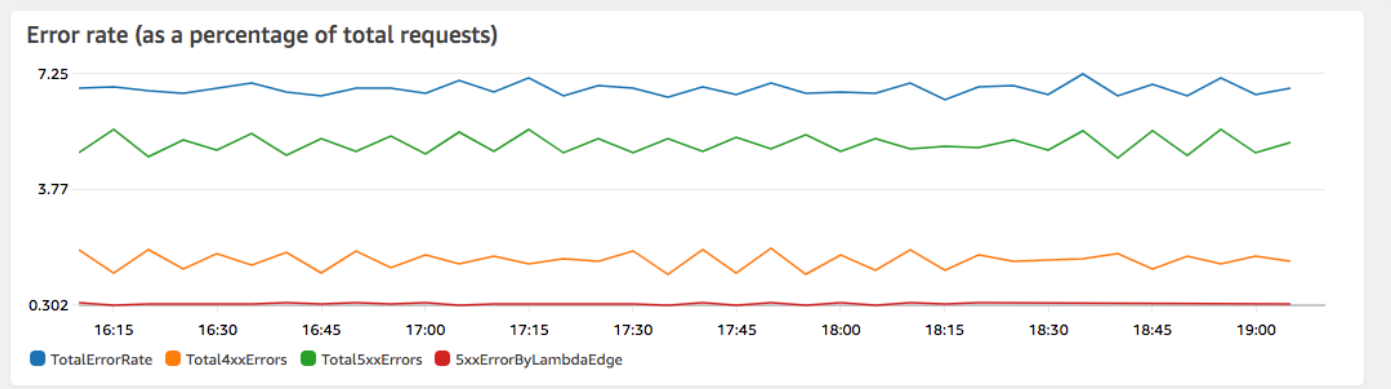
Come stabilire il tipo di errore

Per aiutarti a decidere dove concentrarti mentre esegui il debug e lavori per risolvere gli errori restituiti da CloudFront, è utile identificare il motivo per cui sta restituendo un errore HTTP. CloudFront Per iniziare, puoi utilizzare i grafici forniti nella sezione Monitoraggio della CloudFront console su. Console di gestione AWS Per ulteriori informazioni sulla visualizzazione dei grafici nella sezione Monitoraggio della CloudFront console, vedere. Monitoraggio delle metriche CloudFront con Amazon CloudWatch

I seguenti grafici possono essere particolarmente utili quando desideri stabilire se gli errori vengono restituiti da origini o da una funzione Lambda e limitare il tipo di problema quando si tratta di un errore di una funzione Lambda.

Grafico delle percentuali di errore

Uno dei grafici che puoi visualizzare nella scheda Overview (Panoramica) per ciascuna delle distribuzioni è un grafico Error rates (Percentuali di errore). Questo grafico visualizza la percentuale di errori come una percentuale di richieste totali pervenute alla distribuzione. Il grafico mostra la percentuale di errori totale, gli errori 4xx totali, gli errori 5xx totali e gli errori 5xx totali da funzioni Lambda. In base al tipo di errore e al volume, puoi eseguire fasi per individuare e risolvere la causa.



- Se sono visibili errori Lambda, puoi indagare ulteriormente osservando i tipi di errori specifici restituiti dalla funzione. La scheda Lambda@Edge errors (Errori Lambda@Edge) include grafici che classificano errori di funzioni in base al tipo per individuare il problema per una funzione specifica.
- Se riscontri CloudFront degli errori, puoi risolverli e correggere gli errori di origine o modificare la CloudFront configurazione. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi ai codici di stato della risposta agli errori in CloudFront.

Errori di esecuzione e grafici delle rispose di funzione non validi

La scheda Lambda@Edge errors (Errori Lambda@Edge) include grafici che classificano gli errori Lambda@Edge per una distribuzione specifica, in base al tipo. Ad esempio, un grafico mostra tutti gli errori di esecuzione in base alla Regione AWS.

Per semplificare la risoluzione dei problemi, puoi cercare problemi specifici aprendo ed esaminando i file di log per funzioni specifiche in base alla regione.

Come visualizzare i file di log per una funzione specifica in base alla regione

1. Nella scheda Errori Lambda@Edge, in Funzioni Lambda@Edge associate, scegli il nome della funzione, quindi seleziona Visualizza metriche.
2. Nella pagina con il nome della funzione, nell'angolo in alto a destra, scegli Visualizza log delle funzioni, quindi seleziona una regione.

   Ad esempio, se visualizzi problemi nel grafico Errori per la regione Stati Uniti occidentali (Oregon), scegli tale regione dall'elenco a discesa. Verrà aperta la CloudWatch console Amazon.
3. Nella CloudWatch console di quella regione, in Log stream, scegli un flusso di log per visualizzare gli eventi relativi alla funzione.

Inoltre, leggi le seguenti sezioni in questo capitolo per ulteriori suggerimenti sulla risoluzione dei problemi e la correzione degli errori.

Grafico di throttling

La scheda Lambda@Edge errors (Errori Lambda@Edge) include anche un grafico Throttles (Throttle). Talvolta, il servizio Lambda limita le invocazioni della funzione in base alla regione, se raggiungi la quota (precedentemente nota come limite) di simultaneità regionale. Se viene visualizzato un errore di superamento del limite, la tua funzione ha raggiunto una quota che il servizio Lambda impone sulle esecuzioni in una regione. Per ulteriori informazioni su come richiedere un aumento della quota, consulta Quote di Lambda@Edge.

Per un esempio su come utilizzare queste informazioni nella risoluzione di errori HTTP, consulta Quattro fasi per il debug della distribuzione di contenuti su AWS.

Risoluzione dei problemi relativi alle risposte non valide della funzione Lambda@Edge (errori di convalida)

Se si identifica che il problema è un errore di convalida Lambda, significa che la funzione Lambda sta restituendo una risposta non valida a. CloudFront Segui le indicazioni in questa sezione per prendere provvedimenti per rivedere la tua funzione e assicurarti che la risposta sia conforme ai requisiti. CloudFront

CloudFront convalida la risposta di una funzione Lambda in due modi:

- La risposta Lambda deve rispettare la struttura richiesta dell'oggetto. Tra gli esempi di errata struttura dell'oggetto figurano i seguenti: JSON non analizzabile, campi obbligatori mancanti

e un oggetto non valido nella risposta. Per ulteriori informazioni, consulta Struttura dell'evento Lambda@Edge.

- La risposta deve includere solo i valori di oggetti validi. Si verifica un errore se la risposta include un oggetto valido ma con valori non supportati. Alcuni esempi sono i seguenti: l'aggiunta o l'aggiornamento di intestazioni inserite nella blacklist o di sola lettura (consulta Restrizioni sulle funzioni edge) che superano la dimensione del corpo massima (consulta Restrizioni sulla dimensione della risposta generata nell'argomento Lambda@Edge Errori) e caratteri o valori non validi (vedi Struttura dell'evento Lambda@Edge).

Quando Lambda restituisce una risposta non valida a CloudFront, i messaggi di errore vengono scritti nei file di registro che vengono CloudFront inviati nella regione CloudWatch in cui è stata eseguita la funzione Lambda. È il comportamento predefinito a cui inviare i file di registro in CloudWatch caso di risposta non valida. Tuttavia, se hai associato una funzione Lambda a CloudFront prima del rilascio della funzionalità, potrebbe non essere abilitata per la tua funzione. Per ulteriori informazioni, consulta Stabilire se l'account invia i log a CloudWatch più avanti in questo argomento.

CloudFront invia i file di registro nella regione corrispondente a dove è stata eseguita la funzione, nel gruppo di log associato alla distribuzione. I gruppi di log hanno il seguente formato:`/aws/cloudfront/LambdaEdge/`*`DistributionId`*, *`DistributionId`* dov'è l'ID della tua distribuzione. Per determinare la regione in cui trovare i file di CloudWatch registro, consulta Determinazione della regione Lambda @Edge più avanti in questo argomento.

Se l'errore è riproducibile, puoi creare una nuova richiesta che genera l'errore e quindi trovare l'ID della richiesta in una CloudFront risposta non riuscita (`X-Amz-Cf-Id`intestazione) per individuare un singolo errore nei file di registro. La voce del file di log contiene informazioni che consentono di identificare perché l'errore viene restituito ed elenca anche l'id della richiesta Lambda corrispondente che permette di analizzare la causa principale nel contesto di una singola richiesta.

Se un errore è intermittente, è possibile utilizzare i log di CloudFront accesso per trovare l'ID della richiesta per una richiesta non riuscita e quindi cercare nei CloudWatch log i messaggi di errore corrispondenti. Per ulteriori informazioni, consulta la sezione precedente, Determinazione del Tipo di fallimento.

Risoluzione dei problemi relativi agli errori di esecuzione della funzione Lambda@Edge

Se il problema è un errore di esecuzione Lambda, può essere utile creare istruzioni di registrazione per le funzioni Lambda, scrivere messaggi nei file di CloudWatch registro che monitorano

l'esecuzione della funzione CloudFront e determinare se funziona come previsto. Quindi puoi cercare queste istruzioni nei file di CloudWatch registro per verificare che la tua funzione funzioni.

> **Note**
>
> Anche se non hai modificato la funzione Lambda@Edge, gli aggiornamenti per l'ambiente di esecuzione della funzione Lambda potrebbero influenzarla e potrebbero restituire un errore di esecuzione. Per informazioni sui test e la migrazione a una versione successiva, consulta Prossimi aggiornamenti dell'ambiente di esecuzione AWS Lambda e AWS Lambda @Edge.

Determinazione della regione Lambda@Edge

Per vedere le regioni in cui la tua funzione Lambda @Edge riceve traffico, visualizza le metriche per la funzione sulla CloudFront console su. Console di gestione AWS Le metriche vengono visualizzate per ogni regione. AWS Nella stessa pagina, puoi scegliere una regione e visualizzare i file di log per tale regione, in modo da analizzare i problemi. È necessario esaminare i file di CloudWatch registro nella AWS regione corretta per visualizzare i file di registro creati durante l' CloudFront esecuzione della funzione Lambda.

Per ulteriori informazioni sulla visualizzazione dei grafici nella sezione Monitoraggio della CloudFront console, consulta. Monitoraggio delle metriche CloudFront con Amazon CloudWatch

Determina se il tuo account invia i log a CloudWatch

Per impostazione predefinita, CloudFront abilita la registrazione delle risposte della funzione Lambda non valide e invia i file di registro utilizzando uno dei. CloudWatch Ruoli collegati ai servizi per Lambda@Edge Se hai funzioni Lambda @Edge che hai aggiunto CloudFront prima del rilascio della funzionalità di registro delle risposte della funzione Lambda non valida, la registrazione viene abilitata al successivo aggiornamento della configurazione Lambda @Edge, ad esempio aggiungendo un trigger. CloudFront

Puoi verificare che l'invio dei file di registro a CloudWatch sia abilitato per il tuo account effettuando le seguenti operazioni:

- Controlla se i log vengono visualizzati in CloudWatch: assicurati di cercare nella regione in cui è stata eseguita la funzione Lambda @Edge. Per ulteriori informazioni, consulta Determinazione della regione Lambda@Edge.

- Verifica se il ruolo collegato al servizio correlato esiste nell'account in IAM: devi disporre del ruolo IAM `AWSServiceRoleForCloudFrontLogger` nell'account. Per ulteriori informazioni su questo ruolo, consulta Ruoli collegati ai servizi per Lambda@Edge.

Eliminazione delle funzioni e delle repliche Lambda@Edge

È possibile eliminare una funzione Lambda@Edge solo quando le repliche della funzione sono state eliminate da CloudFront. Le repliche di una funzione Lambda vengono eliminate automaticamente nei seguenti casi:

- Dopo aver rimosso l'ultima associazione della funzione da tutte le distribuzioni CloudFront. Se più di una distribuzione utilizza una funzione, le repliche vengono eliminate solo dopo aver rimosso l'associazione della funzione dall'ultima distribuzione.
- Dopo aver eliminato l'ultima distribuzione a cui era associata una funzione.

In genere, le repliche vengono eliminate entro poche ore. Non è possibile eliminare manualmente le repliche delle funzioni Lambda@Edge. Ciò consente di evitare una situazione in cui viene eliminata una replica che è ancora in uso, il che comporterebbe un errore.

> **Warning**
>
> Non creare applicazioni che utilizzano repliche di funzioni Lambda @Edge al di fuori di. CloudFront Queste repliche vengono eliminate quando le associazioni con le distribuzioni vengono rimosse o quando le distribuzioni stesse vengono eliminate. Pertanto, la replica da cui dipende un'applicazione esterna potrebbe essere rimossa senza l'emissione di un avviso, causando il mancato funzionamento dell'applicazione.

Per eliminare un'associazione di funzioni Lambda @Edge da una distribuzione CloudFront

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli l'ID della distribuzione con l'associazione della funzione Lambda@Edge da eliminare.
3. Scegli la scheda Behaviors (Comportamenti).
4. Seleziona il comportamento cache che dispone dell'associazione della funzione Lambda@Edge da eliminare e quindi scegli Modifica.

5. In Associazioni di funzioni, Tipo di funzione, scegli Nessuna associazione per eliminare l'associazione della funzione Lambda@Edge.
6. Scegli Save changes (Salva modifiche).

Dopo aver eliminato un'associazione di funzioni Lambda @Edge da una CloudFront distribuzione, puoi facoltativamente eliminare la funzione Lambda o la versione della funzione da. AWS Lambda Attendi alcune ore dopo aver eliminato l'associazione della funzione in modo che le repliche della funzione Lambda@Edge possano essere pulite. Successivamente, puoi eliminare la funzione utilizzando la console Lambda, l'API AWS CLI Lambda o un SDK. AWS

Puoi anche eliminare una versione specifica di una funzione Lambda se alla versione non è associata alcuna CloudFront distribuzione. Dopo aver rimosso tutte le associazioni per una versione della funzione Lambda, attendi alcune ore. Quindi puoi eliminare la versione della funzione.

Struttura dell'evento Lambda@Edge

I seguenti argomenti descrivono gli oggetti evento di richiesta e risposta che CloudFront passano a una funzione Lambda @Edge quando viene attivata.

Argomenti

Selezione origine dinamica

Puoi utilizzare il modello di percorso in un comportamento cache per instradare richieste a un'origine, in base al percorso e al nome dell'oggetto richiesto, ad esempio `images/*.jpg`. Utilizzando Lambda@Edge, puoi anche instradare richieste a un'origine in base ad altre caratteristiche, ad esempio i valori nelle intestazioni di richiesta.

La selezione dinamica dell'origine può risultare utile in vari modi. Ad esempio, puoi distribuire richieste in più origini di aree geografiche differenti per facilitare il bilanciamento del carico globale. Oppure puoi instradare richieste in modo selettivo a diverse origini, ognuna delle quali svolge una funzione particolare: gestione di bot, ottimizzazione di SEO, autenticazione e così via. Per codici di esempio che illustrano come utilizzare questa funzionalità, consulta Esempi di selezione dinamica dell'origine in funzione del contenuto.

Nell'evento CloudFront origin request, l'`origin`oggetto nella struttura degli eventi contiene informazioni sull'origine a cui verrebbe indirizzata la richiesta, in base al modello di percorso. Puoi aggiornare i valori nell'oggetto `origin` dell'origine per instradare una richiesta un'altra origine. Quando si aggiorna l'oggetto `origin`, non è necessario definire l'origine nella distribuzione. È inoltre possibile sostituire un oggetto di origine Amazon S3 con un oggetto di origine personalizzato e viceversa. Tuttavia, è possibile specificare solo una singola origine per richiesta; un'origine personalizzata o un'origine Amazon S3, ma non entrambe.

Richiedi Eventi

I seguenti argomenti mostrano la struttura dell'oggetto che CloudFront passa a una funzione Lambda per gli eventi di richiesta viewer e origin. Questi esempi mostrano una richiesta `GET` senza corpo. Dopo gli esempi è riportato un elenco di tutti i possibili campi negli eventi di richiesta di visualizzazione e origine.

Argomenti

- Richiesta visualizzatore di esempio
- Esempio di richiesta di origine
- Richiedi campi evento

Richiesta visualizzatore di esempio

L'esempio seguente mostra un oggetto evento richiesta visualizzatore.

```
{
  "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": "/"
        }
      }
    }
  ]
}
```

Esempio di richiesta di origine

L'esempio seguente mostra un oggetto evento richiesta 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,
              "responseCompletionTimeout": 30,
              "sslProtocols": [
                "TLSv1",
                "TLSv1.1",
```

```
                "TLSv1.2"
              ]
            }
          },
          "querystring": "",
          "uri": "/"
        }
      }
    }
  ]
}
```

Richiedi campi evento

I dati dell'oggetto evento di richiesta sono contenuti in due sottooggetti: `config` (`Records.cf.config`) e `request` (`Records.cf.request`). I seguenti elenchi descrivono i campi di ciascun oggetto secondario.

Campi nell'oggetto config

Nella seguente lista sono descritti i campi dell'oggetto `config` (`Records.cf.config`).

`distributionDomainName` (solo lettura)

Il nome di dominio della distribuzione associata alla richiesta.

`distributionID` (solo lettura)

L'ID della distribuzione associata alla richiesta.

`eventType` (solo lettura)

Il tipo di trigger associato alla richiesta: `viewer-request` o `origin-request`.

`requestId` (solo lettura)

Una stringa crittografata che identifica in modo univoco una richiesta. viewer-to-CloudFront Il valore `requestId` è visualizzato anche nei log di accesso di CloudFront come `x-edge-request-id`. Per ulteriori informazioni, consultare Registri di accesso (registri standard) e Campi di file di log.

Campi nell'oggetto richiesta

Nella seguente lista sono descritti i campi dell'oggetto `request` (`Records.cf.request`).

`clientIp` (solo lettura)

L'indirizzo IP del visualizzatore che ha effettuato la richiesta. Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico per inviare la richiesta, il valore è l'indirizzo IP del proxy o del sistema di bilanciamento del carico.

intestazioni (lettura/scrittura)

Le intestazioni nella richiesta. Tieni presente quanto segue:

- Le chiavi nell'oggetto `headers` sono versioni in minuscolo di nomi di intestazione HTTP standard. L'utilizzo di chiavi in minuscolo fornisce accesso ai valori delle intestazioni senza distinzione tra maiuscole e minuscole.
- Ogni intestazione (ad esempio, `headers["accept"]` o `headers["host"]`) è una matrice di coppie chiave-valore. Per una determinata intestazione, la matrice contiene una coppia chiave-valore per ogni valore nella risposta generata.
- `key` contiene il nome con distinzione tra maiuscole e minuscole dell'intestazione come appare nella richiesta HTTP; ad esempio `Host`, `User-Agent`, `X-Forwarded-For`, `Cookie` e così via.
- `value` contiene il valore dell'intestazione come è apparso nella richiesta HTTP.
- Quando la funzione Lambda aggiunge o modifica le intestazioni di richiesta e non si include il campo di intestazione `key`, Lambda @Edge inserisce automaticamente un'intestazione `key` utilizzando il nome dell'intestazione fornito. Indipendentemente dalla formattazione del nome dell'intestazione, la chiave dell'intestazione automaticamente inserita sarà formattata con iniziale maiuscola per tutte le parti, separate da trattini (-).

  Ad esempio, è possibile aggiungere un'intestazione come quella seguente, senza una chiave dell'intestazione: `key`

  ```
  "user-agent": [
    {
      "value": "ExampleCustomUserAgent/1.X.0"
    }
  ]
  ```

  In questo esempio, Lambda @Edge inserisce automaticamente `"key": "User-Agent"`.

Per informazioni sulle restrizioni di utilizzo delle intestazioni, consulta Restrizioni sulle funzioni edge.

`method` (solo lettura)

Metodo HTTP nella richiesta.

`querystring` (lettura/scrittura)

La stringa di query, se presente, nella richiesta. Se la richiesta non include una stringa di query, l'oggetto evento include comunque `querystring` con un valore vuoto. Per ulteriori informazioni sulle stringhe di query, vedi Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

`uri` (lettura/scrittura)

Il percorso relativo dell'oggetto richiesto. Se la funzione Lambda modifica il valore `uri`, annotare quanto segue:

- Il nuovo valore `uri` deve iniziare con una barra (/).
- Se una funzione modifica il valore `uri`, l'oggetto richiesto dal visualizzatore viene modificato.
- Se una funzione modifica il valore `uri`, il comportamento della cache per la richiesta o l'origine a cui la richiesta viene inoltrata non viene modificato.

`body` (lettura/scrittura)

Il corpo della richiesta HTTP. La struttura `body` può contenere i seguenti campi:

`inputTruncated` (solo lettura)

Un flag booleano che indica se l'organismo è stato troncato da Lambda@Edge. Per ulteriori informazioni, consulta Restrizioni sul corpo della richiesta con l'opzione Includi corpo.

`action` (lettura/scrittura)

L'operazione che si desidera richiedere con il corpo. Le opzioni per `action` sono le seguenti:

- `read-only:` Questa è l'impostazione predefinita. Quando viene restituita la risposta dalla funzione Lambda, se `action` è di sola lettura, Lambda@Edge ignora tutte le modifiche a `encoding` o `data`.
- `replace:` specificare questo quando si desidera sostituire il corpo inviato all'origine.

`encoding` (lettura/scrittura)

La codifica per il corpo. Quando Lambda@Edge espone il corpo alla funzione Lambda, converte per prima cosa il corpo nella codifica base64-encoding. Se scegli `replace` per

`action` per sostituire il corpo, è possibile decidere se utilizzare la codifica `base64` (questa è l'impostazione predefinita) o `text`. Se specifichi `encoding` come `base64` ma il corpo non è valido in base64, CloudFront restituisce un errore.

`data` (lettura/scrittura)

I contenuti del corpo della richiesta.

`origin` (lettura/scrittura) (solo eventi di origine)

L'origine a cui inviare la richiesta. La struttura `origin` deve contenere esattamente un'origine, che può essere un'origine personalizzata o un'origine Amazon S3.

A seconda del tipo di origine specificato (origini personalizzate o Amazon S3), è necessario specificare i seguenti campi nella richiesta:

`customHeaders` (lettura/scrittura) (origini personalizzate e Amazon S3)

(Facoltativo) Puoi includere intestazioni personalizzate con la richiesta specificando un nome di intestazione e una coppia di valori per ogni intestazione personalizzata. Non è possibile aggiungere intestazioni che non sono consentite e in `Records.cf.request.headers` un'intestazione con lo stesso nome non può essere presente. Le note sulle intestazioni di richiesta si applicano anche alle intestazioni personalizzate. Per ulteriori informazioni, consulta Intestazioni personalizzate che CloudFront non può aggiungere alle richieste di origine e Restrizioni sulle funzioni edge.

`domainName` (lettura/scrittura) (origini personalizzate e Amazon S3)

Il nome di dominio dell'origine. Il nome di dominio non può essere vuoto.

- Per origini personalizzate - specificare un nome di dominio DNS, ad esempio `www.example.com`. Il nome di dominio non può includere due punti (:) e non può essere un indirizzo IP. Il nome di dominio può contenere fino a 253 caratteri.
- Per origini Amazon S3: specificare il nome di dominio DNS del bucket Amazon S3, ad esempio `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. Il nome può contenere fino a 128 caratteri e deve essere tutto in minuscolo.

`path` (lettura/scrittura) (origini personalizzate e Amazon S3)

Il percorso di directory sul server di origine in cui la richiesta deve trovare il contenuto. Il percorso può iniziare con una barra (/) ma non può terminare con una barra (ad esempio, non può terminare con `example-path/`). Solo per le origini personalizzate, il percorso deve essere codificato con URL e avere una lunghezza massima di 255 caratteri.

`keepaliveTimeout` (lettura/scrittura) (solo origini personalizzate)

Per quanto tempo, in secondi, si CloudFront dovrebbe cercare di mantenere la connessione all'origine dopo aver ricevuto l'ultimo pacchetto della risposta. Il valore deve essere un numero compreso tra 1 e 120, inclusi.

`port` (lettura/scrittura) (solo origini personalizzate)

La porta a cui CloudFront deve connettersi all'origine personalizzata. La porta deve essere 80, 443 oppure un numero nell'intervallo 1024-65535, inclusi.

`protocol` (lettura/scrittura) (solo origini personalizzate)

Il protocollo di connessione da CloudFront utilizzare per la connessione all'origine. Il valore può essere `http` o `https`.

`readTimeout` (lettura/scrittura) (origini personalizzate e Amazon S3)

Quanto tempo, in secondi, CloudFront occorre attendere per ricevere una risposta dopo aver inviato una richiesta all'indirizzo di origine. Questo specifica anche quanto tempo CloudFront deve attendere dopo aver ricevuto un pacchetto di una risposta prima di ricevere il pacchetto successivo. Il valore deve essere un numero compreso tra 1 e 120, inclusi.

Se hai bisogno di una quota maggiore, consulta Timeout di risposta per origine.

`responseCompletionTimeout` (lettura/scrittura) (origini personalizzate e Amazon S3)

Il tempo (in secondi) in cui una richiesta dall' CloudFront origine può rimanere aperta e attendere una risposta. Se la risposta completa non viene ricevuta dall'origine entro quest'ora, CloudFront termina la connessione.

Il valore per `responseCompletionTimeout` deve essere maggiore o uguale al valore per `readTimeout`. Se imposti questo valore su 0, rimuove qualsiasi valore precedente impostato e torna al valore predefinito. Puoi anche ottenere lo stesso risultato eliminando il campo `responseCompletionTimeout` dalla richiesta evento.

`sslProtocols` (lettura/scrittura) (solo origini personalizzate)

Il SSL/TLS protocollo minimo che CloudFront è possibile utilizzare per stabilire una connessione HTTPS con l'origine. I valori possono essere uno dei seguenti: `TLSv1.2`, `TLSv1.1`, `TLSv1` o `SSLv3`.

`authMethod` (lettura/scrittura) (solo origini Amazon S3)

Se stai usando un'identità di accesso origine (OAI), imposta questo campo su `origin-access-identity`. Se non stai usando una OAI, impostalo su `none`. Se si imposta `authMethod` su `origin-access-identity`, ci sono diversi requisiti:

- È necessario specificare `region` (vedere il seguente campo).
- È necessario utilizzare lo stesso OAI quando si modifica la richiesta da un'origine Amazon S3 a un'altra.
- Non è possibile utilizzare una OAI quando si modifica la richiesta da un'origine personalizzata a un'origine Amazon S3.

> **Note**
>
> Questo campo non supporta il controllo dell'accesso all'origine (OAC).

`region` (lettura/scrittura) (solo origini Amazon S3)

La AWS regione del tuo bucket Amazon S3. Questo è necessario solo quando si imposta `authMethod` su `origin-access-identity`.

Eventi di risposta

I seguenti argomenti mostrano la struttura dell'oggetto che CloudFront passa a una funzione Lambda per gli eventi di risposta del visualizzatore e dell'origine. Dopo gli esempi c'è un elenco di tutti i campi possibili in eventi di risposta del visualizzatore e origine.

Argomenti

- Esempio di risposta all'origine
- Risposta del visualizzatore di esempio
- Campi eventi di risposta

Esempio di risposta all'origine

L'esempio seguente mostra un oggetto evento risposta 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,
              "responseCompletionTimeout": 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"
      }
    }
  }
```

```
  ]
}
```

Risposta del visualizzatore di esempio

Nell'esempio seguente viene illustrato un oggetto evento risposta visualizzatore.

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

Campi eventi di risposta

I dati dell'oggetto evento risposta sono contenuti in tre sottooggetti: `config` 8`Records.cf.config`), `request` (`Records.cf.request`) e `response` (`Records.cf.response`). Per ulteriori informazioni sui campi dell'oggetto richiesta, vedere Campi nell'oggetto richiesta. Gli elenchi seguenti descrivono i campi nei sottooggetti `config` e `response`.

Campi nell'oggetto config

Nella seguente lista sono descritti i campi dell'oggetto `config` (`Records.cf.config`).

`distributionDomainName` (solo lettura)

Il nome di dominio della distribuzione associata alla risposta.

`distributionID` (solo lettura)

L'ID della distribuzione associata alla risposta.

`eventType` (solo lettura)

Il tipo di trigger associato alla risposta: `origin-response` o `viewer-response`.

`requestId` (solo lettura)

Una stringa crittografata che identifica in modo univoco la viewer-to-CloudFront richiesta a cui è associata questa risposta. Il `requestId` valore appare anche nei registri di CloudFront accesso come. `x-edge-request-id` Per ulteriori informazioni, consultare Registri di accesso (registri standard) e Campi di file di log.

Campi nell'oggetto risposta

Nella seguente lista sono descritti i campi dell'oggetto `response` (`Records.cf.response`). Per informazioni sull'utilizzo di una funzione Lambda @Edge per generare una risposta HTTP, vedere Generazione di risposte HTTP in trigger di richiesta.

`headers` (lettura/scrittura)

Le intestazioni nella risposta. Tieni presente quanto segue:

- Le chiavi nell'oggetto `headers` sono versioni in minuscolo di nomi di intestazione HTTP standard. L'utilizzo di chiavi in minuscolo fornisce accesso ai valori delle intestazioni senza distinzione tra maiuscole e minuscole.
- Ogni intestazione (ad esempio, `headers["content-type"]` o `headers["content-length"]`) è una matrice di coppie chiave-valore. Per una determinata intestazione, la matrice contiene una coppia chiave-valore per ogni valore nella risposta generata.
- `key` contiene il nome con distinzione tra maiuscole e minuscole dell'intestazione come appare nella risposta HTTP; ad esempio `Content-Type`, `Content-Length`, `Cookie` e così via.
- `value` contiene il valore dell'intestazione come appare nella risposta HTTP.
- Quando la funzione Lambda aggiunge o modifica le intestazioni di risposta e non si include il campo di intestazione `key`, Lambda @Edge inserisce automaticamente un'intestazione `key` utilizzando il nome dell'intestazione fornito. Indipendentemente dalla formattazione del nome

dell'intestazione, la chiave dell'intestazione automaticamente inserita sarà formattata con iniziale maiuscola per tutte le parti, separate da trattini (-).

Ad esempio, è possibile aggiungere un'intestazione come quella seguente, senza una chiave dell'intestazione: `key`

```
"content-type": [
  {
    "value": "text/html;charset=UTF-8"
  }
]
```

In questo esempio, Lambda @Edge inserisce automaticamente `"key": "Content-Type"`.

Per informazioni sulle restrizioni di utilizzo delle intestazioni, consulta Restrizioni sulle funzioni edge.

`status`

Il codice di stato HTTP per la risposta.

`statusDescription`

Descrizione dello stato HTTP della risposta.

Utilizzo di richieste e risposte

Per utilizzare le richieste e le risposte di Lambda@Edge, consulta i seguenti argomenti:

Argomenti

- Utilizzo delle funzioni Lambda@Edge con failover di origine
- Generazione di risposte HTTP in trigger di richiesta
- Aggiornamento delle risposte HTTP nei trigger di risposta origine
- Accesso al corpo della richiesta scegliendo l'opzione includi corpo

Utilizzo delle funzioni Lambda@Edge con failover di origine

Puoi utilizzare le funzioni Lambda @Edge con le CloudFront distribuzioni che hai configurato con i gruppi di origine, ad esempio per il failover di origine che configuri per garantire un'elevata disponibilità. Per usare una funzione Lambda con un gruppo di origine, specifica la funzione

in una richiesta all'origine o di risposta di origine trigger per un gruppo di origine quando crei il comportamento cache.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Crea gruppi di origine: Creazione di un gruppo di origine
- Come funziona il failover di origine con Lambda@Edge: Utilizzo del failover di origine con le funzioni Lambda@Edge

Generazione di risposte HTTP in trigger di richiesta

Quando si CloudFront riceve una richiesta, è possibile utilizzare una funzione Lambda per generare una risposta HTTP che CloudFront ritorna direttamente al visualizzatore senza inoltrare la risposta all'origine. La generazione di risposte HTTP riduce il carico sull'origine e in genere riduce la latenza per il visualizzatore.

Alcuni scenari comuni per la generazione di risposte HTTP sono:

- Restituzione di una piccola pagina Web al visualizzatore
- Restituzione di un codice di stato HTTP 301 o 302 per reindirizzare l'utente a un'altra pagina Web
- Restituzione di un codice di stato HTTP 401 al visualizzatore quando l'utente non ha eseguito la procedura di autenticazione

Una funzione Lambda@Edge può generare una risposta HTTP quando si verificano i seguenti eventi di CloudFront:

Eventi di richiesta visualizzatore

Quando una funzione viene attivata da un evento di richiesta del visualizzatore, CloudFront restituisce la risposta al visualizzatore e non la memorizza nella cache.

Eventi di richiesta origine

Quando una funzione viene attivata da un evento di richiesta di origine, CloudFront verifica nella cache edge la presenza di una risposta precedentemente generata dalla funzione.

- Se la risposta è nella cache, la funzione non viene eseguita e CloudFront restituisce la risposta memorizzata nella cache al visualizzatore.
- Se la risposta non è nella cache, la funzione viene eseguita e CloudFront restituisce la risposta al visualizzatore e la memorizza nella cache.

Per vedere il codice di esempio per la generazione di risposte HTTP, consulta Esempi di funzioni Lambda@Edge. È inoltre possibile sostituire le risposte HTTP nei trigger di risposta. Per ulteriori informazioni, consulta Aggiornamento delle risposte HTTP nei trigger di risposta origine.

Modello di programmazione

Questa sezione descrive il modello di programmazione che consente di utilizzare Lambda@Edge per generare risposte HTTP.

Argomenti

- Oggetto Response
- Errori
- Campi obbligatori

Oggetto Response

La risposta che restituisci come parametro `result` del metodo `callback` deve avere la seguente struttura (nota che solo il campo `status` è obbligatorio).

```
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'oggetto di risposta può includere i seguenti valori:

body

Il corpo, se presente, che si desidera CloudFront restituire nella risposta generata.

`bodyEncoding`

La codifica per il valore che hai specificato in `body`. Le uniche codifiche valide sono `text` e `base64`. Se includete `body` nell'`response`oggetto ma lo omettete`bodyEncoding`, CloudFront considera il corpo come testo.

Se specifichi `bodyEncoding` come `base64`, ma il corpo non è valido in base64, CloudFront restituisce un errore.

`headers`

Intestazioni che desiderate CloudFront restituire nella risposta generata. Tenere presente quanto segue:

- Le chiavi nell'oggetto `headers` sono versioni in minuscolo di nomi di intestazione HTTP standard. L'utilizzo di chiavi in minuscolo fornisce accesso ai valori delle intestazioni senza distinzione tra maiuscole e minuscole.
- Ogni intestazione (ad esempio, `headers["accept"]` o `headers["host"]`) è una matrice di coppie chiave-valore. Per una determinata intestazione, la matrice contiene una coppia chiave-valore per ogni valore nella risposta generata.
- `key` (facoltativo) è il nome dell'intestazione con distinzione tra maiuscole e minuscole come visualizzato in una richiesta HTTP, ad esempio `accept` o `host`.
- Specifica `value` come valore dell'intestazione.
- Se non includi la chiave dell'intestazione parte della coppia chiave-valore, Lambda@Edge inserisce automaticamente una chiave dell'intestazione utilizzando il nome dell'intestazione che fornisci. Indipendentemente dalla formattazione del nome dell'intestazione, la chiave dell'intestazione automaticamente inserita sarà formattata con iniziale maiuscola per tutte le parti, separate da trattini (-).

  Ad esempio, è possibile aggiungere un'intestazione come quella seguente, senza una chiave dell'intestazione: `'content-type': [{ value: 'text/html;charset=UTF-8' }]`

  In questo esempio, Lambda@Edge crea la chiave dell'intestazione seguente: `Content-Type`.

Per informazioni sulle restrizioni di utilizzo delle intestazioni, consulta Restrizioni sulle funzioni edge.

`status`

Codice di stato HTTP . Fornisci il codice di stato come stringa. CloudFront utilizza il codice di stato fornito per quanto segue:

- Restituzione nella risposta
- Cache nella cache CloudFront edge, quando la risposta è stata generata da una funzione attivata da un evento di richiesta di origine
- Effettua il login CloudFront Registri di accesso (registri standard)

Se il valore `status` non è compreso tra 200 e 599, CloudFront restituisce un errore al visualizzatore.

`statusDescription`

La descrizione che desideri CloudFront restituire nella risposta, da allegare al codice di stato HTTP. Non hai bisogno di utilizzare le descrizioni standard, ad esempio `OK` per un codice di stato HTTP 200.

Errori

Di seguito sono riportati possibili errori per le risposte HTTP generate.

La risposta contiene un corpo e specifica un codice di stato 204 (Nessun contenuto)

Quando una funzione viene attivata da una richiesta del visualizzatore, CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) al visualizzatore quando entrambe le seguenti condizioni sono vere:

- Il valore di `status` è 204 (Nessun contenuto)
- La risposta include un valore per `body`

Questo perché Lambda@Edge impone la restrizione facoltativa inclusa in RFC 2616, che indica che una risposta `HTTP 204` non deve contenere un corpo di messaggio.

Restrizioni relative alla dimensione della risposta generata

La dimensione massima di una risposta generata da una funzione Lambda dipende dall'evento che ha attivato la funzione:

- Eventi di richiesta visualizzatore - 40 KB
- Eventi di richiesta origine - 1 MB

Se la risposta è maggiore della dimensione consentita, CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) al visualizzatore.

Campi obbligatori

Il campo `status` è obbligatorio.

Tutti gli altri campi sono facoltativi.

Aggiornamento delle risposte HTTP nei trigger di risposta origine

Quando CloudFront riceve una risposta HTTP dal server di origine, se al comportamento della cache è associato un trigger di risposta all'origine, è possibile modificare la risposta HTTP per sovrascrivere ciò che è stato restituito dall'origine.

Alcuni scenari comuni per l'aggiornamento di risposte HTTP sono:

- Modifica dello stato per impostare un codice di stato HTTP 200 e creazione di contenuto di corpo statico da restituire al visualizzatore quando un'origine restituisce un codice di stato di errore (4xx e 5xx). Per il codice di esempio, consulta Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 200.
- Modifica dello stato per impostare un codice di stato HTTP 301 o 302, al fine di reindirizzare l'utente a un altro sito Web quando un'origine restituisce un codice di stato di errore (4xx e 5xx). Per il codice di esempio, consulta Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 302.

> **Note**
>
> La funzione deve restituire un valore di stato compreso tra `200` e `599` (incluso), altrimenti CloudFront restituisce un errore al visualizzatore.

È inoltre possibile sostituire le risposte HTTP negli eventi di richiesta origine e visualizzatore. Per ulteriori informazioni, consulta Generazione di risposte HTTP in trigger di richiesta.

Quando utilizzi la risposta HTTP, Lambda@Edge non espone il corpo restituito dal server di origine al trigger di risposta origine. Puoi generare un corpo di contenuto statico impostandolo sul valore desiderato oppure rimuovere il corpo nella funzione impostando un valore vuoto. Se non aggiorni il campo del corpo nella funzione, il corpo originale restituito dal server di origine viene restituito al visualizzatore.

Accesso al corpo della richiesta scegliendo l'opzione includi corpo

Ora puoi fare in modo che Lambda@Edge esponga il corpo in una richiesta per metodi HTTP con possibilità di scrittura (POST, PUT, DELETE e così via), in modo che tu possa accedervi dalla tua funzione Lambda. È possibile scegliere le autorizzazioni di accesso in sola lettura, oppure è possibile specificare che sarà possibile sostituire il corpo.

Per attivare questa opzione, scegli Include Body (Includi corpo) al momento della creazione di un trigger CloudFront per la tua funzione, per una richiesta di un visualizzatore o per un evento di richiesta del server di origine. Per ulteriori informazioni, consulta Aggiunta di trigger per una funzione Lambda@Edge o per ulteriori informazioni su come usare Include Body (Includi corpo) con la tua funzione, vedi Struttura dell'evento Lambda@Edge.

Tra gli scenari in cui è possibile utilizzare questa funzionalità figurano i seguenti:

- Elaborazione di moduli Web, ad esempio "Contattaci", senza l'invio di dati di input del cliente a server di origine.
- Raccolta di dati di beacon Web inviati dai browser dei visualizzatori e l'elaborazione al confine.

Per il codice di esempio, consulta Esempi di funzioni Lambda@Edge.

> **Note**
>
> Se il corpo della richiesta è di grandi dimensioni, Lambda@Edge lo tronca. Per informazioni dettagliate sulle dimensioni massime e il troncamento, consulta Restrizioni sul corpo della richiesta con l'opzione Includi corpo.

Esempi di funzioni Lambda@Edge

Guarda i seguenti esempi per utilizzare le funzioni Lambda con Amazon. CloudFront

> **Note**
>
> Se scegli Node.js 18 o versioni successive come runtime per la funzione Lambda@Edge, viene creato automaticamente un file `index.mjs`. Per utilizzare i seguenti esempi di codice, rinomina invece il file `index.mjs` in `index.js`.

Argomenti

Esempi generali

Gli esempi seguenti mostrano i modi più comuni di usare Lambda @Edge in. CloudFront

Argomenti

Esempio: test A/B

È possibile utilizzare l'esempio seguente per testare due diverse versioni di un'immagine senza creare reindirizzamenti o modificare l'URL. Questo esempio legge i cookie nella richiesta del visualizzatore e modifica l'URL della richiesta di conseguenza. Se il visualizzatore non invia un cookie con uno dei valori previsti, l'esempio assegna casualmente il visualizzatore a uno dei. URLs

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
```

Esempio: sostituzione di un'intestazione di risposta

L'esempio seguente mostra come modificare il valore di un'intestazione di risposta in base al valore di un'altra intestazione.

Node.js

```
export const handler = async (event) => {
    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()] = [{
            key: headerNameDst,
```

```
            value: headers[headerNameSrc.toLowerCase()][0].value,
        }];
        console.log(`Response header "${headerNameDst}" was set to ` +
                    `"${headers[headerNameDst.toLowerCase()][0].value}"`);
    }

    return response;
};
```

Python

```
import json

def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']
    headers = response['headers']

    header_name_src = 'X-Amz-Meta-Last-Modified'
    header_name_dst = 'Last-Modified'

    if headers.get(header_name_src.lower()):
        headers[header_name_dst.lower()] = [{
            'key': header_name_dst,
            'value': headers[header_name_src.lower()][0]['value']
        }]
        print(f'Response header "{header_name_dst}" was set to '
              f'"{headers[header_name_dst.lower()][0]["value"]}"')

    return response
```

Generazione di risposte: esempi

Gli esempi seguenti illustrano come è possibile usare Lambda@Edge per generare risposte.

Argomenti

- Esempio: distribuzione di contenuto statico (risposta generata)
- Esempio: generazione di un reindirizzamento HTTP (risposta generata)

Esempio: distribuzione di contenuto statico (risposta generata)

L'esempio seguente mostra come utilizzare una funzione Lambda per distribuire contenuto Web statico e quindi ridurre il carico sul server di origine e la latenza complessiva.

> **Note**
>
> È possibile generare risposte HTTP solo per eventi di richiesta origine e visualizzatore. Per ulteriori informazioni, consulta the section called “Generazione di risposte HTTP in trigger di richiesta”.
> È inoltre possibile sostituire o rimuovere il corpo della risposta HTTP negli eventi di richiesta origine. Per ulteriori informazioni, consulta the section called “Aggiornamento delle risposte HTTP nei trigger di risposta 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
```

Esempio: generazione di un reindirizzamento HTTP (risposta generata)

L'esempio seguente mostra come generare un reindirizzamento HTTP.

> **Note**
>
> È possibile generare risposte HTTP solo per eventi di richiesta origine e visualizzatore. Per ulteriori informazioni, consulta Generazione di risposte HTTP in trigger di richiesta.

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
```

Stringhe di query: esempi

Gli esempi seguenti illustrano i modi in cui è possibile usare Lambda@Edge con le stringhe di query.

Argomenti

- Esempio: aggiunta di un'intestazione in base a un parametro di stringa di query
- Esempio: normalizzazione dei parametri di stringa di query per migliorare il numero di riscontri nella cache
- Esempio: reindirizzamento di utenti non autenticati a un pagina di accesso

Esempio: aggiunta di un'intestazione in base a un parametro di stringa di query

L'esempio seguente mostra come ottenere la coppia chiave-valore di un parametro di stringa di query e aggiungere quindi un'intestazione in base a tali valori.

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
```

Esempio: normalizzazione dei parametri di stringa di query per migliorare il numero di riscontri nella cache

L'esempio seguente mostra come migliorare il rapporto di accesso alla cache apportando le seguenti modifiche alle stringhe di query prima di CloudFront inoltrare le richieste all'origine:

- Ordina alfabeticamente le coppie chiave-valore in base al nome del parametro
- Cambia le coppie chiave-valore da maiuscolo in minuscolo

Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

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
```

Esempio: reindirizzamento di utenti non autenticati a un pagina di accesso

L'esempio seguente mostra come reindirizzare gli utenti a una pagina di accesso se non hanno immesso le loro credenziali.

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
```

Esempi di personalizzazione del contenuto in base alle intestazioni del paese o del tipo di dispositivo

Gli esempi seguenti illustrano come utilizzare Lambda@Edge per personalizzare il comportamento in base alla posizione o al tipo di dispositivo usato dal visualizzatore.

Argomenti

- Esempio: reindirizzamento di richieste visualizzatore a un URL specifico di un paese
- Esempio: distribuzione di versioni differenti di un oggetto in base al dispositivo

Esempio: reindirizzamento di richieste visualizzatore a un URL specifico di un paese

L'esempio seguente mostra come generare una risposta di reindirizzamento HTTP con un URL specifico di un paese e restituire la risposta al visualizzatore. Ciò è utile quando intendi fornire risposte relative a un paese. Ad esempio:

- Se hai sottodomini specifici di un paese, ad esempio us.example.com e tw.example.com, puoi generare una risposta di reindirizzamento quando un visualizzatore richiede example.com.
- Se stai eseguendo lo streaming di video, ma non disponi dei diritti per lo streaming di contenuto in un determinato paese, puoi reindirizzare gli utenti in quel paese a una pagina che spiega perché non sono in grado di riprodurre il video.

Tieni presente quanto segue:

- Devi configurare la tua distribuzione in modo tale che la memorizzazione nella cache venga eseguita in base all'intestazione `CloudFront-Viewer-Country`. Per ulteriori informazioni, consulta Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate).
- CloudFront aggiunge l'`CloudFront-Viewer-Country`intestazione dopo l'evento di richiesta del visualizzatore. Per utilizzare questo esempio, devi creare un trigger per l'evento di richiesta 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
```

Esempio: distribuzione di versioni differenti di un oggetto in base al dispositivo

L'esempio seguente mostra come servire diverse versioni di un oggetto in base al tipo di dispositivo che l'utente sta utilizzando, ad esempio, un dispositivo mobile o un tablet. Tieni presente quanto segue:

- Devi configurare la tua distribuzione in modo tale che la memorizzazione nella cache venga eseguita in base all'intestazione `CloudFront-Is-*-Viewer`. Per ulteriori informazioni, consulta Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate).
- CloudFront aggiunge le `CloudFront-Is-*-Viewer` intestazioni dopo l'evento di richiesta del visualizzatore. Per utilizzare questo esempio, devi creare un trigger per l'evento di richiesta 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
```

Esempi di selezione dinamica dell'origine in funzione del contenuto

Gli esempi seguenti mostrano in che modo è possibile usare Lambda@Edge per l'instradamento a diverse origini in base alle informazioni nella richiesta.

Argomenti

Esempio: utilizzo di un trigger di richiesta origine per passare da un'origine personalizzata a un'origine Amazon S3

Questa funzione mostra come utilizzare un trigger di richiesta origine per passare da un'origine personalizzata a un'origine Amazon S3 da cui il contenuto viene recuperato, in base alle proprietà della richiesta.

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 = 'amzn-s3-demo-bucket.s3.amazonaws.com';

            /* Set S3 origin fields */
            request.origin = {
                s3: {
                    domainName: s3DomainName,
                    region: '',
                    authMethod: 'origin-access-identity',
                    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 = 'amzn-s3-demo-bucket.s3.amazonaws.com'

        # Set S3 origin fields
        request['origin'] = {
            's3': {
                'domainName': s3DomainName,
                'region': '',
                'authMethod': 'origin-access-identity',
                'path': '',
                'customHeaders': {}
```

```
            }
        }
        request['headers']['host'] = [{'key': 'host', 'value': s3DomainName}]
    return request
```

Esempio: utilizzo di un trigger di richiesta origine per modificare la regione dell'origine Amazon S3

Questa funzione mostra come utilizzare un trigger di richiesta origine per modificare l'origine Amazon S3 da cui viene recuperato il contenuto, in base alle proprietà della richiesta.

In questo esempio viene utilizzato il valore dell'intestazione `CloudFront-Viewer-Country` per aggiornare il nome di dominio del bucket S3 in un bucket in una regione più vicina al visualizzatore. Questa modifica può essere utile per vari motivi:

- Riduce le latenze quando la regione specificata è più vicina al paese del visualizzatore.
- Consente il controllo dei dati verificando che siano serviti da un'origine nello stesso paese in cui è stata effettuata la richiesta.

Per utilizzare questo esempio, è necessario eseguire le operazioni indicate di seguito:

- Configurare la tua distribuzione in modo tale che la memorizzazione nella cache venga eseguita in base all'intestazione `CloudFront-Viewer-Country`. Per ulteriori informazioni, consulta Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate).
- Crea un trigger per questa funzione nell'evento di richiesta di origine. CloudFrontaggiunge l'`CloudFront-Viewer-Country`intestazione dopo l'evento viewer request, quindi per usare questo esempio, devi assicurarti che la funzione venga eseguita per una richiesta di origine.

> **Note**
>
> Il codice di esempio seguente utilizza la stessa identità di accesso origine (OAI) per tutti i bucket S3 utilizzati per l'origine. Per ulteriori informazioni, consulta Identità di accesso 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 = `amzn-s3-demo-bucket-in-${region}.s3.
${region}.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 = 'amzn-s3-demo-bucket-in-{0}.s3.
{0}.amazonaws.com'.format(region)
            request['origin']['s3']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Esempio: utilizzo di un trigger di richiesta origine per passare da un'origine Amazon S3 a un'origine personalizzata

Questa funzione mostra come utilizzare un trigger di richiesta origine per passare all'origine personalizzata da cui viene recuperato il contenuto in base alle proprietà della richiesta.

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
```

Esempio: utilizzo di un trigger di richiesta origine per trasferire progressivamente il traffico da un bucket Amazon S3 a un altro

Questa funzione mostra come è possibile trasferire progressivamente il traffico da un bucket Amazon S3 a un altro in modo controllato.

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
```

Esempio: utilizzo di un trigger di richiesta origine per modificare il nome di dominio dell'origine in base all'intestazione del paese

Questa funzione mostra come è possibile modificare il nome di dominio dell'origine in base all'intestazione `CloudFront-Viewer-Country`, affinché il contenuto venga distribuito da un'origine più vicina al paese del visualizzatore.

L'implementazione di questa funzionalità per la distribuzione può offrire i seguenti vantaggi:

- Riduzione delle latenze quando la regione specificata è più vicina al paese del visualizzatore.
- Possibilità di controllare i dati verificando che siano distribuiti da un'origine nello stesso paese in cui è stata effettuata la richiesta.

Per attivare questa funzionalità, è necessario configurare la distribuzione in modo che la memorizzazione nella cache venga eseguita in base all'intestazione `CloudFront-Viewer-Country`. Per ulteriori informazioni, consulta the section called "Cache Based on Selected Request Headers (Cache in base a intestazioni di richiesta selezionate)".

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
```

Aggiornamento degli stati di errore: esempi

Gli esempi seguenti forniscono indicazioni su come è possibile usare Lambda@Edge per modificare lo stato di errore che viene restituito agli utenti.

Argomenti

- Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 200
- Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 302

Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 200

Questa funzione mostra come puoi aggiornare lo stato della risposta a 200 e generare contenuto di corpo statico da restituire al visualizzatore nel seguente scenario:

- La funzione viene attivata in una risposta di origine

- Lo stato delle risposta dal server di origine è codice di stato di errore (4xx e 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
```

Esempio: utilizzo di un trigger di risposta origine per aggiornare il codice di stato di errore a 302

Questa funzione mostra come puoi aggiornare il codice di stato HTTP a 302 per eseguire il reindirizzamento a un altro percorso (comportamento cache) che ha un'origine configurata differente. Tieni presente quanto segue:

- La funzione viene attivata in una risposta di origine
- Lo stato delle risposta dal server di origine è codice di stato di errore (4xx e 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
```

Accesso al corpo della richiesta: esempi

Gli esempi seguenti illustrano come utilizzare Lambda@Edge con le richieste POST.

> **Note**
>
> Per utilizzare questi esempi, è necessario abilitare l'opzione include body (Includi corpo) nell'associazione della funzione Lambda della distribuzione. Non è abilitato per impostazione predefinita.

- Per abilitare questa impostazione nella CloudFront console, seleziona la casella di controllo Include Body in the Lambda Function Association.
- Per abilitare questa impostazione nell' CloudFront API o con CloudFormation, imposta il `IncludeBody` campo su `true` in`LambdaFunctionAssociation`.

Argomenti

Esempio: utilizzo di un trigger di richiesta per leggere un modulo HTML

Questa funzione dimostra come è possibile elaborare il corpo di una richiesta POST generato da un modulo HTML (modulo Web), ad esempio "Contattaci". Ad esempio, potresti avere un modulo HTML come il seguente:

```
<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>
```

Per la funzione di esempio che segue, la funzione deve essere attivata in una richiesta di un visualizzatore CloudFront o di richiesta 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
```

Esempio: utilizzo di un trigger di richiesta per modificare un modulo HTML

Questa funzione dimostra come è possibile modificare il corpo di una richiesta POST generato da un modulo HTML (modulo Web). La funzione viene attivata in una richiesta del CloudFront visualizzatore o in una richiesta di 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)
```

Restrizioni sulle funzioni edge

Negli argomenti seguenti vengono descritte le restrizioni applicabili alle funzioni CloudFront e Lambda@Edge. Alcune restrizioni si applicano a tutte le funzioni edge, mentre altre si applicano solo alle funzioni CloudFront o Lambda@Edge.

Ogni argomento fornisce informazioni dettagliate sulle limitazioni e sui vincoli da considerare quando si sviluppano e si distribuiscono funzioni edge con CloudFront.

La comprensione di queste limitazioni aiuta a garantire che le funzioni edge funzionino come previsto e siano conformi alle funzionalità supportate.

Argomenti

Per ulteriori informazioni sulle quote (precedentemente denominate limiti), consulta Quote sulle funzioni CloudFront e Quote di Lambda@Edge.

Restrizioni su tutte le funzioni edge

Le restrizioni riportate di seguito si applicano a tutte le funzioni edge, sia le funzioni CloudFront che Lambda@Edge.

Argomenti

Account AWSProprietà di

Per associare una funzione edge a una distribuzione CloudFront, la funzione e la distribuzione devono essere di proprietà dello stesso Account AWS.

Combinazione delle funzioni CloudFront con Lambda@Edge

Per un determinato comportamento della cache, si applicano le seguenti restrizioni:

- Ogni tipo di evento (richiesta del visualizzatore, richiesta dell'origine, risposta dell'origine e risposta del visualizzatore) può avere una sola associazione di funzioni edge.
- Non è possibile combinare Funzioni CloudFront e Lambda@Edge negli eventi del visualizzatore (richiesta visualizzatore e risposta visualizzatore).

Sono consentite tutte le altre combinazioni di funzioni edge. Nella tabella seguente sono descritte le combinazioni consentite.

		Funzioni CloudFront	
		Richiesta visualizzatore	Risposta visualizzatore
Lambda@Edge	Richiesta visualizzatore	Non consentito	Non consentito
	Richiesta origine	Consentito	Consentito
	Risposta origine	Consentito	Consentito
	Risposta visualizzatore	Non consentito	Non consentito

Codici di stato HTTP

CloudFront non invoca funzioni edge per eventi di risposta visualizzatore se l'origine restituisce il codice di stato HTTP 400 o superiore.

Le funzioni Lambda@Edge per gli eventi di risposta di origine vengono richiamate per tutte le risposte di origine, incluso quando l'origine restituisce il codice di stato HTTP 400 o superiore. Per ulteriori informazioni, consulta Aggiornamento delle risposte HTTP nei trigger di risposta origine.

Intestazioni HTTP

Alcune intestazioni HTTP non sono consentite, il che significa che non sono esposte a funzioni edge e che le funzioni non possono aggiungerle. Altre intestazioni sono di sola lettura, il che significa che possono essere lette dalle funzioni ma non possono essere aggiunte, modificate o eliminate.

Argomenti

- Intestazioni non consentite
- Intestazioni di sola lettura

Intestazioni non consentite

Le seguenti intestazioni HTTP non sono esposte alle funzioni edge e le funzioni non possono aggiungerle. Se la tua funzione aggiunge una di queste intestazioni, la richiesta non ottiene la convalida di CloudFront e CloudFront restituisce il codice di stato HTTP 502 (Gateway non valido) al visualizzatore.

- `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`

Intestazioni di sola lettura

Le intestazioni di seguito sono di sola lettura. La funzione può leggerle e utilizzarle come input per la logica della funzione, ma non può modificarne i valori. Se la tua funzione aggiunge o modifica un'intestazione di sola lettura, la richiesta non ottiene la convalida di CloudFront e CloudFront restituisce il codice di stato HTTP 502 (Gateway non valido) al visualizzatore.

Intestazioni di sola lettura per eventi di richiesta del visualizzatore

Le seguenti intestazioni sono di sola lettura per gli eventi di richiesta del visualizzatore.

- `Content-Length`
- `Host`
- `Transfer-Encoding`
- `Via`

Intestazioni di sola lettura negli eventi di richiesta di origine (solo Lambda@Edge)

Le seguenti intestazioni sono di sola lettura negli eventi di richiesta di origine, che esistono solo in Lambda @Edge.

- `Accept-Encoding`
- `Content-Length`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Transfer-Encoding`
- `Via`

Intestazioni di sola lettura negli eventi di risposta di origine (solo Lambda@Edge)

Le seguenti intestazioni sono di sola lettura negli eventi di risposta di origine, che esistono solo in Lambda@Edge.

- `Transfer-Encoding`
- `Via`

Intestazioni di sola lettura per eventi di risposta del visualizzatore

Le seguenti intestazioni sono di sola lettura negli eventi di risposta del visualizzatore per Funzioni CloudFront e Lambda @Edge.

- `Warning`
- `Via`

Le seguenti intestazioni sono di sola lettura per gli eventi di risposta del visualizzatore per Lambda@Edge.

- `Content-Length`
- `Content-Encoding`
- `Transfer-Encoding`

Stringhe di query

Le restrizioni seguenti si applicano alle funzioni che leggono, aggiornano o creano una stringa di query in un URI di richiesta.

- (Solo Lambda@Edge) Per accedere alla stringa di query in una funzione di richiesta di origine o di risposta di origine, la policy della cache o la policy di richiesta di origine deve essere impostata su Tuttiper Stringhe di query.
- Una funzione può creare o aggiornare una stringa di query per gli eventi di richiesta del visualizzatore e richiesta di origine (gli eventi di richiesta origine esistono solo in Lambda@Edge).
- Una funzione può leggere una stringa di query ma non può crearne o aggiornarne una per gli eventi di risposta origine e di risposta del visualizzatore (gli eventi di risposta origine esistono solo in Lambda@Edge).

- Se una funzione crea o aggiorna una stringa di query, si applicano le seguenti restrizioni:
  - La stringa di query aggiornata non può includere spazi, caratteri di controllo o l'identificatore di frammento (#).
  - La dimensione totale dell'URI, compresa la stringa di query, deve essere inferiore a 8.192 caratteri.
  - Ti consigliamo di utilizzare la codifica percentuale per l'URI e la stringa di query. Per ulteriori informazioni, consulta Codifica di URI, stringa di query e intestazioni.

URI

Se una funzione modifica l'URI per una richiesta, il comportamento cache per la richiesta o l'origine a cui la richiesta viene inoltrata non viene modificato.

La dimensione totale dell'URI, compresa la stringa di query, deve essere inferiore a 8.192 caratteri.

Codifica di URI, stringa di query e intestazioni

I valori dell'URI, della stringa di query e delle intestazioni passati alle funzioni edge sono codificati UTF-8. La funzione deve utilizzare la codifica UTF-8 per i valori dell'URI, della stringa di query e delle intestazioni restituiti. La codifica percentuale è compatibile con la codifica UTF-8.

Nell'elenco seguente viene spiegato come CloudFront gestisce la codifica dell'URI, della stringa di query e delle intestazioni:

- Quando i valori nella richiesta sono codificati in UTF-8, CloudFront inoltra i valori alla tua funzione senza modificarli.
- Se i valori nella richiesta sono codificati in ISO-8859-1, CloudFront converte i valori in UTF-8 prima di inoltrarli alla funzione.
- Se i valori nella richiesta sono codificati utilizzando una qualsiasi altra codifica caratteri, CloudFront presuppone che siano codificati in ISO-8859-1 e prova a convertirli da ISO-8859-1 a UTF-8.

> **Important**
>
> I caratteri convertiti potrebbero essere un'interpretazione non accurata dei valori nella richiesta originale. In tal caso, una funzione o la tua origine potrebbe produrre un risultato inatteso.

I valori dell'URI, della stringa di query e delle intestazioni inoltrati da CloudFront all'origine dipendono dal fatto che una funzione modifichi i valori:

- Se una funzione non modifica l'URI, la stringa di query o le intestazioni, CloudFront inoltra i valori che ha ricevuto nella richiesta all'origine.
- Se una funzione non modifica l'URI, la stringa di query o l'intestazione, CloudFront inoltra i valori con codifica UTF-8.

Microsoft Smooth Streaming

Non è possibile utilizzare le funzioni edge con una distribuzione CloudFront utilizzata per lo streaming di file multimediali transcodificati in formato Microsoft Smooth Streaming.

Tagging

Non è possibile aggiungere tag alle funzioni edge. Per informazioni sull'applicazione di tag in CloudFront, consulta Tagging di una distribuzione.

Restrizioni sulle funzioni CloudFront

Alle funzioni CloudFront si applicano le seguenti restrizioni.

Indice

Per ulteriori informazioni sulle quote (in precedenza denominate limiti), consulta Quote sulle funzioni CloudFront .

Log

I log delle funzioni nelle funzioni CloudFront vengono troncati a 10 KB.

Corpo della richiesta

Le funzioni CloudFront non possono accedere al corpo della richiesta HTTP.

Utilizzo di credenziali temporanee con l'API KeyValueStore di CloudFront

Puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee (note anche come token di sessione). I token di sessione consentono di assumere temporaneamente un ruolo AWS Identity and Access Management (IAM) in modo da poter accedere ai Servizi AWS.

Per chiamare l'API KeyValueStore di CloudFront, utilizza un endpoint regionale in AWS STS per restituire un token di sessione versione 2. Se utilizzi l'endpoint globale per AWS STS (`sts.amazonaws.com`), AWS STS genererà un token di sessione versione 1, non supportato da Signature Version 4A (SigV4A). Di conseguenza, riceverai un errore di autenticazione.

Per chiamare l'API KeyValueStore di CloudFront, puoi utilizzare le seguenti opzioni:

AWS CLI e SDK AWS

Puoi configurare AWS CLI o un SDK AWS per utilizzare gli endpoint AWS STS regionali. Per ulteriori informazioni, consulta Endpoint regionali AWS STS nella Guida di riferimento agli strumenti e agli SDK AWS.

Per ulteriori informazioni sugli endpoint AWS STS disponibili, consulta Endpoint e regioni nella Guida per l'utente IAM.

SAML

Puoi configurare SAML per utilizzare gli endpoint AWS STS regionali. Per ulteriori informazioni, consulta il post del blog How to use regional SAML endpoints for failover.

API **`SetSecurityTokenServicePreferences`**

Invece di utilizzare un endpoint AWS STS regionale, puoi configurare l'endpoint globale per AWS STS restituire i token di sessione della versione 2. A tale scopo, utilizza l'operazione API SetSecurityTokenServicePreferences per configurare l'Account AWS.

Example Esempio: comando della CLI IAM

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

> **Tip**
>
> Ti consigliamo di utilizzare gli endpoint AWS STS regionali anziché questa opzione. Gli endpoint regionali offrono una maggiore disponibilità e scenari di failover.

Provider di identità personalizzato

Se utilizzi un provider di identità personalizzato che esegue la federazione e assume il ruolo, utilizza una delle opzioni precedenti per il sistema provider di identità principale responsabile della generazione del token di sessione.

Runtime

L'ambiente di runtime di Funzioni CloudFront non supporta la valutazione dinamica del codice e limita l'accesso alla rete, al file system, alle variabili di ambiente e ai timer. Per ulteriori informazioni, consulta Funzionalità con restrizioni.

> **Note**
>
> Per utilizzare KeyValueStore di CloudFront, la funzione CloudFront deve utilizzare JavaScript runtime 2.0.

Utilizzo di calcolo

Le funzioni CloudFront hanno un limite al tempo che possono impiegare per l'esecuzione, misurato come utilizzo di calcolo. L'utilizzo di calcolo è un numero compreso tra 0 e 100 che indica il tempo impiegato dalla funzione per l'esecuzione come percentuale del tempo massimo consentito. Ad esempio, un utilizzo di calcolo di 35 significa che la funzione è stata completata nel 35% del tempo massimo consentito.

Quando si esegue il test di una funzione, è possibile visualizzare il valore di utilizzo di calcolo nell'output dell'evento di test. Per le funzioni di produzione, è possibile visualizzare il parametro di utilizzo di calcolo sulla pagina di monitoraggio nella console CloudFront o in CloudWatch.

Restrizioni su Lambda@Edge

A Lambda@Edge si applicano le seguenti restrizioni.

Indice

Per informazioni sulle quote , consulta Quote di Lambda@Edge.

Risoluzione DNS

CloudFront esegue una risoluzione DNS sul nome di dominio di origine prima di eseguire la funzione Lambda@Edge della richiesta di origine. Se il servizio DNS del dominio presenta dei problemi e CloudFront non riesce a risolvere il nome di dominio per ottenere l'indirizzo IP, la funzione Lambda@Edge non verrà invocata. CloudFront restituirà il codice di stato HTTP 502 (Gateway non valido) al client. Per ulteriori informazioni, consulta Errore DNS (`NonS3OriginDnsError`).

Se la logica della funzione modifica il nome di dominio di origine, CloudFront eseguirà un'altra risoluzione DNS sul nome di dominio aggiornato al termine dell'esecuzione della funzione.

Per ulteriori informazioni sulla gestione del failover DNS, consulta Configurazione di un failover DNS nella Guida per gli sviluppatori di Amazon Route 53.

Codici di stato HTTP

Le funzioni Lambda@Edge per gli eventi di risposta del visualizzatore non possono modificare il codice di stato HTTP della risposta, a prescindere dal fatto che la risposta provenga dall'origine o dalla cache CloudFront.

Versione delle funzioni Lambda

È necessario utilizzare una versione numerata della funzione Lambda, non `$LATEST` né alias.

Regione Lambda

La funzione Lambda deve trovarsi nella regione Stati Uniti orientali (Virginia settentrionale).

Autorizzazioni del ruolo Lambda

Il ruolo di esecuzione IAM associato alla funzione Lambda deve consentire ai principali del servizio `lambda.amazonaws.com` e `edgelambda.amazonaws.com` di assumere il ruolo. Per ulteriori informazioni, consulta Configurazione di ruoli e autorizzazioni IAM per Lambda@Edge.

Caratteristiche di Lambda

Le seguenti funzionalità Lambda non sono supportate da Lambda@Edge:

- Configurazioni di gestione del runtime Lambda diverse da Auto (impostazione predefinita)
- Configurazione della funzione Lambda per accedere a risorse presenti nel VPC
- Code DLQ della funzione Lambda
- Variabili di ambiente Lambda (ad eccezione delle variabili di ambiente riservate, che sono supportate automaticamente)
- Funzioni Lambda con Gestione delle dipendenze AWS Lambda con livelli
- Using AWS X-Ray
- Concorrenza con provisioning di Lambda

> **Note**
>
> Le funzioni Lambda@Edge condividono le stesse funzionalità di concorrenza regionale di tutte le funzioni Lambda. Per ulteriori informazioni, consulta Quote di Lambda@Edge.

- Creare una funzione Lambda utilizzando un'immagine di container
- Funzioni Lambda che utilizzano l'architettura arm
- Funzioni Lambda con più di 512 MB di archiviazione temporanea.
- Utilizzo di una chiave gestita dal cliente per crittografare i pacchetti di implementazione .zip

Runtime supportati

Lambda@Edge supporta le versioni più recenti dei runtime Node.js e Python. Per un elenco delle versioni supportate e delle relative date future di obsolescenza, consulta Runtime supportati nella Guida per gli sviluppatori di AWS Lambda.

> **Tip**
>
> - Come best practice, utilizza le versioni più recenti dei runtime forniti per migliorare le prestazioni e usufruire delle nuove funzionalità.
> - Non è possibile creare o aggiornare funzioni con questa versione obsoleta di Node.js. Puoi associare solo funzioni esistenti a queste versioni con distribuzioni CloudFront. Le funzioni con queste versioni associate a distribuzioni continueranno a essere eseguite. Tuttavia, ti consigliamo di trasferire la funzione alle versioni più recenti di Node.js. Per ulteriori informazioni, consulta Policy di deprecazione del runtime nella Guida per gli sviluppatori di AWS Lambda e Node.js release schedule su GitHub.

Intestazioni CloudFront

Le funzioni Lambda@Edge possono leggere, modificare, rimuovere o aggiungere una qualsiasi delle intestazioni CloudFront elencate in Aggiunta di intestazioni della richiesta CloudFront:

> **Note**
>
> - Se desideri che CloudFront aggiunga queste intestazioni, è necessario configurarlo per aggiungerle utilizzando una policy della cache o una policy di richiesta origine.
> - CloudFront aggiunge le intestazioni dopo l'evento di richiesta visualizzatore, il che significa che le intestazioni non sono disponibili per Lambda@Edge in una richiesta visualizzatore. Le intestazioni sono disponibili solo per le funzioni Lambda@Edge in una richiesta origine e una risposta origine.
> - Se la richiesta del visualizzatore include intestazioni con questi nomi e CloudFront è stato configurato per aggiungere queste intestazioni utilizzando una policy della cache o una policy di richiesta origine, CloudFront sovrascrive i valori di intestazione che si trovavano nella richiesta del visualizzatore. Le funzioni rivolte al visualizzatore vedono il valore dell'intestazione dalla richiesta del visualizzatore, mentre le funzioni rivolte all'origine vedono il valore dell'intestazione aggiunto da CloudFront.

- Se la funzione della richiesta visualizzatore aggiunge l'intestazione `CloudFront-Viewer-Country`, non ottiene la convalida e CloudFront restituisce il codice di stato HTTP 502 (Gateway non valido) al visualizzatore.

Restrizioni sul corpo della richiesta con l'opzione Includi corpo

Quando si sceglie l'opzione Includi corpo per esporre il corpo della richiesta alla funzione Lambda@Edge, si applicano i seguenti limiti di informazioni e dimensioni per le parti del corpo che vengono esposte o sostituite.

- CloudFront codifica il corpo della richiesta prima di esporlo a Lambda@Edge sempre in base64.
- Se il corpo della richiesta è di grandi dimensioni, CloudFront lo tronca prima di esporlo a Lambda@Edge nel seguente modo:
  - Per gli eventi di richiesta del visualizzatore, il corpo è troncato a 40 KB.
  - Per gli eventi di richiesta di origine, il corpo è troncato a 1 MB.
- Se accedi al corpo della richiesta in sola lettura, Cloudfront invia all'origine il corpo della richiesta originale completa.
- Se la funzione Lambda@Edge sostituisce il corpo della richiesta, si applicano i seguenti limiti di dimensioni per il corpo restituito dalla funzione:
  - Se la funzione Lambda@Edge restituisce il corpo come testo semplice:
    - Per gli eventi di richiesta visualizzatore, il limite del corpo è 40 KB.
    - Per gli eventi di richiesta origine, il limite del corpo è 1 MB.
  - Se la funzione Lambda@Edge restituisce il corpo codificato in base64:
    - Per gli eventi di richiesta visualizzatore, il limite del corpo è 53,2 KB.
    - Per gli eventi di richiesta origine, il limite del corpo è 1,33 MB.

> **Note**
>
> Se la funzione Lambda@Edge restituisce un corpo che supera questi limiti, la richiesta avrà esito negativo con un codice di stato HTTP 502 (Errore di convalida Lambda). Ti consigliamo di aggiornare la funzione Lambda@Edge in modo che il corpo non superi questi limiti.

Timeout di risposta e timeout keep-alive (solo origini personalizzate)

Se utilizzi le funzioni Lambda@Edge per impostare il timeout di risposta o il timeout keep-alive per le origini di distribuzione, verifica di specificare un valore supportato dall'origine. Per ulteriori informazioni, consulta Quote timeout di risposta e keep-alive.

Report, parametri e log

CloudFront offre diverse opzioni per la segnalazione, il monitoraggio e la registrazione delle risorse. CloudFront Puoi completare le seguenti attività:

- Visualizza e scarica i report per vedere l'utilizzo e l'attività delle tue CloudFront distribuzioni, inclusi report di fatturazione, statistiche sulla cache, contenuti popolari e referrer principali.
- Monitora e monitora CloudFront, comprese le funzioni di edge computing, direttamente nella CloudFront console o utilizzando Amazon CloudWatch. CloudFront invia le metriche CloudWatch per le distribuzioni e le funzioni edge, sia Lambda @Edge che Functions. CloudFront
- Visualizza i log delle richieste dei visualizzatori che le tue CloudFront distribuzioni ricevono con log standard o log di accesso in tempo reale. Oltre ai registri delle richieste dei visualizzatori, puoi utilizzare CloudWatch Logs per ottenere i log delle tue funzioni edge, sia Lambda @Edge che Functions. CloudFront Puoi anche utilizzarlo AWS CloudTrail per ottenere i log dell'attività dell'API nel CloudFront tuo. Account AWS
- Tieni traccia delle modifiche alla configurazione CloudFront delle tue risorse utilizzando AWS Config.

Per ulteriori informazioni su queste opzioni, consulta i seguenti argomenti.

Argomenti

AWS report di fatturazione e utilizzo per CloudFront

AWS fornisce due report di utilizzo per CloudFront:

- Il rapporto di AWS fatturazione è una visualizzazione di alto livello di tutte le attività Servizi AWS che stai utilizzando, tra cui. CloudFront

- Il rapporto AWS sull'utilizzo è un riepilogo delle attività per un servizio specifico, aggregato per ora, giorno o mese. Include anche tabelle di utilizzo che forniscono una rappresentazione grafica dell'utilizzo CloudFront .

> **Note**
>
> Come altri Servizi AWS, ti CloudFront addebita solo ciò che utilizzi. Per ulteriori informazioni, consultare Prezzi di CloudFront.

Argomenti

Visualizza il rapporto di AWS fatturazione per CloudFront

Puoi visualizzare un riepilogo dell' AWS utilizzo e degli addebiti, elencati per servizio, nella pagina Fatture della Gestione dei costi e fatturazione AWS console.

Per visualizzare il rapporto di AWS fatturazione

1. Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo https://console.aws.amazon.com/costmanagement/.
2. Nel riquadro di navigazione selezionare Bills (Fatture).
3. Scegli un Periodo di fatturazione (ad esempio, agosto 2023).
4. Nella scheda Addebiti per servizio, scegli CloudFront, quindi espandi Global o il Regione AWS nome.
5. Per scaricare un report di fatturazione dettagliato in formato CSV, scegli Scarica tutto su CSV.

Per ulteriori informazioni sulla AWS fattura, consulta Visualizzazione della fattura nella Guida per l'AWS Billing utente.

Il rapporto di fatturazione include i seguenti valori che si applicano a CloudFront:

- ProductCode – `AmazonCloudFront`

- UsageType— Uno dei seguenti valori:
  - Un codice che identifica il tipo di trasferimento dei dati
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- ItemDescription— Una descrizione della tariffa di fatturazione per. UsageType
- UsageStart Data e UsageEndDate: il giorno a cui si riferisce l'utilizzo, in UTC (Coordinated Universal Time).
- UsageQuantity— Uno dei seguenti valori:
  - Il numero di richieste durante il periodo di tempo specificato
  - La quantità di dati trasferiti in gigabyte
  - Il numero di oggetti invalidati
  - La somma dei mesi ripartiti proporzionalmente in cui i certificati SSL erano associati alle distribuzioni abilitate. CloudFront Ad esempio, se hai un certificato associato a una distribuzione attivata per un intero mese e un altro certificato associato a una distribuzione attività per la metà del mese, questo valore sarà 1,5.

Visualizza il report sull'utilizzo per AWS CloudFront

AWS fornisce un rapporto CloudFront sull'utilizzo più dettagliato del rapporto di fatturazione ma meno dettagliato dei registri di CloudFront accesso. Il report di utilizzo fornisce dati di utilizzo raggruppati per ora, giorno o mese ed elenca le operazioni per regione e tipo di utilizzo, ad esempio dati trasferiti al di fuori della regione Australia.

Per visualizzare il rapporto sull'utilizzo AWS

1. Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo https://console.aws.amazon.com/costmanagement/.
2. Nel pannello di navigazione, scegliere Cost Explorer.
3. Nella pagina Nuovo report costi e utilizzo, nel riquadro Parametri report, scegli un intervallo di date e una granularità per il report.

4. In Filtri, Servizio, seleziona CloudFront.
5. Seleziona il Tipo di utilizzo.
6. In Suddivisione dei costi e dell'utilizzo, scegli Scarica in formato CSV.

Per ulteriori informazioni sul rapporto sull' AWS utilizzo, consulta Report AWS sull'utilizzo nella Guida Esportazioni di dati AWS per l'utente.

Il rapporto CloudFront sull'utilizzo include i seguenti valori:

- Service – `AmazonCloudFront`
- Operazione: metodo HTTP. I valori includono `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- UsageType— Uno dei seguenti valori:
  - Un codice che identifica il tipo di trasferimento dei dati
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- Risorsa: l'ID della CloudFront distribuzione associato all'utilizzo o l'ID del certificato di un certificato SSL associato a una CloudFront distribuzione.
- StartTime/EndTime— Il giorno a cui si riferisce l'utilizzo, in UTC (Coordinated Universal Time).
- UsageValue— 1) Il numero di richieste durante il periodo di tempo specificato o 2) la quantità di dati trasferiti in byte.

Se utilizzi Amazon S3 come origine per Amazon S3 CloudFront, valuta la possibilità di eseguire anche il report di utilizzo per Amazon S3. Tuttavia, se utilizzi Amazon S3 per scopi diversi da quello di origine per le tue CloudFront distribuzioni, potrebbe non essere chiaro quale parte si riferisca al tuo utilizzo. CloudFront

> **Tip**
>
> Per informazioni dettagliate su ogni richiesta CloudFront ricevuta per i tuoi oggetti, attiva i log di CloudFront accesso per la tua distribuzione. Per ulteriori informazioni, consulta the section called “Registri di accesso (registri standard)”.

Per ulteriori informazioni sulla comprensione degli CloudFront addebiti e dei tipi di utilizzo dei report, consultathe section called “Interpreta i report sulle AWS fatture e sull'utilizzo per CloudFront”.

Interpreta i report sulle AWS fatture e sull'utilizzo per CloudFront

Una volta che hai il rapporto di fatturazione e il rapporto sull'utilizzo, puoi utilizzare questo argomento per capire come interpretare ogni CloudFront addebito visualizzato sulla fattura e il tipo di utilizzo corrispondente per ogni addebito. Questo argomento include i codici e Regione AWS le abbreviazioni che possono apparire in entrambi i report.

La maggior parte dei codici in entrambe le colonne include un'abbreviazione a due lettere che indica l'ubicazione dell'attività. Nella tabella seguente, *`region`* un codice viene sostituito nella AWS fattura e nel rapporto di utilizzo da una delle seguenti abbreviazioni di due lettere:

- AP: Hong Kong, Filippine, Corea del Sud, Taiwan e Singapore (Asia Pacifico)
- AU: Australia
- CA: Canada
- UE: Europa e Israele
- IN: India
- JP: Giappone
- ME: Medio Oriente
- SA: Sud America
- US: Stati Uniti
- ZA: Sud Africa

Per ulteriori informazioni sui prezzi di Regione AWS, consulta CloudFront i prezzi di Amazon.

Note

- Questa tabella non include i costi per il trasferimento di oggetti da un bucket CloudFront Amazon S3 alle edge location. Tali costi, se presenti, sono visualizzati nella sezioneAWS Data Transfer (Trasferimento dati) della fattura AWS .
- La prima colonna elenca gli addebiti visualizzati nel rapporto di AWS fatturazione e spiega il significato di ciascuno di essi.
- La seconda colonna elenca gli elementi che compaiono nel rapporto AWS sull'utilizzo e mostra la correlazione tra gli addebiti delle bollette e gli elementi del rapporto sull'utilizzo.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
region- DataTransfer -Byte in uscita Byte totali serviti dalle CloudFront edge location in risposta *region* a utenti e richieste. `GET HEAD`	*region*-Byte-out-http-static: Byte forniti tramite HTTP per oggetti con TTL ≥ 3.600 secondi. *region*-Byte-uscita-https-statici: Byte forniti tramite HTTPS per oggetti con TTL ≥ 3.600 secondi. *region*-Byte-out-HTTP-dinamici: Byte forniti tramite HTTP per oggetti con TTL < 3.600 secondi. *region*-Byte di uscita-HTTPS-dinamici: Byte forniti tramite HTTPS per oggetti con TTL < 3.600 secondi. *region*-Proxy HTTP in uscita:

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
	Byte restituiti CloudFront ai visualizzatori tramite HTTP in risposta a,, e richieste. `DELETE OPTIONS PATCH POST PUT` *region*-Out-Bytes-HTTPS-Proxy: Byte restituiti CloudFront ai visualizzatori tramite HTTPS in risposta a,, e richieste. `DELETE OPTIONS PATCH POST PUT` Ciò include i byte restituiti CloudFront ai visualizzatori tramite gRPC.
region- -Fuori- DataTransfer OBytes Byte totali trasferiti dalle CloudFront edge location alla funzione di origine o periferica in risposta a `DELETEOPTIONS`, `PATCHPOST`, e `PUT` richieste. I costi includono il trasferimento dei WebSocket dati dal client al server.	*region*OBytes-Proxy HTTP Byte totali trasferiti tramite HTTP dalle CloudFront edge location alla funzione di origine o periferica in risposta a`DELETE`, `OPTIONSPATCH`, `POST` e richieste. `PUT` *region*-Proxy -HTTPS OBytes Byte totali trasferiti tramite HTTPS dalle CloudFront edge location alla funzione di origine o periferica in risposta a`DELETE`, `OPTIONSPATCH`, `POST` e richieste. `PUT` Ciò include i byte trasferiti tramite gRPC CloudFront dalle edge location all'origine CloudFront o alle funzioni.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
region- Richieste - Livello 1 Numero di richieste HTTP `GET` e `HEAD`.	*region*-Richieste-HTTP-Static Numero di richieste HTTP `GET` e `HEAD` fornite per oggetti con TTL ≥ 3600 secondi. *region*-Richieste-HTTP-Dynamic Numero di richieste HTTP `GET` e `HEAD` fornite per oggetti con TTL < 3600 secondi
region-Richieste - livello 2 - HTTPS Numero di richieste HTTPS `GET` e `HEAD`.	*region*-Richieste-https-static Numero di richieste HTTPS `GET` e `HEAD` fornite per oggetti con TTL ≥ 3600 secondi. *region*-Richieste-HTTPS-Dynamic Numero di richieste HTTPS `GET` e `HEAD` fornite per oggetti con TTL < 3600 secondi.
region-Richieste-HTTP-Proxy Numero di `PUT` richieste HTTP`DELETE`,, `OPTIONS`, `PATCH`, `POST`, e che vengono inoltrate alla funzione CloudFront origin o edge. Include anche il numero di WebSocketrichieste HTTP (`GET`richieste con l'`Upgrade: websocket` intestazione) che vengono CloudFront inoltrate alla funzione origin o edge.	*region*-Richieste-HTTP-Proxy Uguale all'articolo corrispondente nella fattura. CloudFront

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
region-Richieste-HTTPS-Proxy Numero di HTTPS`DELETE`,, `OPTIONS` `PATCH` `POST`, e `PUT` richieste inoltrate alla funzione di CloudFront origine o edge. Include anche i seguenti tipi di richiesta: • Il numero di WebSocketrichieste HTTPS (`GET`richieste con l'`Upgrade: websocket` intestazione) che vengono CloudFront inoltrate all'origine o alla funzione edge. • Numero di richieste HTTPS	*region*-Richieste-HTTPS-Proxy Uguale all'articolo corrispondente nella fattura. CloudFront
region-richieste-https-proxy-file Numero di HTTPS `DELETE` e `POST` richieste elaborate con `OPTIONS` crittografia a `PATCH` livello di campo che inoltra all'origine o alla funzione edge. CloudFront	*region*-Richieste-HTTPS-proxy-file Uguale all'articolo corrispondente nella fattura. CloudFront
region-Byte- OriginShield Byte totali trasferiti dall'origine a qualsiasi edge cache regionale, inclusa la cache edge regionale abilitata come Origin Shield.	*region*-Byte- OriginShield Uguale all'articolo corrispondente nella fattura CloudFront .
region-OBytes-OriginShield Byte totali trasferiti all'origine da qualsiasi edge cache regionale, inclusa la cache edge regionale abilitata come Origin Shield.	*region*-OBytes-OriginShield Uguale all'articolo corrispondente nella CloudFront fattura.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
region-Richieste- OriginShield Numero di richieste che vanno a Origin Shield come livello incrementale. Per le richieste dinamiche (non memorizzabili nella cache) che vengono inoltrate tramite proxy all'origine, Origin Shield è sempre un livello increment ale. Per le richieste memorizzabili nella cache, Origin Shield è talvolta un livello incrementale. Per ulteriori informazioni, consulta the section called “Stima dei costi di Origin Shield”.	*region*-Richieste- OriginShield Uguale all'articolo corrispondente nella CloudFront fattura.
Invalidations L'addebito per l'invalidazione degli oggetti (rimozione degli oggetti dai CloudFront bordi). Per ulteriori informazioni, consulta Pagamento per l’invalidazione dei file.	Invalidations Uguale all'articolo corrispondente nella fattura CloudFront .
SSL-Cert-Custom Il costo per l'utilizzo di un certificato SSL con un nome di dominio CloudFront alternati vo come example.com anziché utilizzare il certificato CloudFront SSL predefinito e il nome di dominio assegnato alla distribuzione. CloudFront	SSL-Cert-Custom Uguale all'articolo corrispondente nella fattura. CloudFront
RealTimeLog-KinesisDataStream L'addebito per il numero di righe generate per i registri di accesso in tempo reale.	RealTimeLog-KinesisDataStream Uguale all'articolo corrispondente nella CloudFront fattura.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
Esecuzioni- CloudFrontFunctions Il costo per il numero di chiamate di CloudFront Functions.	Esecuzioni- CloudFrontFunctions Uguale all'articolo corrispondente nella CloudFront fattura.
region-Richiesta Lambda-Edge Il costo per il numero di invocazioni della funzione Lambda@Edge.	***region***-Richiesta Lambda-Edge Uguale all'articolo corrispondente nella fattura. CloudFront
region-Lambda-Edge-GB/secondo L'addebito per la durata dal momento in cui la funzione Lambda@Edge viene invocata a quando ritorna o termina.	***region***-Lambda-Edge-GB/secondo Uguale all'articolo corrispondente nella fattura. CloudFront
KeyValueStore-EdgeReads L'addebito per il numero di chiamate in lettura ai CloudFront KeyValueStoremetodi,`get()`,`exists()`, `emeta()`. Per ulteriori informazioni, consulta Metodi helper per archivi di valori delle chiavi.	KeyValueStore-EdgeReads Uguale all'articolo corrispondente nella CloudFront fattura.
KeyValueStore-APIOperations L'addebito per il numero di chiamate all'CloudFront KeyValueStoreAPI.	KeyValueStore-APIOperations Uguale all'articolo corrispondente nella CloudFront fattura.

Visualizzazione dei report CloudFront nella console

Ogni report fornisce informazioni dettagliate e visualizzazioni, in modo da poter ottimizzare la distribuzione dei contenuti, identificare i colli di bottiglia delle prestazioni e prendere decisioni basate sui dati. Che tu abbia bisogno di monitorare l'efficienza della cache, analizzare i modelli di traffico o comprendere meglio i visualizzatori, puoi utilizzare questi report per monitorare e analizzare in modo efficace le distribuzioni CloudFront.

Puoi visualizzare i seguenti report sull'attività di CloudFront nella console:

Argomenti

La maggior parte di questi report è basata sui dati nei log di accesso di CloudFront, che contengono informazioni dettagliate su ogni richiesta utente che CloudFront riceve. Non è necessario attivare i log di accesso per visualizzare i report. Per ulteriori informazioni, consulta Registri di accesso (registri standard).

Visualizzazione dei report sulle statistiche della cache di CloudFront

Il report sulle statistiche della cache di Amazon CloudFront include le seguenti informazioni:

- Richieste totali: mostra il numero totale di richieste per tutti i codici di stato HTTP (ad esempio, 200 o 404) e tutti i metodi (ad esempio, GET, HEAD o POST).
- Percentuale di richieste visualizzatore per tipo di risultato: occorrenze, mancati riscontri ed errori come percentuale delle richieste totali del visualizzatore per la distribuzione CloudFront selezionata.
- Byte trasferiti a visualizzatori: totale dei byte e i byte dai mancati riscontri
- Codici di stato HTTP: mostra le richieste visualizzatore per codice di stato HTTP.
- Percentuale di richieste GET che non hanno completato il download: mostra le richieste GET del visualizzatore che non hanno completato il download dell'oggetto richiesto come percentuale delle richieste totali

I dati per queste statistiche provengono dalla stessa origine dei log di accesso CloudFront. Tuttavia, non è necessario abilitare la registrazione degli accessi per visualizzare le statistiche della cache.

Puoi visualizzare grafici per un determinato intervallo di tempo negli ultimi 60 giorni, con punti dati ogni ora o ogni giorno. In genere, puoi visualizzare i dati sulle richieste che CloudFront ha ricevuto appena un'ora prima, ma i dati possono talvolta essere ritardati fino a 24 ore.

Argomenti

Visualizzazione dei report sulle statistiche della cache di CloudFront nella console

Puoi visualizzare il report sulle statistiche della cache di CloudFront nella console.

Come visualizzare il report sulle statistiche della cache di CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Statistiche cache.
3. Nel riquadro Report sulle statistiche della cache di CloudFront per Data inizio e Data fine, seleziona l'intervallo di date per il quale desideri visualizzare i grafici sulle statistiche della cache. Gli intervalli disponibili dipendono dal valore selezionato per Granularity (Granularità):

   - Daily (Giorno): per visualizzare grafici con un punto dati per giorno, seleziona qualsiasi intervallo di date negli ultimi 60 giorni.
   - Hourly (Ora): per visualizzare grafici con un punto dati per ogni ora, seleziona qualsiasi intervallo di date fino a 14 giorni negli ultimi 60 giorni.

   Date e ore sono in formato UTC.
4. In Granularity (Granularità) specifica se visualizzare un punto dati per giorno o per ora nei grafici. Se si specifichi un intervallo di date superiore a 14 giorni, l'opzione per specificare un punto dati per ora non è disponibile.
5. In Viewer Location (Ubicazione visualizzatore), scegli il continente da cui provengono le richieste visualizzatore, oppure scegli All Locations (Tutte le ubicazioni). I grafici sulle statistiche della cache includono dati per le richieste che CloudFront ha ricevuto dall'ubicazione specificata.
6. Nell'elenco Distribution (Distribuzione), seleziona le distribuzioni per le quali intendi visualizzare i dati nei grafici di utilizzo:

   - Una singola distribuzione: i grafici visualizzano i dati per la distribuzione CloudFront selezionata. L'elenco Distribution (Distribuzione) visualizza l'ID della distribuzione e gli

eventuali nomi di dominio alternativi (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include i nomi di dominio di origine per la distribuzione.

- Tutte le distribuzioni: i grafici visualizzano i dati sommati per tutte le distribuzioni associate all'Account AWS corrente, escluse le distribuzioni eliminate.

7. clicca su Aggiorna.

> **Tip**
>
> - Per visualizzare i dati per un punto dati orario o giornaliero in un grafico, passa il mouse sul punto dati.
> - Per i grafici che mostrano i dati trasferiti, puoi impostare la scala verticale su gigabyte, megabyte o kilobyte.

Download di dati in formato CSV

Puoi scaricare il report sulle statistiche della cache in formato CSV. Questa sezione descrive come scaricare il report e i valori nel report.

Download del report sulle statistiche della cache in formato CSV

1. Durante la visualizzazione del report sulle statistiche della cache, scegli CSV.
2. Nella finestra di dialogo Opening file name (Apertura nome file), scegli se aprire o salvare il file.

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Version

La versione del formato per questo file CSV.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure ALL se hai eseguito il report per tutte le distribuzioni.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Granularità

Se ogni riga nel report rappresenta un'ora o un giorno.

ViewerLocation

Il continente da cui provengono le richieste visualizzatore, oppure ALL se scegli di scaricare il report per tutte le ubicazioni.

Dati nel report sulle statistiche della cache

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure ALL se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

ViewerLocation

Il continente da cui provengono le richieste visualizzatore, oppure ALL se scegli di scaricare il report per tutte le ubicazioni.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

RequestCount

Il numero totale di richieste per tutti i codici di stato HTTP (ad esempio, 200 o 404) e tutti i metodi (ad esempio, GET, HEAD o POST).

HitCount

Il numero di richieste visualizzatore per le quali l'oggetto viene distribuito da una cache edge di CloudFront.

MissCount

Il numero di richieste visualizzatore per le quali l'oggetto non è attualmente in una cache edge; CloudFront deve quindi ottenere l'oggetto dall'origine.

ErrorCount

Il numero di richieste visualizzatore che hanno generato un errore e comportato la mancata distribuzione dell'oggetto da parte di CloudFront.

IncompleteDownloadCount

Il numero di richieste visualizzatore per le quali il visualizzatore ha iniziato ma non completato il download dell'oggetto.

HTTP2xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 2xx (riuscito).

HTTP3xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 3xx (è richiesta un'azione supplementare).

HTTP4xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 4xx (errore client).

HTTP5xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 5xx (errore server).

TotalBytes

Il numero totale di byte distribuiti da CloudFront ai visualizzatori in risposta a tutte le richieste per tutti i metodi HTTP.

BytesFromMisses

Il numero di byte distribuiti ai visualizzatori per gli oggetti non presenti nella cache edge al momento della richiesta. Questo valore è una buona approssimazione dei byte trasferiti dalla tua origine alle cache edge di CloudFront. Tuttavia, esclude le richieste per oggetti già presenti nella cache edge, ma scaduti.

Come i grafici delle statistiche della cache sono collegati ai dati nei log standard di CloudFront (log di accesso)

La tabella seguente indica come i grafici sulle statistiche della cache nella console di CloudFront corrispondono ai valori nei log di accesso di CloudFront. Per ulteriori informazioni sui log degli accessi di CloudFront, consultare Registri di accesso (registri standard).

Total Requests (Richieste totali)

Questo grafico indica il numero totale di richieste per tutti i codici di stato HTTP (ad esempio, 200 o 404) e tutti i metodi (ad esempio, `GET`, `HEAD` o `POST`). Le richieste totali in questo grafico sono pari al numero totale di richieste nei file di log di accesso per lo stesso periodo di tempo.

Percentage of Viewer Requests by Result Type (Percentuale di richieste visualizzatore per tipo di risultato)

Questo grafico indica riscontri, mancati riscontri ed errori come una percentuale del totale delle richieste visualizzatore per la distribuzione CloudFront selezionata:

- Hit (Riscontro): una richiesta visualizzatore per la quale l'oggetto viene distribuito da una cache edge di CloudFront. Nei log di accesso, si tratta delle richieste per le quali il valore di `x-edge-response-result-type` è `Hit`.
- Miss (Mancato riscontro): una richiesta visualizzatore per la quale l'oggetto non è correntemente in una cache edge; CloudFront deve quindi ottenere l'oggetto dall'origine. Nei log di accesso, si tratta delle richieste per le quali il valore di `x-edge-response-result-type` è `Miss`.
- Error (Errore): una richiesta visualizzatore che ha restituito un errore; CloudFront non ha distribuito l'oggetto. Nei log di accesso, sono le richieste per le quali il valore di `x-edge-response-result-type` è `Error`, `LimitExceeded` o `CapacityExceeded`.

Il grafico non include i riscontri di aggiornamento, ovvero richieste per oggetti nella cache edge, ma scaduti. Nei log di accesso, i riscontri di aggiornamento sono richieste per le quali il valore di `x-edge-response-result-type` è `RefreshHit`.

Bytes Transferred to Viewers (Byte trasferiti a visualizzatori)

Questo grafico indica due valori:

- Total Bytes (Totale Byte): il numero totale di byte distribuiti da CloudFront ai visualizzatori in risposta a tutte le richieste per tutti i metodi HTTP. Nei log di accesso di CloudFront, Total Bytes (Totale byte) è la somma dei valori nella colonna `sc-bytes` per tutte le richieste durante lo stesso periodo di tempo.
- Bytes from Misses (Byte da mancati riscontri): il numero di byte distribuiti ai visualizzatori per gli oggetti non presenti nella cache edge al momento della richiesta. Nei log di accesso di CloudFront, Bytes from Misses (Byte da mancati riscontri) è la somma dei valori nella colonna `sc-bytes` per le richieste dove il valore di `x-edge-result-type` è `Miss`. Questo valore è una buona approssimazione dei byte trasferiti dalla tua origine alle cache edge di CloudFront. Tuttavia, esclude le richieste per oggetti già presenti nella cache edge, ma scaduti.

Codici di stato HTTP

Questo grafico indica le richieste visualizzatore per codice di stato HTTP. Nei log di accesso di CloudFront, i codici di stato sono visualizzati nella colonna `sc-status`.

- 2xx: la richiesta è riuscita.
- 3xx: è richiesta un'azione supplementare. Ad esempio, 301 (Spostato in modo permanente) significa che l'oggetto richiesto è stato spostato in una posizione differente.
- 4xx: si è verificato un errore nel client. Ad esempio, 404 (Non trovato) indica che il client ha richiesto un oggetto introvabile.
- 5xx: il server di origine non ha soddisfatto la richiesta. Ad esempio, 503 (Servizio non disponibile) significa che il server di origine non è attualmente disponibile.

Percentage of GET Requests that Didn't Finish Downloading (Percentuale di richieste GET che non hanno completato il download)

Questo grafico mostra le richieste `GET` visualizzatore che non hanno completato il download dell'oggetto richiesto come percentuale delle richieste totali. In genere, il download di un oggetto non viene completato in quanto il visualizzatore ha annullato il download, ad esempio, facendo clic su un altro collegamento o chiudendo il browser. Nei log di accesso di CloudFront, queste richieste hanno un valore `200` nella colonna `sc-status` e un valore `Error` nella colonna `x-edge-result-type`.

Visualizzazione dei report CloudFront sugli oggetti più popolari

Visualizza il report sugli oggetti più popolari di Amazon CloudFront per vedere i 50 oggetti più popolari per una distribuzione durante un determinato intervallo di date compreso negli ultimi 60 giorni. Puoi anche visualizzare le statistiche su tali oggetti, incluse le seguenti:

- Numero di richieste per l'oggetto
- Numero di riscontri e mancati riscontri
- Hit Ratio (Percentuale di riscontri)
- Numero di byte serviti per mancati riscontri
- Byte totali serviti
- Numero di download incompleti
- Numero di richieste per codice di stato HTTP (2xx, 3xx, 4xx e 5xx)

I dati per queste statistiche provengono dalla stessa origine dei log di accesso CloudFront. Tuttavia, non devi abilitare la registrazione degli accessi per visualizzare gli oggetti più popolari.

Argomenti

Visualizzazione dei report sugli oggetti più popolari di CloudFront nella console

Puoi visualizzare i report sugli oggetti più popolari di CloudFront nella console.

Come visualizzare gli oggetti più popolari per una distribuzione CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Oggetti popolari.
3. Nel riquadro CloudFront Popular Objects Report (Report oggetti popolari CloudFront) per Start Date (Data inizio) e End Date (Data fine), seleziona l'intervallo di date per il quale desideri

visualizzare un elenco di oggetti popolari. Puoi scegliere qualsiasi intervallo di date negli ultimi 60 giorni.

Date e ore sono in formato UTC.

4. Nell'elenco Distribution (Distribuzione), seleziona la distribuzione per la quale intendi visualizzare un elenco di oggetti popolari.
5. Scegliere Aggiorna.

Come CloudFront calcola le statistiche sugli oggetti più popolari

Per ottenere un conteggio accurato dei primi 50 oggetti nella distribuzione, CloudFront conta le richieste per tutti gli oggetti a intervalli di 10 minuti a partire da mezzanotte e mantiene un totale parziale dei primi 150 oggetti per le 24 ore successive. (CloudFront conserva inoltre i totali giornalieri dei primi 150 oggetti per 60 giorni).

Nella parte inferiore dell'elenco, gli oggetti guadagnano posizioni o scompaiono del tutto, di conseguenza i totali relativi a tali oggetti sono approssimazioni. I 50 oggetti nella parte superiore dell'elenco di 150 oggetti possono perdere o guadagnare posizioni, ma raramente scompaiono dall'elenco, di conseguenza i totali di tali oggetti sono più affidabili.

Quando un oggetto esce dall'elenco dei primi 150 oggetti e in seguito vi appare di nuovo nel corso del giorno, CloudFront aggiunge un numero stimato di richieste per il periodo durante il quale l'oggetto non era nell'elenco. La stima si basa sul numero di richieste ricevute da qualsiasi oggetto nella parte bassa dell'elenco durante tale periodo di tempo.

Se in seguito l'oggetto entra nei primi 50 oggetti nel corso della giornata, le stime del numero di richieste che CloudFront ha ricevuto mentre l'oggetto non era tra i primi 150 oggetti in genere determina un numero di richieste nel report sugli oggetti popolari superiore al numero di richieste che appaiono nei log di accesso per quell'oggetto.

Download di dati in formato CSV

Puoi scaricare il report sugli oggetti popolari in formato CSV. Questa sezione descrive come scaricare il report e i valori nel report.

Download del report sugli oggetti popolari in formato CSV

1. Durante la visualizzazione del report sugli oggetti più popolari, scegli CSV.
2. Nella finestra di dialogo Opening file name (Apertura nome file), scegli se aprire o salvare il file.

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Version

La versione del formato per questo file CSV.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per cui hai eseguito il report.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Dati nel report sugli oggetti popolari

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per cui hai eseguito il report.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

Oggetto

Gli ultimi 500 caratteri dell'URL per l'oggetto.

RequestCount

Il numero totale di richieste per questo oggetto.

HitCount

Il numero di richieste visualizzatore per le quali l'oggetto viene distribuito da una cache edge di CloudFront.

MissCount

Il numero di richieste visualizzatore per le quali l'oggetto non è attualmente in una cache edge; CloudFront deve quindi ottenere l'oggetto dall'origine.

HitCountPct

Il valore di `HitCount` come percentuale del valore di `RequestCount`.

BytesFromMisses

Il numero di byte distribuiti ai visualizzatori per quell'oggetto quando l'oggetto non era nella cache edge al momento della richiesta.

TotalBytes

Il numero totale di byte distribuiti da CloudFront; ai visualizzatori per quell'oggetto in risposta a tutte le richieste per tutti i metodi HTTP.

IncompleteDownloadCount

Il numero di richieste visualizzatore per quell'oggetto per le quali il visualizzatore ha avviato ma non completato il download dell'oggetto.

HTTP2xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 2xx (riuscito).

HTTP3xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 3xx (è richiesta un'azione supplementare).

HTTP4xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 4xx (errore client).

HTTP5xx

Il numero di richieste visualizzatore per le quali il codice di stato HTTP era un valore 5xx (errore server).

Come i dati nel rapporto degli oggetti popolari sono collegati ai dati nei log standard di CloudFront (log di accesso)

L'elenco seguente mostra come i valori nel report sugli oggetti popolari nella console di CloudFront corrispondono ai valori nei log di accesso di CloudFront. Per ulteriori informazioni sui log degli accessi di CloudFront, consultare Registri di accesso (registri standard).

URL

Gli ultimi 500 caratteri dell'URL che i visualizzatori utilizzano per accedere all'oggetto.

Richieste

Il numero totale di richieste per l'oggetto. Questo valore è spesso prossimo al numero di richieste `GET` per l'oggetto nei log di accesso di CloudFront.

Hits (occorrenze)

Il numero di richieste visualizzatore per le quali l'oggetto è stato distribuito da una cache edge di CloudFront. Nei log di accesso, si tratta delle richieste per le quali il valore di `x-edge-response-result-type` è `Hit`.

Misses (Mancati riscontri)

Il numero di richieste visualizzatore per le quali l'oggetto non era in una cache edge. CloudFront ha quindi recuperato l'oggetto dalla tua origine. Nei log di accesso, si tratta delle richieste per le quali il valore di `x-edge-response-result-type` è `Miss`.

Hit Ratio (Percentuale di riscontri)

Il valore della colonna Hits (Occorrenze) come percentuale del valore della colonna Requests (Richieste).

Bytes from Misses (Byte da mancati riscontri)

Il numero di byte distribuiti ai visualizzatori per gli oggetti non presenti nella cache edge al momento della richiesta. Nei log di accesso di CloudFront, Bytes from Misses (Byte da mancati riscontri) è la somma dei valori nella colonna `sc-bytes` per le richieste dove il valore di `x-edge-result-type` è `Miss`.

Total Bytes (Totale byte)

Il numero totale di byte distribuiti da CloudFront ai visualizzatori in risposta a tutte le richieste per l'oggetto per tutti i metodi HTTP. Nei log di accesso di CloudFront, Total Bytes (Totale byte) è

la somma dei valori nella colonna `sc-bytes` per tutte le richieste durante lo stesso periodo di tempo.

Incomplete Downloads (Download non completati)

Il numero di richieste visualizzatore che non hanno completato il download dell'oggetto richiesto. In genere, un download non viene completato in quanto il visualizzatore lo ha annullato, ad esempio, facendo clic su un altro collegamento o chiudendo il browser. Nei log di accesso di CloudFront, queste richieste hanno un valore `200` nella colonna `sc-status` e un valore `Error` nella colonna `x-edge-result-type`.

2xx

Il numero di richieste per le quali il codice di stato HTTP è `2xx`, `Successful`. Nei log di accesso di CloudFront, i codici di stato sono visualizzati nella colonna `sc-status`.

3xx

Il numero di richieste per le quali il codice di stato HTTP è `3xx`, `Redirection`. I codici di stato `3xx` indicano che è richiesta un'azione supplementare. Ad esempio, 301 (Spostato in modo permanente) significa che l'oggetto richiesto è stato spostato in una posizione differente.

4xx

Il numero di richieste per le quali il codice di stato HTTP è `4xx`, `Client Error`. I codici di stato `4xx` indicano che il client ha generato un errore. Ad esempio, 404 (Non trovato) indica che il client ha richiesto un oggetto introvabile.

5xx

Il numero di richieste per le quali il codice di stato HTTP è `5xx`, `Server Error`. I codici di stato `5xx` indicano che il server di origine non ha soddisfatto la richiesta. Ad esempio, 503 (Servizio non disponibile) significa che il server di origine non è attualmente disponibile.

Visualizzazione dei report sui principali referrer di CloudFront

Il report sui referrer principali di CloudFront include quanto segue per qualsiasi intervallo di date negli ultimi 60 giorni:

- I 25 referrer principali (domini dei siti web che hanno generato il maggior numero di richieste HTTP e HTTPS per gli oggetti che CloudFront sta distribuendo per la distribuzione)
- Numero di richieste da un referrer

- Numero di richieste provenienti da un referrer come percentuale del numero totale di richieste durante il periodo specificato

I dati per il report sui referrer principali hanno la stessa origine dei log di accesso di CloudFront. Tuttavia, non è necessario abilitare la registrazione degli accessi per visualizzare i referrer principali.

I referrer principali possono essere motori di ricerca, altri siti web con un collegamento diretto agli oggetti, oppure il tuo stesso sito web. Ad esempio, se `https://example.com/index.html` si collega a 10 grafici, `example.com` è il referrer per tutti i 10 grafici.

> **Note**
>
> Se un utente immette un URL direttamente nella riga dell'indirizzo di un browser, non esistono referrer per l'oggetto richiesto.

Argomenti

Visualizzazione dei report sui referrer principali di CloudFront nella console

Puoi visualizzare i report sui referrer principali di CloudFront nella console.

Come visualizzare i referrer principali per una distribuzione CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Referrer principali.
3. Nel riquadro CloudFront Top Referrers Report (Report referrer principali CloudFront) per Start Date (Data inizio) e End Date (Data fine), seleziona l'intervallo di date per il quale desideri visualizzare un elenco dei referrer principali.

   Date e ore sono in formato UTC.

4. Nell'elenco Distribution (Distribuzione), seleziona la distribuzione per la quale intendi visualizzare un elenco dei referrer principali.
5. Scegliere Aggiorna.

Come CloudFront calcola le statistiche sui referrer principali

Per ottenere un conteggio accurato dei primi 25 referrer, CloudFront conteggia le richieste per tutti i tuoi oggetti a intervalli di 10 minuti e mantiene un totale parziale dei primi 75 referrer. Nella parte inferiore dell'elenco, i referrer guadagnano posizioni o scompaiono del tutto, di conseguenza i totali relativi a tali referrer sono approssimazioni.

I 25 referrer nella parte superiore dell'elenco di 75 referrer possono perdere o guadagnare posizioni nell'elenco, ma raramente scompaiono dall'elenco, di conseguenza i totali di tali referrer sono in genere più affidabili.

Download di dati in formato CSV

Puoi scaricare il report sui referrer principali in formato CSV. Questa sezione descrive come scaricare il report e i valori nel report.

Download del report sui referrer principali in formato CSV

1. Durante la visualizzazione del report sui referrer principali, scegli CSV.
2. Nella finestra di dialogo Opening file name (Apertura nome file), scegli se aprire o salvare il file.

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Version

La versione del formato per questo file CSV.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Dati nel report sui referrer principali

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

Referrer

Il nome di dominio del referrer.

RequestCount

Il numero totale di richieste provenienti dal nome di dominio nella colonna `Referrer`.

RequestsPct

Il numero di richieste inviate dal referrer come percentuale del numero totale di richieste durante il periodo specificato.

Come i dati nel report sui referrer principali sono collegati ai dati nei log standard di CloudFront (log di accesso)

L'elenco seguente mostra come i valori nel report sui referrer principali nella console di CloudFront corrispondono ai valori nei log di accesso di CloudFront. Per ulteriori informazioni sui log degli accessi di CloudFront, consultare Registri di accesso (registri standard).

Referrer

Il nome di dominio del referrer. Nel log di accesso, i referrer sono elencati nella colonna `cs(Referer)`.

Request Count (Numero richieste)

Il numero totale di richieste provenienti dal nome di dominio nella colonna Referrer. Questo valore in genere è prossimo al numero di richieste `GET` provenienti dal referrer nei log di accesso di CloudFront.

Richiesta %

Il numero di richieste inviate dal referrer come percentuale del numero totale di richieste durante il periodo specificato. Se hai più di 25 referrer, non puoi calcolare Request % (% richieste) in base ai dati in questa tabella poiché la colonna Request Count (Numero richieste) non include tutte le richieste durante il periodo specificato.

Visualizzazione dei report di utilizzo CloudFront

I report di utilizzo di CloudFront includono le seguenti informazioni:

- Number of Requests (Numero di richieste): mostra il numero di richieste totali a cui CloudFront risponde dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata.
- Data Transferred by Protocol (Dati trasferiti per protocollo) e Data Transferred by Destination (Dati trasferiti per destinazione): entrambi mostrano la quantità totale di dati trasferiti dalle edge location di CloudFront nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata. Essi separano i dati in modo diverso, come segue:
  - Per protocollo: separa i dati per protocollo: HTTP o HTTPS.
  - Per destinazione: separa i dati per destinazione, ai visualizzatori o alla tua origine.

Il report di utilizzo di CloudFront si basa sul report di utilizzo AWS per CloudFront. Questo report non richiede alcuna configurazione aggiuntiva. Per ulteriori informazioni, consulta Visualizza il report sull'utilizzo per AWS CloudFront.

Puoi visualizzare report per un determinato intervallo di tempo negli ultimi 60 giorni, con punti dati ogni ora o ogni giorno. In genere, puoi visualizzare i dati sulle richieste che CloudFront ha ricevuto appena quattro ore prima, ma i dati possono talvolta essere ritardati fino a 24 ore.

Per ulteriori informazioni, consulta Relazione tra i grafici di utilizzo e i dati nel report di utilizzo di CloudFront.

Argomenti

Visualizzazione dei report di utilizzo di CloudFront nella console

Puoi visualizzare i report di utilizzo di CloudFront nella console.

Come visualizzare i report di utilizzo di CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione scegliere Reports (Report).
3. Nel riquadro CloudFront Usage Reports (Report di utilizzo di CloudFront) per Start Date (Data inizio) e End Date (Data fine), seleziona l'intervallo di date per il quale desideri visualizzare i grafici di utilizzo. Gli intervalli disponibili dipendono dal valore selezionato per Granularity (Granularità):

   - Daily (Giorno): per visualizzare grafici con un punto dati per giorno, seleziona qualsiasi intervallo di date negli ultimi 60 giorni.
   - Hourly (Ora): per visualizzare grafici con un punto dati per ogni ora, seleziona qualsiasi intervallo di date fino a 14 giorni negli ultimi 60 giorni.

   Date e ore sono in formato UTC.
4. In Granularity (Granularità) specifica se visualizzare un punto dati per giorno o per ora nei grafici. Se si specifichi un intervallo di date superiore a 14 giorni, l'opzione per specificare un punto dati per ora non è disponibile.
5. Per Billing Region (Regione fatturazione), scegli la regione di fatturazione di CloudFront che dispone dei dati che intendi visualizzare, oppure scegli All Regions (Tutte le regioni). I grafici di utilizzo includono dati per le richieste che CloudFront elabora nelle edge location nella regione specificata. La regione in cui CloudFront elabora le richieste può corrispondere o meno all'ubicazione dei visualizzatori.

Seleziona solo le regioni che sono incluse nella classe di prezzo della distribuzione. Altrimenti, i grafici di utilizzo probabilmente non conterranno alcun dato. Ad esempio, se scegli Price Class 200 (Categoria prezzo 200) per la tua distribuzione, le regioni di fatturazione Sud America e Australia non sono incluse, di conseguenza CloudFront probabilmente non elaborerà le richieste da tali regioni. Per ulteriori informazioni sulle classi di prezzo, consulta Prezzi di CloudFront.

6. Nell'elenco Distribution (Distribuzione), seleziona le distribuzioni per le quali intendi visualizzare i dati nei grafici di utilizzo:

   - Una singola distribuzione: i grafici visualizzano i dati per la distribuzione CloudFront selezionata. L'elenco Distribution (Distribuzione) visualizza l'ID della distribuzione e gli eventuali nomi di dominio alternativi (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include i nomi di dominio di origine per la distribuzione.
   - Tutte le distribuzioni (escluse quelle eliminate): i grafici visualizzano i dati sommati per tutte le distribuzioni associate all'account AWS corrente, escluse le distribuzioni che hai eliminato.
   - Tutte le distribuzioni eliminate: i grafici visualizzano i dati sommati per tutte le distribuzioni associate all'account AWS corrente ed eliminate negli ultimi 60 giorni.

7. Seleziona Aggiorna grafici.

> **Tip**
>
> - Per visualizzare i dati per un punto dati orario o giornaliero in un grafico, passa il mouse sul punto dati.
> - Per i grafici che mostrano i dati trasferiti, puoi impostare la scala verticale su gigabyte, megabyte o kilobyte.

Download di dati in formato CSV

Puoi scaricare il report di utilizzo in formato CSV. Questa sezione descrive come scaricare il report e i valori nel report.

Download del report di utilizzo in formato CSV

1. Durante la visualizzazione del report di utilizzo, scegli CSV.
2. Nella finestra di dialogo Opening file name (Apertura nome file), scegli se aprire o salvare il file.

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Version

La versione del formato per questo file CSV.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, `ALL` se hai eseguito il report per tutte le distribuzioni oppure `ALL_DELETED` se lo hai eseguito per tutte le distribuzioni eliminate.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Granularità

Se ogni riga nel report rappresenta un'ora o un giorno.

BillingRegion

Il continente da cui hanno origine le richieste visualizzatore, oppure `ALL`, se scegli di scaricare il report per tutte le regioni di fatturazione.

Dati nel report di utilizzo

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, `ALL` se hai eseguito il report per tutte le distribuzioni oppure `ALL_DELETED` se lo hai eseguito per tutte le distribuzioni eliminate.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

BillingRegion

La regione di fatturazione di CloudFront per la quale hai eseguito il report, oppure `ALL`.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

HTTP

Il numero di richieste HTTP a cui CloudFront ha risposto dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata. I valori includono:

- Il numero di richieste `GET` e `HEAD`, a seguito delle quali CloudFront trasferisce dati ai visualizzatori.
- Il numero di richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`, a seguito delle quali CloudFront trasferisce dati alla tua origine.

HTTPS

Il numero di richieste HTTPS a cui CloudFront ha risposto provenienti dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata. I valori includono:

- Il numero di richieste `GET` e `HEAD`, a seguito delle quali CloudFront trasferisce dati ai visualizzatori.
- Il numero di richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`, a seguito delle quali CloudFront trasferisce dati alla tua origine.

HTTPBytes

La quantità totale di dati trasferiti via HTTP dalle edge location di CloudFront nella regione di fatturazione selezionata durante il periodo di tempo per la distribuzione CloudFront specificata. I valori includono:

- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `GET` e `HEAD`.
- I dati trasferiti dai visualizzatori a CloudFront per le richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

HTTPSBytes

La quantità totale di dati trasferiti via HTTPS dalle edge location di CloudFront nella regione di fatturazione selezionata durante il periodo di tempo per la distribuzione CloudFront specificata. I valori includono:

- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `GET` e `HEAD`.
- I dati trasferiti dai visualizzatori a CloudFront per le richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

BytesIn

La quantità totale di dati trasferiti da CloudFront alla tua origine per le richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT` nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata.

BytesOut

La quantità totale di dati trasferiti via HTTP e HTTPS da CloudFront ai visualizzatori nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata. I valori includono:

- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `GET` e `HEAD`.
- I dati trasferiti da CloudFront ai visualizzatori in risposta alle richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

Relazione tra i grafici di utilizzo e i dati nel report di utilizzo di CloudFront

L'elenco seguente mostra come i grafici di utilizzo nella console di CloudFront corrispondono ai valori nella colonna Usage Type (Tipo di utilizzo) nel report di utilizzo di CloudFront.

Argomenti

- Number of Requests (Numero di richieste)
- Data Transferred by Protocol (Dati trasferiti per protocollo)
- Data Transferred by Destination (Dati trasferiti per destinazione)

Number of Requests (Numero di richieste)

Questo grafico mostra il numero totale di richieste a cui CloudFront risponde da edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata, separate da protocollo (HTTP o HTTPS) e tipo (statico, dinamico o proxy).

Number of HTTP Requests (Numero di richieste HTTP)

- *regione*-Requests-HTTP-Static: il numero di richieste HTTP `GET` e `HEAD` servite per oggetti con TTL ≥ 3600 secondi.
- *regione*-Requests-HTTP-Dynamic: il numero di richieste HTTP `GET` e `HEAD` servite per oggetti con TTL < 3600 secondi
- *regione*-Requests-HTTP-Proxy: il numero di richieste HTTP `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT` che CloudFront inoltra alla tua origine

Number of HTTPS Requests (Numero di richieste HTTPS)

- *regione*-Requests-HTTPS-Static: il numero di richieste HTTPS `GET` e `HEAD` servite per oggetti con TTL ≥ 3600 secondi.
- *regione*-Requests-HTTPS-Dynamic: il numero di richieste HTTPS `GET` e `HEAD` servite per oggetti con TTL < 3600 secondi
- *regione*-Requests-HTTPS-Proxy: il numero di richieste HTTPS `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT` che CloudFront inoltra alla tua origine

Data Transferred by Protocol (Dati trasferiti per protocollo)

Questo grafico mostra la quantità totale di dati trasferiti dalle posizioni edge CloudFront nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata, separati per protocollo (HTTP o HTTPS), tipo (statico, dinamico o proxy) e destinazione (visualizzatori o origine).

Data Transferred over HTTP (Dati trasferiti via HTTP)

- *regione*-Out-Bytes-HTTP-Static: byte serviti via HTTP per oggetti con TTL ≥ 3600 secondi.
- *regione*-Out-Bytes-HTTP-Dynamic: byte serviti via HTTP per oggetti con TTL < 3600 secondi
- *regione*-Out-Bytes-HTTP-Proxy: byte restituiti da CloudFront a visualizzatori via HTTP in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- *regione*-Out-OBytes-HTTP-Proxy: totale dei byte trasferiti via HTTP da edge location di CloudFront alla tua origine in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

Data Transferred over HTTPS (Dati trasferiti via HTTPS)

- *regione*-Out-Bytes-HTTPS-Static: byte serviti via HTTPS per oggetti con TTL ≥ 3600 secondi
- *region*-Out-Bytes-HTTPS-Dynamic: byte serviti via HTTPS per oggetti con TTL <3600 secondi
- *regione*-Out-Bytes-HTTPS-Proxy: byte restituiti da CloudFront a visualizzatori via HTTPS in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- *regione*-Out-OBytes-HTTPS-Proxy: totale dei byte trasferiti via HTTPS da edge location di CloudFront alla tua origine in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

Data Transferred by Destination (Dati trasferiti per destinazione)

Questo grafico mostra la quantità totale di dati trasferiti dalle posizioni edge CloudFront nella regione selezionata durante ogni intervallo di tempo per la distribuzione CloudFront specificata, separati per destinazione (visualizzatori o origine), protocollo (HTTP o HTTPS) e tipo (statico, dinamico o proxy).

Dati trasferiti da CloudFront ai visualizzatori

- *regione*-Out-Bytes-HTTP-Static: byte serviti via HTTP per oggetti con TTL ≥ 3600 secondi.
- *regione*-Out-Bytes-HTTPS-Static: byte serviti via HTTPS per oggetti con TTL ≥ 3600 secondi
- *regione*-Out-Bytes-HTTP-Dynamic: byte serviti via HTTP per oggetti con TTL < 3600 secondi
- *region*-Out-Bytes-HTTPS-Dynamic: byte serviti via HTTPS per oggetti con TTL <3600 secondi
- *regione*-Out-Bytes-HTTP-Proxy: byte restituiti da CloudFront a visualizzatori via HTTP in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- *regione*-Out-Bytes-HTTPS-Proxy: byte restituiti da CloudFront a visualizzatori via HTTPS in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

Dati trasferiti da CloudFront a Origin

- *regione*-Out-OBytes-HTTP-Proxy: totale dei byte trasferiti via HTTP da edge location di CloudFront alla tua origine in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.
- *regione*-Out-OBytes-HTTPS-Proxy: totale dei byte trasferiti via HTTPS da edge location di CloudFront alla tua origine in risposta a richieste `DELETE`, `OPTIONS`, `PATCH`, `POST` e `PUT`.

Visualizzazione dei report sui visualizzatori di CloudFront

I report sui visualizzatori di CloudFront includono le informazioni seguenti per qualsiasi intervallo di date negli ultimi 60 giorni:

- Dispositivi: i tipi di dispositivi utilizzati più frequentemente per accedere ai contenuti (ad esempio, desktop o dispositivi mobili)
- Browser: i 10 browser più utilizzati per accedere ai contenuti (ad esempio, Chrome o Firefox)
- Sistemi operativi: i 10 sistemi operativi più utilizzati per accedere ai contenuti (ad esempio, Linux, macOS o Windows)
- Località: le prime 50 località (paesi o stati/territori degli Stati Uniti) dei visualizzatori che accedono più frequentemente ai contenuti
  - Puoi anche visualizzare le località con punti dati orari per qualsiasi intervallo di date fino a 14 giorni nei 60 giorni precedenti.

> **Note**
>
> Non è necessario abilitare la registrazione degli accessi per visualizzare i grafici e i report relativi ai visualizzatori.

Argomenti

Visualizzazione di grafici e report su visualizzatori nella console

Puoi visualizzate grafici e report su visualizzatori di CloudFront nella console.

Come visualizzare grafici e report di CloudFront Viewers

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Visualizzatori.
3. Nel riquadro CloudFront Viewers (Visualizzatori CF) per Start Date (Data inizio) e End Date (Data fine), seleziona l'intervallo di date per il quale desideri visualizzare grafici e report sui visualizzatori.

Per il grafico sulle ubicazioni, gli intervalli disponibili dipendono dal valore selezionato per Granularity (Granularità):

- Daily (Giorno): per visualizzare grafici con un punto dati per giorno, seleziona qualsiasi intervallo di date negli ultimi 60 giorni.
- Hourly (Ora): per visualizzare grafici con un punto dati per ogni ora, seleziona qualsiasi intervallo di date fino a 14 giorni negli ultimi 60 giorni.

Date e ore sono in formato UTC.

4. (Solo grafici su browser e sistemi operativi) Per Grouping (Raggruppamento), specifica se intendi raggruppare browser e sistemi operativi per nome (Chrome, Firefox) oppure per nome e versione (Chrome 40.0, Firefox 35.0).
5. (Solo grafico sulle ubicazioni) Per Granularity (Granularità), specifica se visualizzare un punto dati per giorno o per ora nei grafici. Se si specifichi un intervallo di date superiore a 14 giorni, l'opzione per specificare un punto dati per ora non è disponibile.
6. (Solo grafico sulle ubicazioni) Per Details (Dettagli), specifica se visualizzare le principali ubicazioni per paese o per stato degli Stati Uniti.
7. Nell'elenco Distribution (Distribuzione), seleziona la distribuzione per la quale intendi visualizzare i dati nei grafici di utilizzo:

   - Una singola distribuzione: i grafici visualizzano i dati per la distribuzione CloudFront selezionata. L'elenco Distribution (Distribuzione) visualizza l'ID della distribuzione e un eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.
   - Tutte le distribuzioni (escluse quelle eliminate): i grafici visualizzano i dati sommati per tutte le distribuzioni associate all'account AWS corrente, escluse le distribuzioni che hai eliminato.
8. Scegliere Aggiorna.

Per visualizzare i dati per un punto dati orario o giornaliero in un grafico, passa il mouse sul punto dati.

Download di dati in formato CSV

Puoi scaricare ogni report sui visualizzatori in formato CSV. Questa sezione descrive come scaricare i report e i valori nel report.

Download dei report sui visualizzatori in formato CSV

1. Durante la visualizzazione del report sui visualizzatori, scegli CSV.
2. Scegli i dati che intendi scaricare, ad esempio, Devices (Dispositivi) o Devices Trends (Trend dispositivi).
3. Nella finestra di dialogo Opening file name (Apertura nome file), scegli se aprire o salvare il file.

Dati inclusi nei report sui visualizzatori

Le prime righe di ogni report includono le seguenti informazioni:

Versione

La versione del formato per questo file CSV.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Grouping (Raggruppamento) (solo report su browser e sistemi operativi)

Raggruppamento dei dati per nome o per nome e versione del browser o del sistema operativo.

Granularità

Se ogni riga nel report rappresenta un'ora o un giorno.

Details (Dettagli) (solo report su ubicazioni)

Elenco delle richieste per paese o per stato degli Stati Uniti.

I seguenti argomenti descrivono le informazioni contenute nei diversi report sui visualizzatori.

Argomenti

Report sui dispositivi

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

Richieste

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di dispositivo.

RequestsPct

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di dispositivo come percentuale del numero totale di richieste che CloudFront ha ricevuto da tutti i dispositivi.

Personalizza

Le richieste per le quali il valore dell'intestazione HTTP `User-Agent` non era associato a uno dei tipi di dispositivo standard, ad esempio, `Desktop` o `Mobile`.

Report sui trend per dispositivi

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

Desktop

Il numero di richieste che CloudFront ha ricevuto da computer desktop durante il periodo.

Mobile

Il numero di richieste che CloudFront ha ricevuto da dispositivi mobili durante il periodo. I dispositivi mobili possono includere tablet e cellulari. Nel caso in cui CloudFront non possa determinare se l'origine di una richiesta è un dispositivo mobile o un tablet, la richiesta viene conteggiata nella colonna `Mobile`.

Smart TV

Il numero di richieste che CloudFront ha ricevuto da dispositivi smart TV durante il periodo.

Tablet

Il numero di richieste che CloudFront ha ricevuto da tablet durante il periodo. Nel caso in cui CloudFront non possa determinare se l'origine di una richiesta è un dispositivo mobile o un tablet, la richiesta viene conteggiata nella colonna `Mobile`.

Sconosciuto

Le richieste per le quali il valore dell'intestazione HTTP `User-Agent` non era associato a uno dei tipi di dispositivo standard, ad esempio, `Desktop` o `Mobile`.

Empty (Vuoto)

Il numero di richieste che CloudFront ha ricevuto e che non includevano un valore nell'intestazione HTTP `User-Agent` durante il periodo.

Report sui browser

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

Group (Gruppo)

Il browser o il browser e la versione da cui CloudFront ha ricevuto le richieste, a seconda del valore di `Grouping`. Oltre a nomi di browser, i valori possibili sono:

- Bot/Crawler: soprattutto richieste da motori di ricerca che indicizzano il tuo contenuto.
- Empty (Vuoto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` era vuoto.
- Other (Altro): browser che CloudFront ha identificato ma che non sono tra quelli più popolari. Se `Bot/Crawler`, `Empty` e/o `Unknown` non appaiono tra i primi nove valori, sono inclusi anche in `Other`.
- Unknown (Sconosciuto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` non era associato a un browser standard. La maggior parte delle richieste in questa categoria proviene da script o applicazioni personalizzate.

Richieste

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di browser.

RequestsPct

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di browser come percentuale del numero totale di richieste che CloudFront ha ricevuto durante il periodo di tempo.

Report sui trend per browser

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

(Browsers) (Browser)

Le colonne rimanenti nel report elencano i browser o i browser e le relative versioni, a seconda del valore di `Grouping`. Oltre a nomi di browser, i valori possibili sono:

- Bot/Crawler: soprattutto richieste da motori di ricerca che indicizzano il tuo contenuto.
- Empty (Vuoto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` era vuoto.
- Other (Altro): browser che CloudFront ha identificato ma che non sono tra quelli più popolari. Se `Bot/Crawler`, `Empty` e/o `Unknown` non appaiono tra i primi nove valori, sono inclusi anche in `Other`.
- Unknown (Sconosciuto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` non era associato a un browser standard. La maggior parte delle richieste in questa categoria proviene da script o applicazioni personalizzate.

Report sui sistemi operativi

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

Group (Gruppo)

Il sistema operativo o il sistema operativo e la versione da cui CloudFront ha ricevuto le richieste, a seconda del valore di `Grouping`. Oltre a nomi di sistemi operativi, i valori possibili sono:

- Bot/Crawler: soprattutto richieste da motori di ricerca che indicizzano il tuo contenuto.
- Empty (Vuoto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` era vuoto.
- Other (Altro): sistemi operativi che CloudFront ha identificato ma che non sono tra quelli più popolari. Se `Bot/Crawler`, `Empty` e/o `Unknown` non appaiono tra i primi nove valori, sono inclusi anche in `Other`.
- Unknown (Sconosciuto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` non era associato a un browser standard. La maggior parte delle richieste in questa categoria proviene da script o applicazioni personalizzate.

Richieste

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di sistema operativo.

RequestsPct

Il numero di richieste che CloudFront ha ricevuto da ogni tipo di sistema operativo come percentuale del numero totale di richieste che CloudFront ha ricevuto durante il periodo di tempo.

Report sui trend per sistemi operativi

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

(Operating systems) (Sistemi operativi)

Le altre colonne nel report elencano i sistemi operativi o i sistemi operativi e le relative versioni, a seconda del valore di `Grouping`. Oltre a nomi di sistemi operativi, i valori possibili sono:

- Bot/Crawler: soprattutto richieste da motori di ricerca che indicizzano il tuo contenuto.
- Empty (Vuoto): richieste per le quali il valore dell'intestazione HTTP `User-Agent` era vuoto.
- Other (Altro): sistemi operativi che CloudFront ha identificato ma che non sono tra quelli più popolari. Se `Bot/Crawler`, `Empty` e/o `Unknown` non appaiono tra i primi nove valori, sono inclusi anche in `Other`.
- Unknown (Sconosciuto): richieste per le quali il sistema operativo non è specificato nell'intestazione HTTP `User-Agent`.

Report sulle ubicazioni

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

LocationCode

L'abbreviazione per l'ubicazione da cui CloudFront ha ricevuto richieste. Per ulteriori informazioni sui possibili valori, consulta la descrizione di Location (Ubicazione) in Come i dati nel report sulle ubicazioni sono collegati ai dati nei log standard di CloudFront (log di accesso).

LocationName

Il nome dell'ubicazione da cui CloudFront ha ricevuto richieste.

Richieste

Il numero di richieste che CloudFront ha ricevuto da ogni edge location.

RequestsPct

Il numero di richieste che CloudFront ha ricevuto da ogni ubicazione come percentuale del numero totale di richieste che CloudFront ha ricevuto da tutte le ubicazioni durante il periodo di tempo.

TotalBytes

Il numero di byte che CloudFront ha servito ai visualizzatori in questo paese o stato, per la distribuzione e il periodo specificati.

Report sui trend per ubicazioni

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per la quale hai eseguito il report, oppure `ALL` se hai eseguito il report per tutte le distribuzioni.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

(Locations) (Ubicazioni)

Le altre colonne nel report elencano le ubicazioni da cui CloudFront ha ricevuto richieste. Per ulteriori informazioni sui possibili valori, consulta la descrizione di Location (Ubicazione) in

Come i dati nel report sulle ubicazioni sono collegati ai dati nei log standard di CloudFront (log di accesso).

Come i dati nel report sulle ubicazioni sono collegati ai dati nei log standard di CloudFront (log di accesso)

L'elenco seguente mostra come i dati nel report sulle ubicazioni nella console di CloudFront corrispondono ai valori nei log di accesso di CloudFront. Per ulteriori informazioni sui log degli accessi di CloudFront, consultare Registri di accesso (registri standard).

Ubicazione

Il paese o lo stato degli Stati Uniti in cui si trova il visualizzatore. Nei log di accesso, la colonna `c-ip` contiene l'indirizzo IP del dispositivo in cui il visualizzatore è in esecuzione. Utilizziamo dati di geolocalizzazione per identificare l'ubicazione geografica del dispositivo in base all'indirizzo IP.

Se stai visualizzando il report sulle località per paese, l'elenco di paesi è basato sulla norma ISO 3166-2, Codici per la rappresentazione dei nomi di paesi e delle relative suddivisioni – Parte 2: codici delle suddivisioni dei paesi. L'elenco di paesi include i seguenti valori supplementari:

- Anonymous Proxy (Proxy anonimo): la richiesta originata da un proxy anonimo.
- Satellite Provider (Provider satellitare): la richiesta originata da un provider satellitare che fornisce servizi Internet a più paesi. I visualizzatori potrebbero trovarsi in paesi con un elevato rischio di frode.
- Europe (Unknown) (Europa (Sconosciuto)): la richiesta originata da un IP in un blocco utilizzato da più paesi europei. Il paese da cui proviene la richiesta non può essere determinato. CloudFront utilizza Europe (Unknown) (Europa (Sconosciuto)) come valore di default.
- Asia/Pacific (Unknown) (Asia Pacifico (Sconosciuto)): la richiesta originata da un IP in un blocco utilizzato da più paesi nella regione Asia Pacifico. Il paese da cui proviene la richiesta non può essere determinato. CloudFront utilizza Asia/Pacific (Unknown) (Asia Pacifico (Sconosciuto)) come valore di default.

Se visualizzi il report sulle Locations (Ubicazioni) per stato degli Stati Uniti, nota che il report può includere territori e regioni militari statunitensi.

> **Note**
>
> Se CloudFront non è in grado di determinare la posizione di un utente, questa verrà visualizzata come sconosciuta nei report del visualizzatore.

Request Count (Numero richieste)

Il numero totale di richieste dal paese o stato degli Stati Uniti in cui si trova il visualizzatore, per la distribuzione e il periodo specificati. Questo valore in genere è prossimo al numero di richieste `GET` provenienti da indirizzi IP in quel paese o stato nei log di accesso di CloudFront.

Richiesta %

Una delle seguenti opzioni, a seconda del valore selezionato per Details (Dettagli):

- Countries (Paesi): le richieste da questo paese come percentuale del numero totale di richieste.
- Stati (Stati Uniti): le richieste da questo stato come percentuale del numero totale di richieste provenienti dagli Stati Uniti.

Se le richieste provengono da più di 50 paesi, non puoi calcolare Request % (% richieste) in base ai dati in questa tabella poiché la colonna Request Count (Numero richieste) non include tutte le richieste durante il periodo specificato.

Byte

Il numero di byte che CloudFront ha servito ai visualizzatori in questo paese o stato, per la distribuzione e il periodo specificati. Per visualizzare i dati in questa colonna in KB, MB o GB, scegli il collegamento nell'intestazione della colonna.

Monitoraggio delle metriche CloudFront con Amazon CloudWatch

Amazon CloudFront è integrato con Amazon CloudWatch e pubblica automaticamente le metriche operative per le distribuzioni e le funzioni edge (sia Lambda@Edge che Funzioni CloudFront). Puoi usare queste metriche per risolvere, tenere traccia ed eseguire il debug dei problemi. Molti di questi parametri vengono visualizzati in una serie di grafici nella Console CloudFront e sono anche accessibili utilizzando l'API o la CLI di CloudFront. Tutti i parametri sono disponibili nella console CloudWatcho tramite l'API o la CLI di CloudWatch. Le metriche CloudFront non vengono conteggiate nelle quote di CloudWatch (precedentemente note come limiti) e non comportano alcun costo aggiuntivo.

Oltre ai parametri predefiniti, è possibile abilitare ulteriori parametri a un costo aggiuntivo. I parametri aggiuntivi si applicano alle distribuzioni CloudFront e devono essere abilitati separatamente per ciascuna distribuzione. Per ulteriori informazioni sui costi, consulta the section called “Stima dei costi per le metriche aggiuntive di CloudFront”.

Puoi anche impostare gli allarmi in base a queste metriche nella console CloudFront o nella console CloudWatch, nell'API o nella CLI. Ad esempio, è possibile impostare un allarme in base al parametro `5xxErrorRate`, che rappresenta la percentuale di tutte le richieste del visualizzatore per le quali il codice di stato HTTP della risposta è compreso nell'intervallo da `500` a `599`. Quando il tasso di errore raggiunge un determinato valore per un determinato periodo di tempo, ad esempio il 5% delle richieste per 5 minuti continui, l'allarme viene attivato. Quando si crea l'allarme, è possibile specificare il valore dell'allarme e la relativa unità di tempo.

> **Note**
>
> - Quando crei un allarme CloudWatch nella console CloudFront, uno viene creato automaticamente nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`). Se crei un allarme dalla console CloudWatch, devi usare la stessa Regione. Poiché CloudFront è un servizio globale, le metriche per il servizio vengono inviate a Stati Uniti orientali (Virginia settentrionale).
> - Quando si creano allarmi, si applicano i prezzi standard di CloudWatch.

Argomenti

Visualizzazione delle metriche delle funzioni di CloudFront ed edge

È possibile visualizzare i parametri operativi relativi alle distribuzioni CloudFront e alle funzioni edge nella console CloudFront.

Come visualizzare le metriche delle funzioni CloudFront ed edge in CloudFront

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Monitoring (Monitoraggio).
3. Per visualizzare i grafici relativi all'attività per una distribuzione CloudFront o una funzione edge, sceglierne una, quindi scegliere View distribution metrics (Visualizza parametri di distribuzione) oppure View metrics (Visualizza parametri).
4. Puoi personalizzare i grafici nel modo seguente:
   a. Per modificare l'intervallo di tempo per le informazioni visualizzate nel grafico, scegliere 1h (1 ora), 3h (3 ore) o a un altro intervallo, oppure specificare un intervallo personalizzato.
   b. Per modificare la frequenza con cui CloudFront aggiorna le informazioni contenute nel grafico, scegliere la freccia giù accanto all'icona di aggiornamento, quindi selezionare un intervallo di aggiornamento. La velocità di aggiornamento predefinita è di 1 minuto, ma è possibile scegliere altre opzioni.
5. Per visualizzare i grafici CloudFront nella console CloudWatch, scegliere Aggiungi al dashboard. È necessario utilizzare la Regione Stati Uniti orientali (Virginia Settentrionale) per visualizzare i grafici nella console CloudWatch.

Argomenti

Metriche di distribuzione predefinite di CloudFront

I seguenti parametri predefiniti sono inclusi per tutte le distribuzioni CloudFront, senza costi aggiuntivi:

Richieste

Il numero totale di richieste di visualizzatore ricevute da CloudFront, per tutti i metodi HTTP e per le richieste HTTP e HTTPS.

Byte scaricati

Il numero totale di byte scaricati dai visualizzatori per le richieste `GET` e `HEAD`.

Byte caricati

Il numero totale di byte caricati dai visualizzatori in CloudFront, tramite le richieste `OPTIONS`, `POST` e `PUT`.

Frequenza di errore 4xx

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `4xx`.

Frequenza di errore 5xx

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `5xx`.

Frequenza di errore totale

Percentuale di tutte le richieste del visualizzatore per le quali il codice di stato HTTP della risposta è `4xx` o `5xx`.

Queste metriche sono mostrate nei grafici per ogni distribuzione CloudFront nella pagina Monitoraggio della console CloudFront. Su ogni grafico, i totali vengono visualizzati con granularità di 1 minuto. Oltre a visualizzare i grafici, è anche possibile scaricare i report delle metriche come file CSV.

Attivazione di ulteriori metriche di distribuzione CloudFront

Oltre ai parametri predefiniti, è possibile attivare ulteriori parametri a un costo aggiuntivo. Per ulteriori informazioni sui costi, consulta the section called “Stima dei costi per le metriche aggiuntive di CloudFront”.

Tali parametri aggiuntivi devono essere attivati separatamente per ogni distribuzione:

Percentuale di riscontri nella cache

La percentuale di richieste che possono essere memorizzate nella cache per le quali CloudFront ha fornito il contenuto dalla propria cache. Le richieste HTTP `POST` e `PUT` e gli errori non sono considerati memorizzabili nella cache.

Latenza di origine

Il tempo totale trascorso da quando CloudFront riceve una richiesta a quando inizia a fornire una risposta alla rete (non al visualizzatore), per le richieste che vengono servite dall'origine, non dalla cache CloudFront. Questo è anche noto come latenza di primo byte, o time-to-first-byte.

Tasso di errore per codice di stato

La percentuale di tutte le richieste del visualizzatore per le quali il codice di stato HTTP della risposta è un codice particolare nell'intervallo `4xx` o `5xx`. Questa metrica è disponibile per tutti i seguenti codici di errore: `401`, `403`, `404`, `502`, `503` e `504`.

È possibile attivare parametri aggiuntivi nella console CloudFront, con CloudFormation, con l'AWS Command Line Interface (AWS CLI) o con l'API CloudFront.

Console

Come attivare metriche aggiuntive

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Monitoring (Monitoraggio).
3. Scegliere la distribuzione per cui attivare ulteriori parametri, quindi scegliere View distribution metrics (Visualizza parametri di distribuzione).
4. Scegliere Manage additional metrics (Gestisci parametri aggiuntivi).
5. Nella finestra Manage additional metrics (Gestisci parametri aggiuntivi), attiva Enabled (Abilitato). Dopo aver abilitato i parametri aggiuntivi, puoi chiudere la finestra Manage additional metrics (Gestisci parametri aggiuntivi).

   Dopo aver abilitato i parametri aggiuntivi, questi vengono visualizzati nei grafici. Su ogni grafico, i totali vengono visualizzati con granularità di 1 minuto. Oltre a visualizzare i grafici, è anche possibile scaricare i report delle metriche come file CSV.

CloudFormation

Per attivare metriche aggiuntive con CloudFormation, utilizza il tipo di risorsa `AWS::CloudFront::MonitoringSubscription`. L'esempio seguente mostra la sintassi del modello CloudFormation, in formato YAML, per l'abilitazione di parametri aggiuntivi.

```
Type: AWS::CloudFront::MonitoringSubscription
Properties:
  DistributionId: EDFDVBD6EXAMPLE
  MonitoringSubscription:
    RealtimeMetricsSubscriptionConfig:
      RealtimeMetricsSubscriptionStatus: Enabled
```

CLI

Per gestire parametri aggiuntivi con AWS Command Line Interface (AWS CLI), utilizzare uno dei seguenti comandi:

Come attivare metriche aggiuntive per una distribuzione

- Utilizza il comando create-monitoring-subscription come nell'esempio seguente. Sostituisci *EDFDVBD6EXAMPLE* con l'ID della distribuzione per la quale stai abilitando metriche aggiuntive.

```
aws cloudfront create-monitoring-subscription --
distribution-id EDFDVBD6EXAMPLE --monitoring-subscription
 RealtimeMetricsSubscriptionConfig={RealtimeMetricsSubscriptionStatus=Enabled}
```

Come vedere se sono attivate metriche aggiuntive per una distribuzione

- Utilizza il comando get-monitoring-subscription come nell'esempio seguente. Sostituisci *EDFDVBD6EXAMPLE* con l'ID della distribuzione che stai controllando.

```
aws cloudfront get-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

Come disattivare metriche aggiuntive per una distribuzione

- Utilizza il comando delete-monitoring-subscription come nell'esempio seguente. Sostituisci *EDFDVBD6EXAMPLE* con l'ID della distribuzione per la quale stai disattivando metriche aggiuntive.

```
aws cloudfront delete-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

API

Per gestire metriche aggiuntive con l'API CloudFront, utilizzare una delle seguenti operazioni API.

- Per abilitare parametri aggiuntivi per una distribuzione, utilizzare CreateMonitoringSubscription.
- Per verificare se sono abilitati parametri aggiuntivi per una distribuzione, utilizzare GetMonitoringSubscription.
- Per disattivare parametri aggiuntivi per una distribuzione, utilizzare DeleteMonitoringSubscription.

Per ulteriori informazioni su queste operazioni API, consulta la documentazione di riferimento delle API per l'SDK AWS o un altro client API.

Stima dei costi per le metriche aggiuntive di CloudFront

Quando si abilitano parametri aggiuntivi per una distribuzione, CloudFront invia fino a 8 parametri a CloudWatch nella regione Stati Uniti orientali (Virginia settentrionale). CloudWatch addebita una tariffa fissa bassa per ogni metrica. Questa tariffa viene addebitata una sola volta al mese per parametro (fino a otto parametri per distribuzione). Si tratta di una tariffa fissa, pertanto i costi restano invariati indipendentemente dal numero di richieste o risposte che la distribuzione CloudFront riceve o invia. Per la tariffa per parametro, consultare la pagina dei prezzi di Amazon CloudWatch e il calcolatore dei prezzi di CloudWatch. Quando si recuperano i parametri mediante l'API CloudWatch, vengono applicati addebiti aggiuntivi per le API.

Metriche predefinite della funzione Lambda@Edge

È possibile utilizzare i parametri CloudWatch per monitorare in tempo reale i problemi con le funzioni Lambda@Edge. Non sono previsti costi aggiuntivi per l'utilizzo di questi parametri.

Quando colleghi una funzione Lambda@Edge a un comportamento della cache in una distribuzione CloudFront, Lambda inizia a inviare i parametri a CloudWatch in modo automatico. I parametri sono disponibili per tutte le regioni Lambda, ma per visualizzare le metriche nella console CloudWatch o ottenere i dati delle metriche dall'API CloudWatch, è necessario utilizzare l'area Stati Uniti orientali (Virginia settentrionale) (`us-east-1`). Il nome del gruppo di parametri ha il seguente formato: `AWS/CloudFront/`*`distribution-ID`*, dove *`distribution-ID`* è l'ID della distribuzione CloudFront a

cui è associata la funzione Lambda@Edge. Per ulteriori informazioni sulle metriche di CloudWatch, consulta la Guida per l'utente di Amazon CloudWatch.

Queste metriche predefinite vengono mostrate nei grafici per ogni funzione Lambda@Edge nella pagina Monitoraggio della console CloudFront:

- `5xx`Frequenza di errore per Lambda@Edge
- Errori di esecuzione Lambda
- Risposte non valide Lambda
- Throttle Lambda

I grafici includono il numero di chiamate, errori, throttle e così via. Su ogni grafico, i totali vengono visualizzati con granularità di 1 minuto, raggruppati in base alla regione AWS.

Se viene registrato un picco di errori che si desidera analizzare, ad esempio, puoi scegliere una funzione e quindi visualizzare i file di log in base alla regione AWS, finché non determini la funzione che causa i problemi e in quale regione AWS. Per ulteriori informazioni sulla risoluzione di errori Lambda@Edge, consulta:

- the section called “Come stabilire il tipo di errore”
- Quattro passaggi per eseguire il debug della distribuzione dei contenuti in AWS

Metriche predefinite di Funzioni CloudFront

CloudFront Functions invia i parametri operativi ad Amazon CloudWatch in modo che tu possa monitorare le tue funzioni. La visualizzazione di queste metriche consente di risolvere, tenere traccia ed eseguire il debug dei problemi. CloudFront Functions pubblica i seguenti parametri su CloudWatch:

- Richiami (`FunctionInvocations`): il numero di volte in cui la funzione è stata avviata (richiamata) in un determinato periodo di tempo.
- Errori di convalida (`FunctionValidationErrors`): il numero di errori di convalida prodotti dalla funzione in un determinato periodo di tempo. Gli errori di convalida si verificano quando la funzione viene eseguita correttamente ma restituisce dati non validi (un oggetto evento non valido).
- Errori di esecuzione (`FunctionExecutionErrors`): il numero di errori di esecuzione che si sono verificati in un determinato periodo di tempo. Gli errori di esecuzione si verificano quando la funzione non viene completata correttamente.

- Utilizzo del calcolo (`FunctionComputeUtilization`): la quantità di tempo impiegata per l'esecuzione della funzione come percentuale del tempo massimo consentito. Ad esempio, un valore pari a 35 significa che la funzione è stata completata nel 35% del tempo massimo consentito. Questo parametro è un numero compreso tra 0 e 100.

  Se questo valore raggiunge o si avvicina a 100, la funzione ha utilizzato o sta per utilizzare il tempo di esecuzione consentito e le richieste successive potrebbero essere limitate. Se la funzione è in esecuzione con un utilizzo pari o superiore all'80%, ti consigliamo di rivedere la funzione per ridurre il tempo di esecuzione e migliorare l'utilizzo. Ad esempio, potrebbe essere necessario registrare solo gli errori, semplificare eventuali espressioni regolari complesse o rimuovere l'analisi non necessaria di oggetti JSON complessi.
- Throttle (`FunctionThrottles`): il numero di volte in cui la funzione è stata limitata in un determinato periodo di tempo. Le funzioni possono essere limitate per i seguenti motivi:
  - La funzione supera continuamente il tempo massimo consentito per l'esecuzione
  - La funzione provoca errori di compilazione
  - Il numero di richieste al secondo è insolitamente elevato

KeyValueStore di CloudFront invia anche le seguenti metriche operative ad Amazon CloudWatch:

- Richieste di lettura (`KvsReadRequests`): il numero di volte in cui la funzione ha letto correttamente dall'archivio di valori delle chiavi in un determinato periodo di tempo.
- Errori di lettura (`KvsReadErrors`): Il numero di volte in cui la funzione non è riuscita a leggere dall'archivio di valori delle chiavi entro un determinato periodo di tempo.

Tutti questi parametri vengono pubblicati su CloudWatch nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), nello spazio dei nomi CloudFront. Puoi visualizzare tali parametri anche dalla console CloudWatch. Nella console CloudWatch, puoi visualizzare i parametri in base alla funzione o in base alla funzione per distribuzione.

Puoi anche usare CloudWatch per impostare gli allarmi in base ai parametri. Ad esempio, puoi impostare un avviso in base al parametro del tempo di esecuzione (`FunctionComputeUtilization`), che rappresenta la percentuale di tempo disponibile impiegato dalla funzione per l'esecuzione. Quando il tempo di esecuzione raggiunge un determinato valore per un periodo di tempo specifico. Ad esempio, se si sceglie un valore superiore al 70% del tempo disponibile per 15 minuti consecutivi, l'allarme viene attivato. Quando si crea l'allarme, è possibile specificare il valore dell'allarme e la relativa unità di tempo.

> **Note**
>
> Funzioni CloudFront invia parametri a CloudWatch solo per le funzioni che si trovano nella fase `LIVE` che vengono eseguite in risposta alle richieste di produzione e alle risposte. Durante il test di una funzione, CloudFront non invia alcun parametro a CloudWatch. L'output del test contiene informazioni su errori, utilizzo del calcolo e log delle funzioni (istruzioni `console.log()`), ma queste informazioni non vengono inviate a CloudWatch.

Per informazioni su come ottenere questi parametri con l'API CloudWatch, consulta the section called "Metriche CloudFront".

Creazione di allarmi per i parametri di

Nella console CloudFront, è possibile impostare gli allarmi per la notifica tramite Amazon Simple Notification Service (Amazon SNS) in base a specifiche metriche CloudFront.

Come creare allarmi per le metriche

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel pannello di navigazione, seleziona Alarms (Allarmi).
3. Selezionare Create Alarm (Crea allarme).
4. Per Dettagli, specifica quanto segue:
   a. Nome allarme: un nome per l'allarme.
   b. Distribuzione: la distribuzione CloudFront per cui stai creando l'allarme.
5. Per Condizione, specifica quanto segue:
   a. Metrica: la metrica per cui stai creando l'allarme.
   b. "IF" <condizione>: la soglia quando CloudWatch deve attivare un allarme e inviare una notifica all'argomento Amazon SNS. Ad esempio, per ricevere una notifica quando il tasso di errore `5xx` supera l'1%, specificare quanto segue:

      Tasso di errore 5xx > 1
   c. "FOR" periodi consecutivi: periodo di tempo durante il quale la condizione deve essere soddisfatta prima che venga attivato un allarme. Quando si sceglie un valore, puntare a un

giusto equilibrio tra un valore che non attivi allarmi per problemi temporanei, ma attivi allarmi per problemi persistenti o reali.

d. (Facoltativo) Notifica: l'argomento Amazon SNS a cui inviare una notifica se questa metrica attiva un allarme.

6. Scegli Crea allarme.

> **Note**
>
> - Quando inserisci i valori per la condizione, usa numeri interi senza punteggiatura. Ad esempio, per specificare mille, immetti **`1000`**.
> - Per i tassi di errore `4xx`, `5xx` e totali, il valore che specifichi è una percentuale.
> - Per le richieste, i byte scaricati e i byte caricati, il valore specificato è unità. Ad esempio, 1073742000 byte.

Per ulteriori informazioni sulla creazione di argomenti Amazon SNS, consulta Creazione di un argomento Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Download di dati sulle metriche in formato CSV

È possibile scaricare i dati delle metriche CloudWatch per una distribuzione CloudFront in formato CSV.

Come eseguire il download di dati sulle metriche in formato CSV

1. Accedi alla Console di gestione AWS e apri la console CloudFront all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Monitoring (Monitoraggio).
3. Scegli la distribuzione, quindi seleziona Visualizza metriche di distribuzione.
4. Scegli Scarica CSV, quindi seleziona il periodo di tempo (ad esempio, Nell'ultimo giorno (periodo di 1 ora).
5. Dopo aver scaricato il file, aprilo per visualizzare le seguenti informazioni.

Argomenti

- Informazioni sul report

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Version

La versione dei report di CloudFront.

Report

Il nome del report.

DistributionID

L'ID della distribuzione per cui è stato eseguito il report.

StartDateUTC

La data d'inizio dell'intervallo di date per il quale esegui il report, in formato UTC.

EndDateUTC

La data di fine dell'intervallo di date per il quale esegui il report, in formato UTC.

GeneratedTimeUTC

La data e l'ora alla quale hai eseguito il report, in formato UTC.

Granularità

Il periodo di tempo per ogni riga nel report, ad esempio, `ONE_MINUTE`.

Dati nel report dei parametri

Il report include i seguenti valori:

DistributionID

L'ID della distribuzione per cui è stato eseguito il report.

FriendlyName

L'eventuale nome di dominio alternativo (CNAME) per la distribuzione. Se una distribuzione non ha nomi di dominio alternativi, l'elenco include un nome di dominio di origine per la distribuzione.

TimeBucket

L'ora o il giorno a cui si riferiscono i dati, in formato UTC.

Richieste

Il numero totale di richieste per tutti i codici di stato HTTP (ad esempio, `200`, `404` e così via) e tutti i metodi (ad esempio, `GET`, `HEAD`, `POST` e così via) durante il periodo di tempo.

BytesDownloaded

Il numero di byte che i visualizzatori hanno scaricato per la distribuzione specificata durante il periodo di tempo.

BytesUploaded

Il numero di byte che i visualizzatori hanno caricato per la distribuzione specificata durante l'intervallo temporale.

TotalErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `4xx` o `5xx` per la distribuzione specificata durante l'intervallo temporale.

4xxErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `4xx` per la distribuzione specificata durante l'intervallo temporale.

5xxErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `5xx` per la distribuzione specificata durante l'intervallo temporale.

Se sono stati attivati parametri aggiuntivi per la distribuzione, il report include anche i seguenti valori aggiuntivi:

401ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `401` per la distribuzione specificata durante l'intervallo temporale.

403ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `403` per la distribuzione specificata durante l'intervallo temporale.

404ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `404` per la distribuzione specificata durante l'intervallo temporale.

502ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `502` per la distribuzione specificata durante l'intervallo temporale.

503ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `503` per la distribuzione specificata durante l'intervallo temporale.

504ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `504` per la distribuzione specificata durante l'intervallo temporale.

OriginLatency

Il tempo totale trascorso, in millisecondi, da quando CloudFront ha ricevuto una richiesta a quando ha iniziato a fornire una risposta alla rete (non al visualizzatore), per le richieste che sono state servite dall'origine, non dalla cache CloudFront. Questo è anche noto come latenza di primo byte, o time-to-first-byte.

CacheHitRate

La percentuale di richieste che possono essere memorizzate nella cache per le quali CloudFront ha fornito il contenuto dalla propria cache. Le richieste HTTP `POST` e `PUT` e gli errori non sono considerati memorizzabili nella cache.

Tipi di metriche per CloudFront

Puoi utilizzare l'API CloudWatch o AWS Command Line Interface (AWS CLI) per ottenere le metriche CloudFront nei programmi o nelle applicazioni create. È possibile utilizzare i dati grezzi per creare dashboard personalizzati, strumenti di avviso e così via.

Per ulteriori informazioni, consulta get-metric-data nel Riferimento ai comandi AWS CLI o l'operazione API GetMetricData nella Documentazione di riferimento delle API di Amazon CloudWatch.

Argomenti

- Valori per tutti i parametri CloudFront
- Valori per i parametri di distribuzione CloudFront
- Valori per i parametri delle funzioni CloudFront

> **Note**
>
> Per ottenere parametri di CloudFront dall'API CloudWatch, è necessario utilizzare la regione degli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`). È inoltre necessario conoscere determinati valori e tipi per ogni parametro.

Valori per tutti i parametri CloudFront

I seguenti valori si applicano a tutti i parametri CloudFront:

`Namespace`

Il valore per `Namespace` è sempre `AWS/CloudFront`.

Dimensioni

Ogni metrica CloudFront dispone delle due dimensioni seguenti:

`DistributionId`

L'ID della distribuzione CloudFront per la quale si desidera ottenere i parametri.

`FunctionName`

Il nome della funzione (in CloudFront Functions) per la quale si desidera ottenere i parametri.

Questa dimensione si applica solo alle funzioni.

`Region`

Il valore di `Region` è sempre `Global`, perché CloudFront è un servizio globale.

Valori per i parametri di distribuzione CloudFront

Utilizza le informazioni contenute nell'elenco seguente per ottenere dettagli sui parametri di distribuzione specifici di CloudFront dall'API CloudWatch. Alcune di questi parametri sono disponibili solo quando sono stati abilitate parametri aggiuntivi per la distribuzione.

> **Note**
>
> Per ogni metrica è applicabile una sola statistica, `Average` o `Sum`. L'elenco seguente specifica quale statistica è applicabile a tale metrica.

Frequenza di errore 4xx

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `4xx`.

- Nome parametro: `4xxErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 401

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `401`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `401ErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 403

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `403`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `403ErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 404

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `404`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `404ErrorRate`
- Statistiche valide:: `Average`

- Unità: `Percent`

Frequenza di errore 5xx

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `5xx`.

- Nome parametro: `5xxErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 502

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `502`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `502ErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 503

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `503`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `503ErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Tasso di errore 504

Percentuale di tutte le richieste del visualizzatore per le quali è il codice di stato HTTP della risposta è `504`. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `504ErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Byte scaricati

Il numero totale di byte scaricati dai visualizzatori per le richieste `GET` e `HEAD`.

- Nome parametro: `BytesDownloaded`

- Statistiche valide:: `Sum`
- Unità: `None`

Byte caricati

Il numero totale di byte caricati dai visualizzatori in CloudFront, tramite le richieste `OPTIONS`, `POST` e `PUT`.

- Nome parametro: `BytesUploaded`
- Statistiche valide:: `Sum`
- Unità: `None`

Percentuale di riscontri nella cache

La percentuale di richieste che possono essere memorizzate nella cache per le quali CloudFront ha fornito il contenuto dalla propria cache. Le richieste HTTP `POST` e `PUT` e gli errori non sono considerati memorizzabili nella cache. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `CacheHitRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Latenza di origine

Il tempo totale trascorso, in millisecondi, da quando CloudFront riceve una richiesta a quando inizia a fornire una risposta alla rete (non al visualizzatore), per le richieste che vengono servite dall'origine, non dalla cache CloudFront. Questo è anche noto come latenza di primo byte, o time-to-first-byte. Per ottenere questo parametro, è necessario attivare ulteriori parametri.

- Nome parametro: `OriginLatency`
- Statistiche valide:: `Percentile`
- Unità: `Milliseconds`

> **Note**
>
> Per ottenere una statistica `Percentile` dall'API CloudWatch, utilizzare il parametro `ExtendedStatistics`, non `Statistics`. Per ulteriori informazioni, consulta GetMetricStatistics nella Documentazione di riferimento delle API di Amazon CloudWatch o la documentazione di riferimento per gli SDK di AWS.

Richieste

Il numero totale di richieste di visualizzatore ricevute da CloudFront, per tutti i metodi HTTP e per le richieste HTTP e HTTPS.

- Nome parametro: `Requests`
- Statistiche valide:: `Sum`
- Unità: `None`

Frequenza di errore totale

Percentuale di tutte le richieste del visualizzatore per le quali il codice di stato HTTP della risposta è `4xx` o `5xx`.

- Nome parametro: `TotalErrorRate`
- Statistiche valide:: `Average`
- Unità: `Percent`

Valori per i parametri delle funzioni CloudFront

Utilizza le informazioni contenute nell'elenco seguente per ottenere dettagli sui parametri CloudFront specifici dall'API CloudWatch.

> **Note**
>
> Per ogni metrica è applicabile una sola statistica, `Average` o `Sum`. L'elenco seguente specifica quale statistica è applicabile a tale metrica.

Invocazioni

Il numero di volte in cui la funzione è stata avviata (richiamata) in un determinato periodo di tempo.

- Nome parametro: `FunctionInvocations`
- Statistiche valide:: `Sum`
- Unità: `None`

Errori di convalida

Il numero di errori di convalida prodotti dalla funzione in un determinato periodo di tempo. Gli errori di convalida si verificano quando la funzione viene eseguita correttamente ma restituisce dati non validi (un oggetto evento non valido).

- Nome parametro: `FunctionValidationErrors`
- Statistiche valide:: `Sum`
- Unità: `None`

Errori di esecuzione

Il numero di errori di esecuzione che si sono verificati in un determinato periodo di tempo. Gli errori di esecuzione si verificano quando la funzione non viene completata correttamente.

- Nome parametro: `FunctionExecutionErrors`
- Statistiche valide:: `Sum`
- Unità: `None`

Utilizzo di calcolo

La quantità di tempo (0-100) impiegata dalla funzione per l'esecuzione come percentuale del tempo massimo consentito. Ad esempio, un valore pari a 35 significa che la funzione è stata completata nel 35% del tempo massimo consentito.

- Nome parametro: `FunctionComputeUtilization`
- Statistiche valide:: `Average`
- Unità: `Percent`

Throttle

Il numero di volte in cui la funzione è stata limitata in un determinato periodo di tempo.

- Nome parametro: `FunctionThrottles`
- Statistiche valide:: `Sum`
- Unità: `None`

CloudFront e registrazione delle funzioni edge

Amazon CloudFront offre diversi tipi di registrazione. Puoi registrare le richieste dei visualizzatori che arrivano alle tue CloudFront distribuzioni oppure puoi registrare l'attività del CloudFront servizio

(attività API) nel tuo AWS account. Puoi anche ottenere i log dalle CloudFront funzioni Functions e Lambda @Edge.

Richieste di registrazione

CloudFront fornisce i seguenti modi per registrare le richieste che arrivano alle tue distribuzioni.

Registri di accesso (registri standard)

CloudFronti registri di accesso forniscono registrazioni dettagliate su ogni richiesta effettuata a una distribuzione. Puoi utilizzare i log per scenari, quali controlli di sicurezza e accesso.

CloudFronti registri di accesso vengono consegnati alla destinazione di consegna specificata.

Usa i log di accesso quando hai bisogno di:

- Analisi e report storici
- Audit di sicurezza e requisiti di conformità
- Conservazione dei log a lungo termine a costi contenuti

Per ulteriori informazioni, consulta Registri di accesso (registri standard).

Registri di accesso in tempo reale

CloudFronti log di accesso in tempo reale vengono consegnati entro pochi secondi dalla ricezione delle richieste e forniscono informazioni sulle richieste effettuate a una distribuzione in tempo reale. È possibile scegliere la frequenza di campionamento per i log di accesso in tempo reale, ovvero la percentuale di richieste per le quali si desidera ricevere i record dei log di accesso in tempo reale. Puoi anche scegliere i campi specifici che desideri siano riportati nei record di log. I log di accesso in tempo reale sono ideali per il monitoraggio in tempo reale delle prestazioni di distribuzione dei contenuti.

CloudFront i log di accesso in tempo reale vengono forniti al flusso di dati di tua scelta in Amazon Kinesis Data Streams. CloudFront costi per i log di accesso in tempo reale, oltre ai costi sostenuti per l'utilizzo di Kinesis Data Streams.

Utilizza i log di accesso in tempo reale quando hai bisogno di:

- Monitoraggio e avvisi in tempo reale
- Dashboard in tempo reale e approfondimenti operativi

Per ulteriori informazioni, consulta Utilizza i log di accesso in tempo reale.

Log delle connessioni

I log di connessione forniscono informazioni dettagliate sulla connessione tra il server e il client per le distribuzioni abilitate per MTL. I log di connessione forniscono visibilità sulle informazioni sul certificato del client, sui motivi degli errori di autenticazione MTLS e sull'eventuale autorizzazione o rifiuto della connessione.

Analogamente ai registri di accesso (registri standard), i registri di connessione vengono consegnati alla destinazione di consegna specificata.

> **Note**
>
> Per abilitare i log di connessione, devi prima abilitare gli MTL per la tua distribuzione.

Utilizzate i log di connessione quando avete bisogno di:

- Motivi dell'esito positivo o negativo delle connessioni durante l'handshake TLS
- Visibilità nelle informazioni sul certificato del client

Per ulteriori informazioni, consulta Osservabilità utilizzando i log di connessione.

Registrazione delle funzioni edge

Puoi usare Amazon CloudWatch Logs per ottenere i log delle tue funzioni edge, sia Lambda @Edge che Functions. CloudFront Puoi accedere ai log utilizzando la CloudWatch console o l'API Logs. CloudWatch Per ulteriori informazioni, consulta the section called “Registri delle funzioni Edge”.

Attività del servizio di registrazione

Puoi utilizzarlo AWS CloudTrail per registrare l'attività del CloudFront servizio (attività API) nel tuo AWS account. CloudTrail fornisce un registro delle azioni API eseguite da un utente, ruolo o AWS servizio in CloudFront. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta API a cui è stata effettuata CloudFront, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni, consulta Registrazione di log delle chiamate API Amazon CloudFront utilizzando AWS CloudTrail.

Per ulteriori informazioni sulla registrazione di log, consulta i seguenti argomenti:

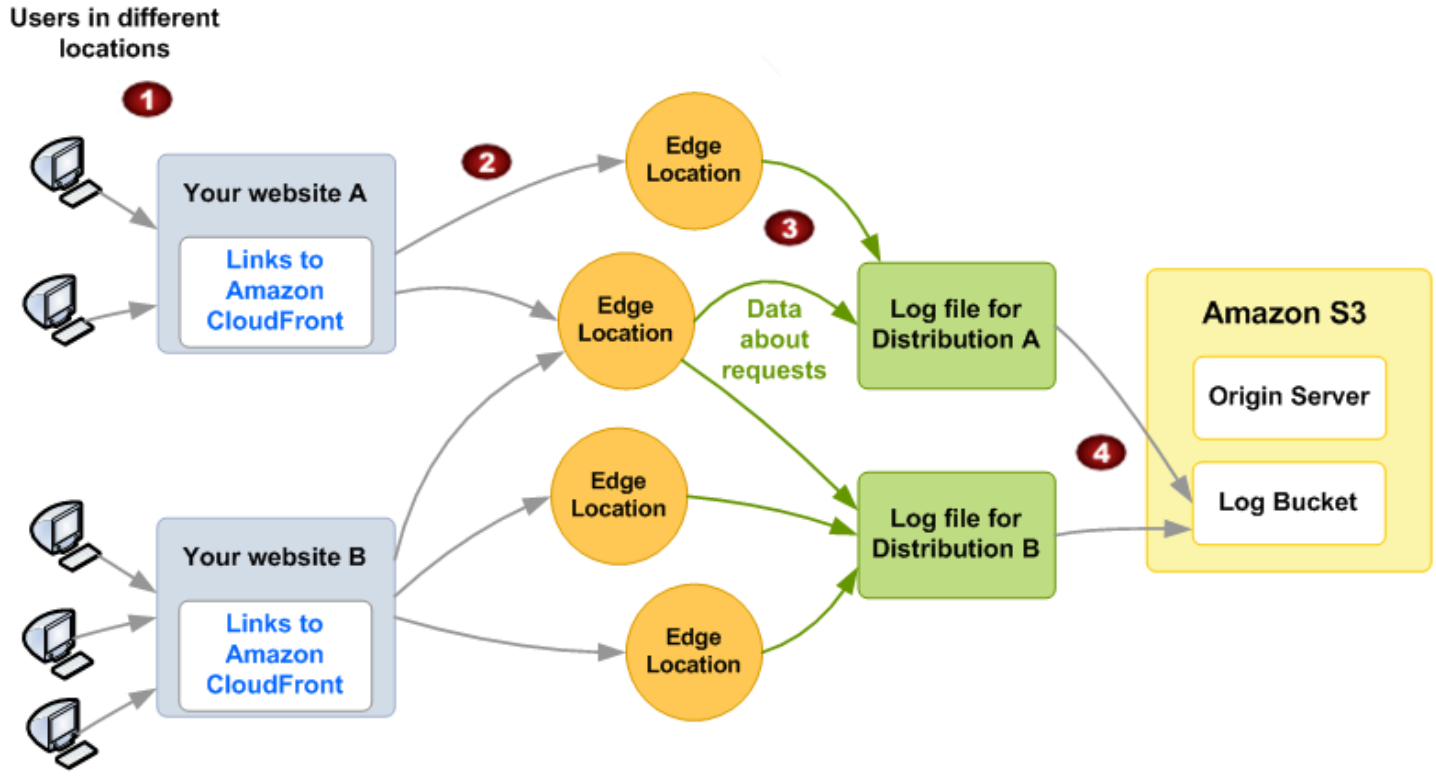
Argomenti

Registri di accesso (registri standard)

È possibile CloudFront configurare la creazione di file di registro che contengono informazioni dettagliate su ogni richiesta dell'utente (visualizzatore) che CloudFront riceve. Questi sono chiamati registri di accesso, noti anche come registri standard.

Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, il tempo di elaborazione, i percorsi delle richieste e le risposte del server. Puoi usare questi log di accesso per analizzare i tempi di risposta e risolvere i problemi.

Il diagramma seguente mostra come CloudFront registra le informazioni sulle richieste relative agli oggetti. In questo esempio, le distribuzioni sono configurate per inviare i log di accesso a un bucket Amazon S3.



1. In questo esempio, avete due siti Web, A e B, e due distribuzioni corrispondenti CloudFront. Gli utenti richiedono i vostri oggetti utilizzando URLs quelli associati alle vostre distribuzioni.
2. CloudFront indirizza ogni richiesta verso la edge location appropriata.
3. CloudFront scrive i dati su ogni richiesta in un file di registro specifico per quella distribuzione. In questo esempio, le informazioni sulle richieste relative alla distribuzione A sono registrate in un file di log per la distribuzione A. Le informazioni sulle richieste relative alla distribuzione B sono registrate in un file di log per la distribuzione B.
4. CloudFront salva periodicamente il file di registro per una distribuzione nel bucket Amazon S3 che hai specificato quando hai abilitato la registrazione. CloudFront inizia quindi a salvare le informazioni sulle richieste successive in un nuovo file di registro per la distribuzione.

   Se i visualizzatori non accedono al contenuto durante una determinata ora, non riceverai alcun file di log per tale ora.

> **Note**
>
> Ti consigliamo di utilizzare i log per comprendere la natura delle richieste relative ai tuoi contenuti, non come contabilità completa di tutte le richieste. CloudFront fornisce i log di accesso con la massima diligenza possibile. È possibile che la voce di log per una specifica richiesta venga distribuita molto tempo dopo l'elaborazione effettiva della richiesta e, in rari casi, che non venga distribuita affatto. Quando una voce di registro viene omessa dai registri di accesso, il numero di voci nei log di accesso non corrisponde all'utilizzo visualizzato nei report di utilizzo e fatturazione di AWS .

CloudFront supporta due versioni di registrazione standard. La registrazione di log standard (legacy) supporta l'invio dei log di accesso solo ad Amazon S3. La registrazione di log standard (v2) supporta destinazioni di consegna aggiuntive. Puoi configurare entrambe le opzioni di registrazione di log o solo una delle due per la distribuzione. Per ulteriori informazioni, consulta i seguenti argomenti:

Argomenti

- Configurazione della registrazione di log standard (v2)
- Configurazione della registrazione di log standard (legacy)
- Riferimento alla registrazione di log standard

> **Tip**
>
> CloudFront offre anche registri di accesso in tempo reale, che forniscono informazioni sulle richieste effettuate a una distribuzione in tempo reale (i log vengono consegnati entro pochi secondi dalla ricezione delle richieste). È possibile utilizzare i log di accesso in tempo reale per monitorare, analizzare e intraprendere azioni in base alle prestazioni di distribuzione dei contenuti. Per ulteriori informazioni, consulta Utilizza i log di accesso in tempo reale.

Configurazione della registrazione di log standard (v2)

Puoi abilitare i log di accesso (log standard) quando crei o aggiorni una distribuzione. La registrazione di log standard (v2) include le seguenti funzionalità:

- Invia i log di accesso ad Amazon CloudWatch Logs, Amazon Data Firehose e Amazon Simple Storage Service (Amazon S3).
- Selezione dei campi di log desiderati. Puoi anche selezionare un sottoinsieme di campi di log di accesso in tempo reale.
- Selezione dei formati file di log di output aggiuntivi.

Se utilizzi Amazon S3, hai a disposizione le seguenti funzionalità opzionali:

- Invia i log a opt-in. Regioni AWS
- Organizzazione dei log con il partizionamento.
- Abilitazione di nomi di file compatibili con Hive.

Per ulteriori informazioni, consulta Invio di log ad Amazon S3.

Per iniziare a utilizzare la registrazione di log standard, completa le fasi seguenti:

1. Imposta le autorizzazioni richieste per la persona specificata Servizio AWS che riceverà i tuoi registri.
2. Configura la registrazione standard dalla CloudFront console o dall'API. CloudWatch
3. Visualizza i log di accesso.

Note

- Se abiliti la registrazione di log standard (v2), ciò non influisce né modifica la registrazione di log standard (legacy). Puoi continuare a utilizzare la registrazione di log standard (legacy) per la distribuzione, oltre a utilizzare la registrazione di log standard (v2). Per ulteriori informazioni, consulta Configurazione della registrazione di log standard (legacy).
- Se hai già abilitato la registrazione di log standard (legacy) e desideri abilitare la registrazione di log standard (v2) su Amazon S3, ti consigliamo di specificare un bucket Amazon S3 diverso o di utilizzare un percorso separato nello stesso bucket (ad esempio, utilizzare un prefisso di log o il partizionamento). Questo consente di tenere traccia di quali file di log sono associati a quale distribuzione ed evita la sovrascrittura reciproca dei file di log.

Permissions

CloudFront utilizza i CloudWatch log forniti per fornire i log di accesso. A tale scopo, sono necessarie le autorizzazioni necessarie per consentire Servizio AWS la consegna dei log.

Per visualizzare le autorizzazioni richieste per ogni destinazione di registrazione, scegli uno dei seguenti argomenti nella Amazon CloudWatch Logs User Guide.

- CloudWatch Log
- Firehose
- Amazon S3

Dopo aver impostato le autorizzazioni per la destinazione della registrazione di log, puoi abilitare la registrazione di log standard per la distribuzione.

Note

CloudFront supporta l'invio di log di accesso a diversi account Account AWS (più account). Per abilitare la consegna tra account, entrambi gli account (il tuo e quello di ricezione) devono disporre delle autorizzazioni necessarie. Per ulteriori informazioni, consulta la Abilitazione della registrazione di log standard per la consegna tra account sezione o l'esempio di consegna tra account nella Amazon CloudWatch Logs User Guide.

Abilitazione della registrazione di log standard

Per abilitare la registrazione standard, puoi utilizzare la CloudFront console o l'API. CloudWatch

Indice

Abilita la registrazione standard (console) CloudFront

Per abilitare la registrazione standard per una CloudFront distribuzione (console)

1. Usa la CloudFront console per aggiornare una distribuzione esistente.
2. Scegli la scheda Logging (Utilizzo log).
3. Scegli Aggiungi, quindi seleziona il servizio di ricezione dei log:
   - CloudWatch Registri
   - Firehose
   - Simple Storage Service (Amazon S3)
4. Per la destinazione, seleziona la risorsa per il servizio in uso. Se non hai ancora creato la risorsa, puoi scegliere Crea o consultare la seguente documentazione.
   - Per CloudWatch Log, inserisci il nome del gruppo di log.
   - Per Firehose, accedi al Flusso di consegna di Firehose.
   - Per Amazon S3, inserisci il Nome bucket.

   > **Tip**
   >
   > Per specificare un prefisso, inserisci il prefisso dopo il nome del bucket, ad esempio `amzn-s3-demo-bucket.s3.amazonaws.com/MyLogPrefix`. Se non specifichi un prefisso, CloudFront ne aggiungerà automaticamente uno. Per ulteriori informazioni, consulta Invio di log ad Amazon S3.
5. Per Impostazioni aggiuntive, facoltativo, puoi specificare le seguenti opzioni:

a. Per Selezione del campo, seleziona i nomi dei campi di log che desideri consegnare alla destinazione. È possibile selezionare i campi del registro degli accessi e un sottoinsieme di campi del registro degli accessi in tempo reale.

b. (Solo Amazon S3) Per Partizionamento, specifica il percorso per partizionare i dati del file di log.

c. (Solo Amazon S3) Per Formato file compatibile con Hive, puoi selezionare la casella di controllo per utilizzare percorsi S3 compatibili con Hive. Questo consente di semplificare il caricamento di nuovi dati negli strumenti compatibili con Hive.

d. Per Formato di output, specifica il formato preferito.

> **Note**
>
> Se scegli Parquet, questa opzione comporta dei CloudWatch costi per la conversione dei log di accesso in Apache Parquet. Per ulteriori informazioni, consulta la sezione Vided Logs per i prezzi. CloudWatch

e. Per Delimitatore di campo, specifica come separare i campi di log.

6. Completa le fasi per aggiornare o creare la distribuzione.
7. Per aggiungere un'altra destinazione, ripeti le fasi da 3 a 6.
8. Nella pagina Log, verifica che lo stato dei log standard sia Abilitato accanto alla distribuzione.
9. (Facoltativo) Per abilitare la registrazione di cookie, scegli Gestione, Impostazioni e attiva la Registrazione di cookie, quindi scegli Salva modifiche.

> **Tip**
>
> Registrazione di cookie è un'impostazione globale che si applica a tutte registrazioni di log standard per la distribuzione. Non puoi sovrascrivere questa impostazione per destinazioni di consegna separate.

Per ulteriori informazioni sui campi di log e di consegna della registrazione di log standard, consulta Riferimento alla registrazione di log standard.

Abilita la registrazione standard (API) CloudWatch

Puoi anche utilizzare l' CloudWatch API per abilitare la registrazione standard per le tue distribuzioni.

> **Note**
>
> - Quando chiami l' CloudWatch API per abilitare la registrazione standard, devi specificare la regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), anche se desideri abilitare la consegna tra regioni verso un'altra destinazione. Ad esempio, se desideri inviare i log di accesso a un bucket S3 nella regione Europa (Irlanda) (`eu-west-1`), utilizza l' CloudWatch API nella regione. `us-east-1`
> - È disponibile un'opzione aggiuntiva per includere i cookie nella registrazione di log standard. Nell' CloudFront API, questo è il parametro. `IncludeCookies` Se configuri la registrazione degli accessi utilizzando l' CloudWatch API e specifichi che desideri includere i cookie, devi utilizzare la CloudFront console o l' CloudFront API per aggiornare la distribuzione in modo da includere i cookie. In caso contrario, non è CloudFront possibile inviare i cookie alla destinazione del registro. Per ulteriori informazioni, consulta Registrazione dei cookie.

Per abilitare la registrazione standard per una distribuzione (CloudWatch API)

1. Dopo aver creato una distribuzione, puoi ottenere il nome della risorsa Amazon (ARN).

   Puoi trovare l'ARN dalla pagina Distribuzione della CloudFront console oppure puoi utilizzare l'operazione GetDistributionAPI. Un ARN di distribuzione segue il formato: `arn:aws:cloudfront::123456789012:distribution/d111111abcdef8`

2. Successivamente, utilizza l'operazione CloudWatch PutDeliverySourceAPI per creare una fonte di consegna per la distribuzione.

   a. Inserisci un nome per l'origine di consegna.

   b. Passa il `resourceArn` della distribuzione.

   c. Per `logType`, specifica `ACCESS_LOGS` come tipo di log che vengono raccolti.

   d. Example AWS CLI put-delivery-source Comando di esempio

      Di seguito è riportato un esempio di configurazione dell'origine di consegna per una distribuzione.

```
aws logs put-delivery-source --name S3-delivery --resource-arn
 arn:aws:cloudfront::123456789012:distribution/d111111abcdef8 --log-type
 ACCESS_LOGS
```

Output

```
{
 "deliverySource": {
 "name": "S3-delivery",
 "arn": "arn:aws:logs:us-east-1:123456789012:delivery-source:S3-delivery",
 "resourceArns": [
 "arn:aws:cloudfront::123456789012:distribution/d111111abcdef8"
 ],
 "service": "cloudfront",
 "logType": "ACCESS_LOGS"
 }
}
```

3. Utilizza l'operazione PutDeliveryDestinationAPI per configurare dove archiviare i log.

   a. Per `destinationResourceArn`, specifica l'ARN della destinazione. Può trattarsi di un gruppo di log CloudWatch Logs, di un flusso di distribuzione Firehose o di un bucket Amazon S3.

   b. Per `outputFormat`, specifica il formato di output per i log.

   c. Example Comando di esempio AWS CLI put-delivery-destination

   Di seguito è riportato un esempio di configurazione di una destinazione di consegna a un bucket Amazon S3.

```
aws logs put-delivery-destination --name S3-destination --delivery-destination-
configuration destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket
```

Output

```
{
    "name": "S3-destination",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-
destination",
    "deliveryDestinationType": "S3",
```

```
    "deliveryDestinationConfiguration": {
        "destinationResourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
}
```

> **Note**
>
> Se stai distribuendo log su più account, devi utilizzare l'operazione PutDeliveryDestinationPolicyAPI per assegnare una policy AWS Identity and Access Management (IAM) all'account di destinazione. La policy IAM consente la consegna da un account a un altro.

4. Utilizza l'operazione CreateDeliveryAPI per collegare l'origine di consegna alla destinazione creata nei passaggi precedenti. Questa operazione API associa l'origine di consegna alla destinazione finale.

   a. Per `deliverySourceName`, specifica il nome dell'origine.

   b. Per `deliveryDestinationArn`, specifica l'ARN della destinazione di consegna.

   c. Per `fieldDelimiter`, specifica la stringa per separare ogni campo di log.

   d. Per `recordFields`, specifica i campi di log che desideri.

   e. Se utilizzi S3, specifica se usare `enableHiveCompatiblePath` e `suffixPath`.

   Example Esempio di AWS CLI comando create-delivery

   Di seguito è riportato un esempio di creazione di una consegna.

```
aws logs create-delivery --delivery-source-name cf-delivery --delivery-destination-
arn arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-destination
```

   Output

```
{
    "id": "abcNegnBoTR123",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery:abcNegnBoTR123",
    "deliverySourceName": "cf-delivery",
    "deliveryDestinationArn": "arn:aws:logs:us-east-1:123456789012:delivery-
destination:S3-destination",
```

```
    "deliveryDestinationType": "S3",
    "recordFields": [
        "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",
        "c-country",
        "cache-behavior-path-pattern"
    ],
     "fieldDelimiter": ""
}
```

5. Dalla CloudFront console, nella pagina Registri, verifica che lo stato standard dei log sia Abilitato accanto alla distribuzione.

Per ulteriori informazioni sui campi di log e di consegna della registrazione di log standard, consulta Riferimento alla registrazione di log standard.

> **Note**
>
> Per abilitare la registrazione standard (v2) per l' CloudFront utilizzo AWS CloudFormation, puoi utilizzare le seguenti proprietà Logs: CloudWatch
>
> - Delivery
> - DeliveryDestination
> - DeliverySource
>
> `ResourceArn`è la CloudFront distribuzione e `LogType` deve essere il tipo di `ACCESS_LOGS` registro supportato.

Abilitazione della registrazione di log standard per la consegna tra account

Se abiliti la registrazione standard per il tuo account Account AWS e desideri inviare i log di accesso a un altro account, assicurati di configurare correttamente l'account di origine e l'account di destinazione. L'account di origine con la CloudFront distribuzione invia i propri log di accesso all'account di destinazione.

In questa procedura di esempio, l'account di origine invia i propri log di accesso a un bucket Amazon S3 nell'account di destinazione (*111111111111*). *222222222222* Per inviare i log di accesso a un bucket Amazon S3 nell'account di destinazione, utilizza la AWS CLI.

Configurazione dell'account di destinazione

Per l'account di destinazione, completa la procedura seguente.

Come configurare l'account di destinazione

1. Per creare la destinazione di consegna dei log, puoi inserire il comando AWS CLI seguente. Questo esempio utilizza la stringa *MyLogPrefix* per creare un prefisso per i log di accesso.

```
aws logs put-delivery-destination --name cloudfront-delivery-destination --
delivery-destination-configuration "destinationResourceArn=arn:aws:s3:::amzn-s3-
demo-bucket-cloudfront-logs/MyLogPrefix"
```

Output

```
{
    "deliveryDestination": {
        "name": "cloudfront-delivery-destination",
        "arn": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination",
        "deliveryDestinationType": "S3",
        "deliveryDestinationConfiguration": {"destinationResourceArn":
 "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/MyLogPrefix"}
    }
}
```

> **Note**
>
> Se specifichi un bucket S3 senza prefisso, lo CloudFront aggiungerà automaticamente `AWSLogs/<account-ID>/CloudFront` come prefisso che appare nella destinazione di consegna S3. `suffixPath` Per ulteriori informazioni, consulta S3. DeliveryConfiguration

2. Aggiungi la policy di risorse per la destinazione di consegna di log per consentire all'account di origine di creare una consegna di log.

   Nella seguente politica, sostituisci *111111111111* con l'ID dell'account di origine e specifica l'ARN della destinazione di consegna dall'output del passaggio 1.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDelivery",
            "Effect": "Allow",
            "Principal": {"AWS": "111111111111"},
```

```
            "Action": ["logs:CreateDelivery"],
            "Resource": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination"
        }
    ]
}
```

3. Salva il file, ad esempio `deliverypolicy.json`.
4. Per allegare la politica precedente alla destinazione di consegna, inserisci il seguente AWS CLI comando.

```
aws logs put-delivery-destination-policy --delivery-destination-name cloudfront-
delivery-destination --delivery-destination-policy file://deliverypolicy.json
```

5. Aggiungi la seguente istruzione alla policy di bucket Amazon S3 di destinazione, sostituendo l'ARN della risorsa e l'ID dell'account di origine. Questa policy consente al principale del servizio `delivery.logs.amazonaws.com` di eseguire l'azione `s3:PutObject`.

```
{
    "Sid": "AWSLogsDeliveryWrite",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceAccount": "111111111111"
        },
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-
source:*"}
    }
}
```

6. Se lo utilizzi AWS KMS per il tuo bucket, aggiungi la seguente dichiarazione alla politica chiave KMS per concedere le autorizzazioni al responsabile del `delivery.logs.amazonaws.com` servizio.

```
{
    "Sid": "Allow Logs Delivery to use the key",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
```

```
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {"aws:SourceAccount": "111111111111"},
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-
source:*"}
    }
}
```

Configurazione dell'account di origine

Dopo aver configurato l'account di destinazione, segui questa procedura per creare l'origine di consegna e abilitare la registrazione di log per la distribuzione nell'account di origine.

Come configurare l'account di origine

1. Crea una fonte di consegna per la registrazione CloudFront standard in modo da poter inviare i file di registro a Logs. CloudWatch

   È possibile immettere il seguente AWS CLI comando, sostituendo il nome e l'ARN della distribuzione.

   ```
   aws logs put-delivery-source --name s3-cf-delivery --resource-arn
    arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC --log-type
    ACCESS_LOGS
   ```

   Output

   ```
   {
       "deliverySource": {
           "name": "s3-cf-delivery",
           "arn": "arn:aws:logs:us-east-1:111111111111:delivery-source:s3-cf-
   delivery",
           "resourceArns":
    ["arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC"],
   ```

```
        "service": "cloudfront",
        "logType": "ACCESS_LOGS"
    }
}
```

2. Crea una consegna per mappare l'origine di consegna dei log dell'account di origine e la destinazione di consegna dei log dell'account di destinazione.

   Nel AWS CLI comando seguente, specificare l'ARN della destinazione di consegna dall'output del Passaggio 1: Configurazione dell'account di destinazione.

   ```
   aws logs create-delivery --delivery-source-name s3-cf-delivery --
   delivery-destination-arn arn:aws:logs:us-east-1:222222222222:delivery-
   destination:cloudfront-delivery-destination
   ```

   Output

   ```
   {
       "delivery": {
           "id": "OPmOpLahVzhx1234",
           "arn": "arn:aws:logs:us-east-1:111111111111:delivery:OPmOpLahVzhx1234",
           "deliverySourceName": "s3-cf-delivery",
           "deliveryDestinationArn": "arn:aws:logs:us-east-1:222222222222:delivery-
   destination:cloudfront-delivery-destination",
           "deliveryDestinationType": "S3",
           "recordFields": [
               "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",
            "c-country",
            "cache-behavior-path-pattern"
        ],
        "fieldDelimiter": "\t"
    }
}
```

3. Verifica che la consegna tra account sia andata a buon fine.

    a. Dall'*source*account, accedi alla CloudFront console e scegli la tua distribuzione. Nella scheda Registrazione di log, in Tipo, viene visualizzata una voce creata per la consegna di log tra account S3.

    b. Dall'*destination*account, accedi alla console Amazon S3 e scegli il tuo bucket Amazon S3. Viene visualizzato il prefisso *MyLogPrefix* nel nome del bucket e gli eventuali log di accesso forniti a tale cartella.

Formato del file di output

A seconda della destinazione di consegna scelta, puoi specificare uno dei seguenti formati per i file di log:

- JSON
- Plain
- w3c

- Raw
- Parquet (solo Amazon S3)

> **Note**
>
> Puoi impostare il formato di output solo quando crei per la prima volta la destinazione di consegna. Questo non può essere aggiornato in seguito. Per modificare il formato di output, elimina la consegna e creane un'altra.

Per ulteriori informazioni, PutDeliveryDestinationconsulta Amazon CloudWatch Logs API Reference.

Modifica delle impostazioni di registrazione di log standard

Puoi abilitare o disabilitare la registrazione e aggiornare altre impostazioni di registro utilizzando la CloudFront console o l' CloudWatch API. Le modifiche apportate alle impostazioni di registrazione diventano effettive entro 12 ore.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Per aggiornare una distribuzione utilizzando la CloudFront console, consultaAggiornamento di una distribuzione.
- Per aggiornare una distribuzione utilizzando l' CloudFront API, UpdateDistributionconsulta Amazon CloudFront API Reference.
- Per ulteriori informazioni sulle operazioni dell'API CloudWatch Logs, consulta l'Amazon CloudWatch Logs API Reference.

Campi dei log di accesso

Puoi selezionare gli stessi campi di log supportati dalla registrazione di log standard (legacy). Per ulteriori informazioni, consulta i campi dei file di log.

Inoltre, puoi selezionare i seguenti campi di log di accesso in tempo reale.

1. **`timestamp(ms)`**: timestamp in millisecondi.
2. **`origin-fbl`**— Il numero di secondi di latenza del primo byte tra l'origine CloudFront e l'origine.
3. **`origin-lbl`**— Il numero di secondi di latenza dell'ultimo byte tra e l'origine. CloudFront
4. **`asn`**: l'Autonomous System Number (ASN) del visualizzatore.

5. **`c-country`**: un codice paese che rappresenta la posizione geografica del visualizzatore, determinata dal relativo indirizzo IP. Per un elenco dei codici paese, vedere ISO 3166-1 alpha-2.
6. **`cache-behavior-path-pattern`**: il modello di percorso che identifica il comportamento della cache corrispondente alla richiesta visualizzatore.

Inviare i log ai Logs CloudWatch

Per inviare log a CloudWatch Logs, create o utilizzate un gruppo di log Logs esistente CloudWatch . Per ulteriori informazioni sulla configurazione di un gruppo di log CloudWatch Logs, vedere Working with Log Groups and Log Streams.

Dopo aver creato un gruppo di log, devi disporre delle autorizzazioni obbligatorie per consentire la registrazione di log standard. Per ulteriori informazioni sulle autorizzazioni richieste, consulta Logs sent to Logs nella Amazon CloudWatch CloudWatch Logs User Guide.

> **Note**
>
> - Quando specifichi il nome del gruppo di log CloudWatch Logs, usa solo lo schema regex. `[\w-]` Per ulteriori informazioni, consulta il funzionamento dell'PutDeliveryDestinationAPI nell'Amazon CloudWatch Logs API Reference.
> - Verifica che la policy di risorse del gruppo di log non superi il limite di dimensione. Consulta la sezione Considerazioni sui limiti di dimensione della politica delle risorse del gruppo CloudWatch Log nell'argomento Logs.

Esempio di log di accesso inviato a Logs CloudWatch

```
{
"date": "2024-11-14",
"time": "21:34:06",
"x-edge-location": "SOF50-P2",
"asn": "16509",
"timestamp(ms)": "1731620046814",
"origin-fbl": "0.251",
"origin-lbl": "0.251",
"x-host-header": "d111111abcdef8.cloudfront.net",
"cs(Cookie)": "examplecookie=value"
}
```

Invio di log a Firehose

Per inviare i log a Firehose, crea o utilizza un flusso di consegna di Firehose esistente. Quindi, specifica il flusso di consegna di Firehose come la distribuzione di consegna dei log. È necessario specificare un flusso di consegna di Firehose nella regione us-east-1 Stati Uniti orientali (Virginia settentrionale).

Per informazioni sulla creazione del flusso di consegna, consulta Creazione di un flusso di consegna di Amazon Data Firehose.

Dopo aver creato un flusso di consegna, devi disporre delle autorizzazioni richieste per consentire la registrazione di log standard. Per ulteriori informazioni, consulta Logs sent to Firehose nella CloudWatch Amazon Logs User Guide.

> **Note**
>
> Durante la specifica del nome del flusso Firehose, utilizza solo il pattern regex `[\w-]`. Per ulteriori informazioni, consulta il funzionamento dell'PutDeliveryDestinationAPI nell'Amazon CloudWatch Logs API Reference.

Esempio di log di accesso inviato a Firehose

```
{"date":"2024-11-15","time":"19:45:51","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699951183","origin-fbl":"0.254","origin-
lbl":"0.254","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
{"date":"2024-11-15","time":"19:45:52","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699952950","origin-fbl":"0.125","origin-
lbl":"0.125","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
```

Invio di log ad Amazon S3

Per inviare log di accesso ad Amazon S3, crea o usa un bucket S3 esistente. Quando abiliti l'accesso CloudFront, specifica il nome del bucket. Per ulteriori informazioni sulla creazione di un bucket, consulta Creazione di un bucket nella Guida per l'utente di Amazon Simple Storage Service.

Dopo aver creato un bucket, devi disporre delle autorizzazioni richieste per consentire la registrazione di log standard. Per ulteriori informazioni, consulta Logs sent to Amazon S3 nella CloudWatch Amazon Logs User Guide.

- Dopo aver abilitato la registrazione, aggiunge AWS automaticamente le policy relative ai bucket necessarie.
- Puoi anche utilizzare i bucket S3 nelle Regioni AWS di adesione.

> **Note**
>
> Se hai già abilitato la registrazione di log standard (legacy) e desideri abilitare la registrazione di log standard (v2) su Amazon S3, ti consigliamo di specificare un bucket Amazon S3 diverso o di utilizzare un percorso separato nello stesso bucket (ad esempio, utilizzare un prefisso di log o il partizionamento). Questo consente di tenere traccia di quali file di log sono associati a quale distribuzione ed evita la sovrascrittura reciproca dei file di log.

Argomenti

Specifica di un bucket S3

Durante la specifica di un bucket S3 come destinazione di consegna, tieni presente quanto segue.

Il nome del bucket S3 può utilizzare solo il modello regex `[\w-]`. Per ulteriori informazioni, consulta il funzionamento dell'PutDeliveryDestinationAPI nell'Amazon CloudWatch Logs API Reference.

Se hai specificato un prefisso per il bucket S3, i log vengono visualizzati in tale percorso. Se non specifichi un prefisso, lo CloudFront aggiungerà automaticamente. `AWSLogs/{account-id}/CloudFront`

Per ulteriori informazioni, consulta Percorsi di esempio per accedere ai log.

Partizionamento

Puoi usare il partizionamento per organizzare i log di accesso quando li CloudFront invii al tuo bucket S3. Ciò consente di organizzare e individuare i log di accesso in base al percorso desiderato.

Puoi utilizzare le seguenti variabili per creare un percorso cartella.

- `{DistributionId}` o `{distributionid}`
- `{yyyy}`
- `{MM}`
- `{dd}`
- `{HH}`
- `{accountid}`

Puoi utilizzare un numero qualsiasi di variabili e specificare i nomi delle cartelle nel tuo percorso. CloudFrontquindi utilizza questo percorso per creare una struttura di cartelle per te nel bucket S3.

Esempi

- *my_distribution_log_data*/{DistributionId}/*logs*
- /*cloudfront*/{DistributionId}/*my_distribution_log_data*/{yyyy}/{MM}/{dd}/{HH}/*logs*

> **Note**
>
> Puoi utilizzare entrambe le variabili per l'ID di distribuzione nel percorso del suffisso. Tuttavia, se stai inviando i log di accesso a AWS Glue, devi usare la `{distributionid}` variabile perché AWS Glue prevede che i nomi delle partizioni siano in minuscolo. Aggiorna la configurazione di registro esistente per sostituirla con. CloudFront `{DistributionId}` `{distributionid}`

Formato del nome del file compatibile con Hive

Puoi utilizzare questa opzione affinché gli oggetti S3 che contengono i log di accesso consegnati utilizzino una struttura di prefissi che consenta l'integrazione con Apache Hive. Per ulteriori informazioni, consulta l'operazione API CreateDelivery.

Example Esempio

```
/cloudfront/DistributionId={DistributionId}/my_distribution_log_data/year={yyyy}/
month={MM}/day={dd}/hour={HH}/logs
```

Per ulteriori informazioni sul partizionamento e sulle opzioni compatibili con Hive, consulta l'elemento S3 DeliveryConfiguration nell'Amazon Logs API Reference. CloudWatch

Percorsi di esempio per accedere ai log

Durante la specifica di un bucket S3 come destinazione, puoi utilizzare le opzioni seguenti per creare il percorso ai log di accesso:

- Un bucket Amazon S3, con o senza prefisso
- Partizionamento, utilizzando una variabile fornita o inserendo una variabile personalizzata CloudFront
- Abilitazione dell'opzione compatibile con Hive

Nelle tabelle seguenti viene mostrato come vengono visualizzati i log di accesso nel bucket, a seconda delle opzioni scelte.

Bucket Amazon S3 con un prefisso

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
`amzn-s3-demo-bucket/MyLogPrefix`	Nessuno	Nessuno	No	`amzn-s3-demo-bucket/MyLogPrefix/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/`	`myFolderA/`	No	`amzn-s3-demo-bucket/MyLogPrefix/myFolderA/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/{yyyy}`	`myFolderA/{yyyy}`	Sì	`amzn-s3-demo-bucket/MyLogPrefix/myFo`

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
				`lderA/yea r=2025`

Bucket Amazon S3 senza un prefisso

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
`amzn-s3-d emo-bucket`	Nessuno	`AWSLogs/{ account-i d}/CloudF ront/`	No	`amzn-s3-d emo-bucke t/AWSLogs / <your-acc ount-ID> / CloudFront/`
`amzn-s3-d emo-bucket`	`myFolderA/`	`AWSLogs/{ account-i d}/CloudF ront/myFo lderA/`	No	`amzn-s3-d emo-bucke t/AWSLogs / <your-acc ount-ID> / CloudFront/ myFolderA/`
`amzn-s3-d emo-bucket`	`myFolderA/`	`AWSLogs/{ account-i d}/CloudF ront/myFo lderA/`	Sì	`amzn-s3-d emo-bucke t/AWSLogs /aws- account- id=<your-acc ount-ID> /`

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
				`CloudFront/myFolderA/`
`amzn-s3-demo-bucket`	`myFolderA/{yyyy}`	`AWSLogs/{account-id}/CloudFront/myFolderA/{yyyy}`	Sì	`amzn-s3-demo-bucket/AWSLogs/aws-account-id=`*`<your-account-ID>`*` /CloudFront/myFolderA/year=2025`

Account AWS ID come partizione

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
`amzn-s3-demo-bucket`	Nessuno	`AWSLogs/{account-id}/CloudFront/`	Sì	`amzn-s3-demo-bucket/AWSLogs/aws-account-id=`*`<your-account-ID>`*` /CloudFront/`
`amzn-s3-demo-bucket`	`myFolderA/{accountid}`	`AWSLogs/{account-i`	Sì	`amzn-s3-demo-bucke`

Nome del bucket Amazon S3	Partizione specificata nel percorso del suffisso	Percorso del suffisso aggiornato	Compatibilità con Hive abilitata?	I log di accesso vengono inviati a
		`d}/CloudFront/myFolderA/{accountid}`		`t/AWSLogs/aws-account-id=<your-account-ID>/CloudFront/myFolderA/accountid= <your-account-ID>`

> **Note**
>
> - La `{account-id}` variabile è riservata CloudFront a. CloudFrontaggiunge automaticamente questa variabile al percorso del suffisso se specifichi un bucket Amazon S3 senza prefisso. Se i log sono compatibili con Hive, questa variabile viene visualizzata come `aws-account-id`.
> - Puoi usare la `{accountid}` variabile in modo da CloudFront aggiungere l'ID del tuo account al percorso del suffisso. Se i log sono compatibili con Hive, questa variabile viene visualizzata come `accountid`.
> - Per ulteriori informazioni sul percorso del suffisso, consulta S3. DeliveryConfiguration

Esempio di log di accesso inviato ad Amazon S3

```
#Fields: date time x-edge-location asn timestamp(ms) x-host-header cs(Cookie)
2024-11-14    22:30:25    SOF50-P2    16509    1731623425421
d111111abcdef8.cloudfront.net    examplecookie=value2
```

Disabilitazione della registrazione di log standard

Puoi disabilitare la registrazione di log standard per la distribuzione se non è più necessaria.

Come disabilitare la registrazione di log standard

1. Accedere alla console CloudFront .
2. Scegli Distribuzione, quindi scegli l'ID distribuzione.
3. Scegli Registrazione, quindi in Accedi alle destinazioni del registro, seleziona la destinazione.
4. Scegli Gestisci, quindi seleziona Elimina.
5. Ripeti la fase precedente se disponi di più registrazioni di log standard.

> **Note**
>
> Quando elimini la registrazione standard dalla CloudFront console, questa azione elimina solo la consegna e la destinazione di consegna. Non elimina la fonte di consegna dal tuo. Account AWS Per eliminare un'origine di consegna, specifica il nome dell'origine di distribuzione nel comando `aws logs delete-delivery-source --name DeliverySourceName`. Per ulteriori informazioni, DeleteDeliverySourceconsulta Amazon CloudWatch Logs API Reference.

Risoluzione dei problemi

Utilizza le seguenti informazioni per risolvere i problemi più comuni quando lavori con la registrazione CloudFront standard (v2).

L'origine di consegna esiste già

Quando si abilita la registrazione di log standard per una consegna, viene creata un'origine di consegna. Puoi quindi utilizzare tale fonte di consegna per creare consegne al tipo di destinazione che desideri: CloudWatch Logs, Firehose, Amazon S3. Attualmente è possibile avere una sola origine di consegna per ogni distribuzione. Se tenti di creare un'altra origine di consegna per la stessa distribuzione, viene visualizzato il seguente messaggio di errore.

```
This ResourceId has already been used in another Delivery Source in this account
```

Per creare un'altra origine di consegna, elimina prima quella esistente. Per ulteriori informazioni, DeleteDeliverySourceconsulta Amazon CloudWatch Logs API Reference.

Ho cambiato il percorso del suffisso e il bucket Amazon S3 non può ricevere i miei log

Se hai abilitato la registrazione standard (v2) e specifichi un bucket ARN senza prefisso CloudFront , aggiungerà il seguente valore predefinito al percorso del suffisso:. `AWSLogs/{account-id}/CloudFront` Se utilizzi la CloudFront console o l'operazione UpdateDeliveryConfigurationAPI per specificare un percorso di suffisso diverso, devi aggiornare la policy del bucket Amazon S3 per utilizzare lo stesso percorso.

Example Esempio: aggiornamento del percorso del suffisso

1. Il percorso del suffisso predefinito è `AWSLogs/{account-id}/CloudFront` e lo sostituisci con `myFolderA`.
2. Poiché il nuovo percorso del suffisso è diverso dal percorso specificato nella policy di bucket di Amazon S3, i log di accesso non verranno consegnati.
3. Puoi effettuare uno dei seguenti passaggi:
   - Aggiorna l'autorizzazione del bucket Amazon S3 da `amzn-s3-demo-bucket/AWSLogs/<your-account-ID>/CloudFront/*` a`amzn-s3-demo-bucket/myFolderA/*`.
   - Aggiorna la configurazione di registrazione di log per usare nuovamente il suffisso predefinito: `AWSLogs/{account-id}/CloudFront`

Per ulteriori informazioni, consulta Permissions.

Eliminazione di file di log

CloudFront non elimina automaticamente i file di registro dalla tua destinazione. Per informazioni sull'eliminazione di file di log, consulta i seguenti argomenti:

Simple Storage Service (Amazon S3)

- Eliminazione di oggetti nella Guida per l'utente di Amazon Simple Storage Service Console.

CloudWatch Registri

- Utilizzo di gruppi di log e flussi di log nella Amazon CloudWatch Logs User Guide
- DeleteLogGroupnel riferimento all'API Amazon CloudWatch Logs

Firehose

- DeleteDeliveryStreamnel riferimento all'API Amazon Data Firehose

Prezzi

CloudFront non addebita alcun costo per l'abilitazione dei log standard. Tuttavia, potrebbero essere addebitati costi per la consegna, l'acquisizione, l'archiviazione o l'accesso, a seconda della destinazione di consegna dei log selezionata. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon CloudWatch Logs. In Livello a pagamento, scegli la scheda Log, quindi in Log forniti, visualizza le informazioni relative a ciascuna destinazione di consegna.

Per ulteriori informazioni sui prezzi di ciascuno di essi Servizio AWS, consulta i seguenti argomenti:

- Prezzi di Amazon CloudWatch Logs
- Prezzi di Amazon Data Firehose
- Prezzi di Amazon S3

> **Note**
>
> Non sono previsti costi aggiuntivi per la consegna dei log ad Amazon S3, ma sono previsti costi Amazon S3 per l'archiviazione e l'accesso ai file di log. Se abiliti l'opzione Parquet per convertire i log di accesso in Apache Parquet, questa opzione comporta dei costi. CloudWatch Per ulteriori informazioni, consulta la sezione Vided Logs per i prezzi. CloudWatch

Configurazione della registrazione di log standard (legacy)

> **Note**
>
> - Questo argomento riguarda la versione precedente della registrazione di log standard. Per la versione più recente, consulta Configurazione della registrazione di log standard (v2).
> - Se hai già abilitato la registrazione di log standard (legacy) e desideri abilitare la registrazione di log standard (v2) su Amazon S3, ti consigliamo di specificare un bucket Amazon S3 diverso o di utilizzare un percorso separato nello stesso bucket (ad esempio, utilizzare un prefisso di log o il partizionamento). Questo consente di tenere traccia di quali

file di log sono associati a quale distribuzione ed evita la sovrascrittura reciproca dei file di log.

Per iniziare a utilizzare la registrazione di log standard (legacy), completa le fasi seguenti:

1. Scegli un bucket Amazon S3 di destinazione dei log e aggiungi autorizzazioni richieste.
2. Configura la registrazione di log standard (legacy) dalla console CloudFront o dall'API CloudFront. Puoi scegliere solo un bucket Amazon S3 per ricevere i log.
3. Visualizza i log di accesso.

Scelta di un bucket Amazon S3 per i log standard

Quando abiliti la registrazione per una distribuzione, specifichi il bucket Amazon S3 in cui desideri che CloudFront memorizzi i file di log. Se utilizzi Amazon S3 come origine, ti consigliamo di utilizzare un bucket separato per i file di log.

Specifica il bucket Amazon S3 in cui CloudFront deve archiviare i log di accesso, ad esempio `amzn-s3-demo-bucket.s3.amazonaws.com`.

Puoi archiviare i file di log per più distribuzioni nello stesso bucket. Quando attivi la registrazione, puoi specificare un prefisso facoltativo per i nomi di file, in modo da sapere quali file di log sono associati a quali distribuzioni.

Informazioni sulla scelta di un bucket S3

- La lista di controllo degli accessi (ACL) deve essere abilitata nel bucket. Se scegli un bucket senza ACL abilitata dalla console CloudFront, verrà visualizzato un messaggio di errore. Per informazioni, consulta Autorizzazioni.
- Non scegliere un bucket Amazon S3 con Proprietà dell'oggetto S3 impostato su bucket owner enforced. Questa impostazione disabilita gli ACL per il bucket e gli oggetti in esso contenuti, il che impedisce a CloudFront di consegnare i file di log al bucket.
- Non scegliere un bucket Amazon S3 nelle seguenti Regioni AWS. CloudFront non invia log standard ai bucket in queste regioni:
  - Africa (Città del Capo)
  - Asia Pacifico (Hong Kong)
  - Asia Pacific (Hyderabad)

- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Canada occidentale (Calgary)
- Europa (Milano)
- Europa (Spagna)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)

Autorizzazioni

Important

A partire da aprile 2023, devi abilitare gli ACL S3 per i nuovi bucket S3 utilizzati per i log standard di CloudFront. Puoi abilitare gli ACL quando crei un bucket o per un bucket esistente.
Per ulteriori informazioni sulle modifiche, consultare le domande frequenti sulle impostazioni predefinite per i nuovi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service e Heads-Up: Amazon S3 Security Changes Are Coming in April of 2023 nel Blog AWS News.

L'Account AWS deve disporre delle seguenti autorizzazioni per il bucket specificato per i file di log:

- L'ACL per il bucket deve concedere l'autorizzazione `FULL_CONTROL`. Se sei il proprietario del bucket, il tuo account dispone di questa autorizzazione per impostazione predefinita. Se non lo sei, il proprietario del bucket deve aggiornare l'ACL per il bucket.
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

ACL per il bucket

Quando si crea o si aggiorna una distribuzione e si abilita la registrazione, CloudFront utilizza queste autorizzazioni per aggiornare l'ACL per il bucket per concedere l'autorizzazione

`awslogsdelivery` dell'account `FULL_CONTROL`. L'account `awslogsdelivery` scrive i file di log nel bucket. Se l'account non dispone delle autorizzazioni necessarie per l'aggiornamento dell'ACL, la creazione o l'aggiornamento della distribuzione non riuscirà.

In alcuni casi, se invii una richiesta a livello di codice per creare un bucket, ma un bucket con il nome specificato esiste già, S3 reimposta le autorizzazioni per il bucket sul valore di default. Se hai configurato CloudFront per salvare log di accesso in un S3 bucket e non ricevi più i log in quel bucket, controlla le autorizzazioni per il bucket per accertarti che CloudFront disponga delle autorizzazioni necessarie.

Ripristino dell'ACL per il bucket

Se si rimuovono le autorizzazioni per l'account `awslogsdelivery`, CloudFront non sarà in grado di salvare i log nel S3 bucket. Per consentire a CloudFront di iniziare nuovamente a salvare i log per la distribuzione, ripristinare l'autorizzazione ACL in uno dei seguenti modi:

- Disabilitare il log per la distribuzione in CloudFront e quindi abilitarlo di nuovo. Per ulteriori informazioni, consulta Registrazione di log standard.
- Aggiungere l'autorizzazione ACL per `awslogsdelivery` manualmente passando al S3 bucket della console Amazon S3 e aggiungendo l'autorizzazione. Per aggiungere l'ACL per `awslogsdelivery`, è necessario fornire l'ID canonico per l'account, che è il seguente:

  ```
  c4c1ede66af53448b93c283ce9448c4ba468c9432aa01d700d3878632f77d2d0
  ```

  Per ulteriori informazioni sull'aggiunta di ACL ai bucket S3, consulta Configurazione di ACL nella Guida per l'utente di Amazon Simple Storage Service Console.

ACL per ogni file di log

Oltre all'ACL sul bucket, è disponibile un ACL su ogni file di log. Il proprietario del bucket dispone dell'autorizzazione `FULL_CONTROL` su ciascun file di log, il proprietario della distribuzione (se diverso dal proprietario del bucket) non ha autorizzazioni e l'account `awslogsdelivery` dispone di autorizzazioni in lettura e in scrittura.

Disattivazione della registrazione

Se disattivi la registrazione, CloudFront non elimina le liste ACL per il bucket o per i file di log. Puoi eliminare gli ACL, se necessario.

Policy chiave necessarie per i bucket SSE/KMS

Se il bucket S3 per i log standard utilizza la crittografia lato server con AWS KMS keys (SSE-KMS) utilizzando una chiave gestita dal cliente, è necessario aggiungere l'istruzione seguente alla policy della chiave gestita dal cliente. Ciò consente a CloudFront di scrivere file di log nel bucket. Non è possibile utilizzare SSE-KMS con la Chiave gestita da AWS perché CloudFront non sarà in grado di scrivere file di log nel bucket.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Se il bucket S3 per i log standard utilizza SSE-KMS con una chiave del bucket S3, è necessario anche aggiungere l'autorizzazione `kms:Decrypt` alla dichiarazione di policy. In tal caso, l'istruzione completa della policy è simile alla seguente.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

> **Note**
>
> Quando abiliti SSE-KMS per il bucket S3, specifica l'ARN completo per la chiave gestita dal cliente. Per ulteriori informazioni, consulta Specifica della crittografia lato server con AWS KMS keys (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

Abilitazione della registrazione di log standard (legacy)

Per abilitare i log standard, utilizza la console CloudFront o l'API CloudFront.

Indice

Abilitazione della registrazione di log standard (legacy) (console CloudFront)

Come abilitare la registrazione di log standard per una distribuzione CloudFront (console)

1. Utilizza la console CloudFront per creare una nuova distribuzione o aggiornarne una esistente.
2. Nella sezione Registrazione di log standard, per Consegna di log, scegli Attivo.
3. (Facoltativo) Per Registrazione di cookie, scegli Attivo se desideri includere i cookie nei log. Per ulteriori informazioni, consulta Registrazione dei cookie.

   > **Tip**
   >
   > Registrazione di cookie è un'impostazione globale che si applica a tutti i log standard per la distribuzione. Non puoi sovrascrivere questa impostazione per destinazioni di consegna separate.

4. Per la sezione Consegna a, specifica Amazon S3 (Legacy).
5. Specifica il bucket Amazon S3. Se non ne hai già uno, puoi scegliere Crea o consultare la documentazione per creare un bucket.
6. (Facoltativo) Per Prefisso di log, specifica l'eventuale stringa utilizzata da CloudFront come prefisso per i nomi dei file di log di accesso per questa distribuzione, ad esempio, `exampleprefix/`. La barra finale (/) è facoltativa ma consigliata per semplificare la navigazione nei file di log. Per ulteriori informazioni, consulta Log Prefix (Prefisso log).
7. Completa le fasi per aggiornare o creare la distribuzione.
8. Nella pagina Log, verifica che lo stato dei log standard sia Abilitato accanto alla distribuzione.

   Per ulteriori informazioni sui campi di log e di consegna della registrazione di log standard, consulta Riferimento alla registrazione di log standard.

Abilitazione della registrazione di log standard (legacy) (API CloudFront)

Puoi anche utilizzare l'API CloudFront per abilitare i log standard per le distribuzioni.

Come abilitare i log standard per una distribuzione (API CloudFront)

- Utilizza l'operazione API CreateDistribution o UpdateDistribution e configura l'oggetto LoggingConfig.

Modifica delle impostazioni di registrazione di log standard

Puoi attivare o disattivare la registrazione, modificare il bucket Amazon S3 in cui sono memorizzati i registri e modificare il prefisso per i file di registro utilizzando la console CloudFront o l'API CloudFront. Le modifiche apportate alle impostazioni di registrazione diventano effettive entro 12 ore.

Per ulteriori informazioni, consultare i seguenti argomenti:

- Per aggiornare una distribuzione utilizzando la console CloudFront, consulta Aggiornamento di una distribuzione.
- Per aggiornare una distribuzione utilizzando l'API CloudFront, consulta UpdateDistribution nella Guida di riferimento API di Amazon CloudFront.

Invio di log ad Amazon S3

Quando invii i log ad Amazon S3, vengono visualizzati nel seguente formato.

Formato del nome file

Il nome di ogni file di log che CloudFront salva nel tuo bucket Amazon S3 utilizza il seguente formato di nome di file:

```
<optional prefix>/<distribution ID>.YYYY-MM-DD-HH.unique-ID.gz
```

La data e l'ora sono in formato UTC.

Ad esempio, se si utilizza `example-prefix` come prefisso e l'ID di distribuzione è `EMLARXS9EXAMPLE`, i nomi dei file sono simili al seguente:

```
example-prefix/EMLARXS9EXAMPLE.2019-11-14-20.RT4KCN4SGK9.gz
```

Quando attivi la registrazione per una distribuzione, puoi specificare un prefisso facoltativo per i nomi di file, in modo da sapere quali file di log sono associati a quali distribuzioni. Se si include un valore per il prefisso del file di log e il prefisso non termina con una barra (/), CloudFront ne aggiunge una automaticamente. Se il prefisso termina con una barra, CloudFront non ne aggiunge un'altra.

L'estensione `.gz` alla fine del nome del file indica che CloudFront ha compresso il file di log utilizzando gzip.

Formato file registro standard

Ogni voce in un file di log fornisce informazioni dettagliate su una singola richiesta visualizzatore. I file di registro presentano le seguenti caratteristiche:

- Utilizzano il formato di file di log W3C esteso.
- Contengono valori separati da tabulatore.
- Contengono record che non sono necessariamente in ordine cronologico.
- Contengono due righe di intestazione: una con la versione del formato del file e un'altra che elenca i campi W3C inclusi in ogni record.
- Contengono equivalenti con codifica URL per spazi e per alcuni altri caratteri nei valori dei campi.

  Gli equivalenti con codifica URL vengono utilizzati per i seguenti caratteri:

  - Codici di caratteri ASCII da 0 a 32, inclusi
  - Codici di caratteri ASCII 127 e superiori
  - Tutti i caratteri nella tabella seguente

  Lo standard di codifica URL è definito in RFC 1738.

Valore con codifica URL	Carattere
%3C	<
%3E	>
%22	"
%23	#
%25	%

Valore con codifica URL	Carattere
%7B	{
%7D	}
%7C	|
%5C	\
%5E	^
%7E	~
%5B	[
%5D	]
%60	`
%27	'
%20	spazio

Eliminazione di file di log

CloudFront non elimina automaticamente i file di log dal bucket Amazon S3. Per ulteriori informazioni sull'eliminazione di file di log da un bucket Amazon S3, consulta Eliminazione di oggetti nella Guida per l'utente di Amazon Simple Storage Service Console.

Prezzi

La registrazione standard è una caratteristica facoltativa di CloudFront. CloudFront non addebita alcun costo per l'abilitazione dei log standard. Tuttavia, vengono addebitati i costi Amazon S3 usuali inerenti all'archiviazione dei file e all'accesso agli stessi in Amazon S3. Puoi eliminarli in qualsiasi momento.

Per maggiori informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

Per ulteriori informazioni sui prezzi di CloudFront, consulta i Prezzi di CloudFront.

Riferimento alla registrazione di log standard

Le sezioni seguenti si applicano sia alla registrazione di log standard (v2) che alla registrazione di log standard (legacy).

Argomenti

Tempistica della consegna dei file di log

CloudFront consegna i log per una distribuzione fino a diverse volte all'ora. In generale, un file di registro contiene informazioni sulle richieste CloudFront ricevute in un determinato periodo di tempo. CloudFront in genere consegna il file di registro per quel periodo di tempo a destinazione entro un'ora dagli eventi visualizzati nel registro. Nota, tuttavia, che alcune o tutte le voci di file di log relative a un periodo di tempo possono talvolta essere ritardate fino a 24 ore. Quando le voci di registro vengono ritardate, le CloudFront salva in un file di registro il cui nome del file include la data e l'ora del periodo in cui si sono verificate le richieste, non la data e l'ora di consegna del file.

Quando si crea un file di registro, CloudFront consolida le informazioni per la distribuzione da tutte le edge location che hanno ricevuto le richieste relative agli oggetti durante il periodo di tempo coperto dal file di registro.

CloudFront può salvare più di un file per un periodo di tempo a seconda del numero di richieste CloudFront ricevute per gli oggetti associati a una distribuzione.

CloudFront inizia a fornire in modo affidabile i log di accesso circa quattro ore dopo l'attivazione della registrazione. È possibile che tu ottenga alcuni log di accesso prima di quel momento.

> **Note**
>
> Se nessun utente richiede i tuoi oggetti durante il periodo di tempo, non riceverai alcun file di log per quel periodo.

Modalità di registrazione delle richieste quando l'URL o le intestazioni di richiesta superano la dimensione massima.

Se la dimensione totale di tutte le intestazioni di richiesta, inclusi i cookie, supera i 20 KB o se l'URL supera 8192 byte, CloudFront non può analizzare completamente la richiesta e non è in grado di registrare la richiesta. Poiché la richiesta non viene registrata, nei file di log non sarà possibile visualizzare il codice di stato dell'errore HTTP restituito.

Se il corpo della richiesta supera la dimensione massima, la richiesta viene registrata, incluso il codice di stato dell'errore HTTP.

Campi di file di log

Il file di registro di una distribuzione contiene 33 campi. L'elenco seguente contiene ogni nome di campo, in ordine, insieme a una descrizione delle informazioni contenute in tale campo.

1. **`date`**

   La data in cui si è verificato l'evento nel formato `YYYY-MM-DD`. Ad esempio, `2019-06-30`. La data e l'ora sono in formato UTC. Per WebSocket le connessioni, questa è la data di chiusura della connessione.

2. **`time`**

   L'ora in cui il CloudFront server ha finito di rispondere alla richiesta (in UTC), ad esempio,. `01:42:39` Per WebSocket le connessioni, questo è il momento in cui la connessione viene chiusa.

3. **`x-edge-location`**

   La edge location che ha servito la richiesta. Ogni posizione del bordo è identificata da un codice di tre lettere e da un numero assegnato arbitrariamente (ad esempio, DFW3). Il codice di tre lettere di solito corrisponde al codice aeroportuale della IATA (International Air Transport Association) per l'aeroporto vicino alla posizione geografica della posizione edge. (Queste abbreviazioni potrebbero cambiare in futuro).

4. **`sc-bytes`**

   Il numero totale di byte che il server ha inviato al visualizzatore in risposta alla richiesta, incluse le intestazioni. Per le connessioni WebSocket e gRPC, questo è il numero totale di byte inviati dal server al client tramite la connessione.

5. **`c-ip`**

L'indirizzo IP del visualizzatore che ha effettuato la richiesta, ad esempio, `192.0.2.183` o `2001:0db8:85a3::8a2e:0370:7334`. Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico (load balancer) per inviare la richiesta, il valore di questo campo è l'indirizzo IP del proxy o del sistema di bilanciamento (load balancer) del carico. Vedere anche il campo `x-forwarded-for`.

6. **`cs-method`**

   Il metodo di richiesta HTTP ricevuto dal visualizzatore.

7. **`cs(Host)`**

   Il nome di dominio della CloudFront distribuzione (ad esempio, d111111abcdef8.cloudfront.net).

8. **`cs-uri-stem`**

   La parte dell'URL della richiesta che identifica il percorso e l'oggetto (ad esempio, `/images/cat.jpg`). Punti interrogativi (?) le stringhe in URLs e di query non sono incluse nel registro.

9. **`sc-status`**

   Contiene uno dei seguenti valori:

   - Il codice di stato HTTP della risposta del server (ad esempio, `200`).
   - `000`, che indica che il visualizzatore ha chiuso la connessione prima che il server potesse rispondere alla richiesta. Se il visualizzatore chiude la connessione dopo che il server inizia a inviare la risposta, questo campo contiene il codice di stato HTTP della risposta che il server ha iniziato a inviare.

10. **`cs(Referer)`**

    Il valore dell'intestazione `Referer` nella richiesta. Questo è il nome del dominio all'origine della richiesta. I referrer comuni includono motori di ricerca, altri siti Web con collegamenti diretti ai tuoi oggetti e il tuo sito Web.

11. **`cs(User-Agent)`**

    Il valore dell'intestazione `User-Agent` nella richiesta. L'intestazione `User-Agent` identifica l'origine della richiesta, ad esempio il tipo di dispositivo e browser che ha inviato la richiesta e, se la richiesta proveniva da un motore di ricerca, il motore di ricerca.

12. **`cs-uri-query`**

    L'eventuale parte della stringa di query nell'URL.

Quando un URL non contiene una stringa di query, il valore di questo campo è un trattino (-). Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.

13 **`cs(Cookie)`**

L'intestazione `Cookie` nella richiesta, incluse le coppie nome-valore e gli attributi associati.

Se abiliti la registrazione dei cookie, CloudFront registra i cookie in tutte le richieste indipendentemente dai cookie che scegli di inoltrare all'origine. Quando una richiesta non include un'intestazione di cookie, il valore di questo campo è un trattino (-). Per ulteriori informazioni sui cookie, consulta Caching dei contenuti basati su cookie.

14 **`x-edge-result-type`**

Come il server ha classificato la risposta dopo che l'ultimo byte ha lasciato il server. In alcuni casi, il tipo di risultato può variare tra il momento in cui il server è pronto a inviare la risposta e il momento in cui ha finito di inviare la risposta. Vedere anche il campo `x-edge-response-result-type`.

Ad esempio, in streaming HTTP, si supponga che il server trovi un segmento del flusso nella cache. In questo scenario, il valore di questo campo sarebbe normalmente `Hit`. Tuttavia, se il visualizzatore chiude la connessione prima che il server abbia distribuito l'intero segmento, il tipo di risultato finale, e quindi il valore di questo campo, è `Error`.

WebSocket e le connessioni gRPC avranno un valore `Miss` per questo campo perché il contenuto non è memorizzabile nella cache e viene inviato tramite proxy direttamente all'origine.

I valori possibili includono:

- `Hit` – Il server ha servito l'oggetto al visualizzatore dalla cache.
- `RefreshHit` – Il server ha trovato l'oggetto nella cache, ma l'oggetto era scaduto, pertanto il server ha contattato l'origine per verificare che la cache disponesse della versione più recente dell'oggetto.
- `Miss` – La richiesta non è stata soddisfatta da un oggetto nella cache, per cui il server ha inoltrato la richiesta all'origine e ha restituito il risultato al visualizzatore.
- `LimitExceeded`— La richiesta è stata rifiutata perché è stata superata una CloudFront quota (precedentemente denominata limite).

- `CapacityExceeded`: il server ha restituito un codice di stato HTTP 503 in quanto non disponeva di capacità sufficiente al momento della richiesta per servire l'oggetto.
- `Error` – In genere, ciò significa che la richiesta ha provocato un errore client (il valore del campo `sc-status` è compreso nell'intervallo `4xx`) o un errore del server (il valore del campo `sc-status` è nell'intervallo `5xx`). Se il valore del campo `sc-status` è `200`, o se il valore di questo campo è `Error` e il valore del campo `x-edge-response-result-type` non è `Error`, significa che la richiesta HTTP ha avuto esito positivo, ma il client si è disconnesso prima di ricevere tutti i byte.
- `Redirect` – Il server ha reindirizzato il visualizzatore da HTTP a HTTPS in base alle impostazioni di distribuzione.
- `LambdaExecutionError`— La funzione Lambda @Edge associata alla distribuzione non è stata completata a causa di un'associazione non valida, di un timeout della funzione, di un problema di AWS dipendenza o di un altro problema di disponibilità generale.

15. **`x-edge-request-id`**

    Una stringa opaca che identifica in modo univoco una richiesta. CloudFront invia anche questa stringa nell'intestazione della `x-amz-cf-id` risposta.

16. **`x-host-header`**

    Il valore che il visualizzatore ha incluso nell'intestazione `Host` per questa richiesta. Se utilizzi il nome di CloudFront dominio nel tuo oggetto URLs (ad esempio d111111abcdef8.cloudfront.net), questo campo contiene quel nome di dominio. Se utilizzi nomi di dominio alternativi () nell'oggetto (come www.example.comCNAMEs), questo campo contiene il nome di dominio URLs alternativo.

    Se utilizzi i nomi di dominio alternativi, consulta `cs(Host)` nel campo 7 per il nome di dominio associato alla distribuzione.

17. **`cs-protocol`**

    Protocollo della richiesta del visualizzatore (`http`, `https`, `grpcs`, `ws` o `wss`).

18. **`cs-bytes`**

    Numero totale di byte di dati che il visualizzatore ha incluso nella richiesta, incluse le intestazioni. Per le connessioni WebSocket e gRPC, questo è il numero totale di byte inviati dal client al server sulla connessione.

19. **`time-taken`**

Il numero di secondi (al millesimo di secondo, ad esempio 0,082) da quando il server riceve la richiesta del visualizzatore a quando il server scrive l'ultimo byte della risposta alla coda di output, misurato sul server. Dal punto di vista del visualizzatore, il tempo totale per ottenere l'oggetto sarà maggiore di questo valore a causa della latenza di rete e del buffering TCP.

20 **`x-forwarded-for`**

Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico (load balancer) per inviare la richiesta, il valore di questo campo `c-ip` è l'indirizzo IP del proxy o del sistema di bilanciamento (load balancer) del carico. In tal caso, questo campo è l'indirizzo IP del visualizzatore all'origine della richiesta. Questo campo può contenere più indirizzi IP separati da virgole. Ogni indirizzo IP può essere un IPv4 indirizzo (ad esempio,`192.0.2.183`) o un IPv6 indirizzo (ad esempio,`2001:0db8:85a3::8a2e:0370:7334`).

Se il visualizzatore non ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico (load balancer), questo valore è un trattino (-).

21 **`ssl-protocol`**

Quando la richiesta utilizza HTTPS, questo campo contiene il SSL/TLS protocollo negoziato dal visualizzatore e dal server per trasmettere la richiesta e la risposta. Per un elenco dei valori possibili, consulta i SSL/TLS protocolli supportati in. Protocolli e cifrari supportati tra visualizzatori e CloudFront

Quando `cs-protocol` nel campo 17 è `http`, il valore per questo campo è un trattino (-).

22 **`ssl-cipher`**

Quando la richiesta utilizzava HTTPS, questo campo contiene il SSL/TLS codice negoziato dal visualizzatore e dal server per crittografare la richiesta e la risposta. Per un elenco dei valori possibili, consulta i cifrari supportati in. SSL/TLS Protocolli e cifrari supportati tra visualizzatori e CloudFront

Quando `cs-protocol` nel campo 17 è `http`, il valore per questo campo è un trattino (-).

23 **`x-edge-response-result-type`**

Il modo in cui il server edge ha classificato la risposta appena prima di restituire la risposta al visualizzatore. Vedere anche il campo `x-edge-result-type`. I valori possibili includono:

- `Hit` – Il server ha servito l'oggetto al visualizzatore dalla cache.

- `RefreshHit` – Il server ha trovato l'oggetto nella cache, ma l'oggetto era scaduto, pertanto il server ha contattato l'origine per verificare che la cache disponesse della versione più recente dell'oggetto.
- `Miss` – La richiesta non poteva essere soddisfatta da un oggetto nella cache, per cui il server ha inoltrato la richiesta al server di origine e ha restituito il risultato al visualizzatore.
- `LimitExceeded`— La richiesta è stata respinta perché è stata superata una CloudFront quota (precedentemente denominata limite).
- `CapacityExceeded`: il server ha restituito un errore 503 in quanto non disponeva di capacità sufficiente al momento della richiesta per servire l'oggetto.
- `Error` – In genere, ciò significa che la richiesta ha provocato un errore client (il valore del campo `sc-status` è compreso nell'intervallo `4xx`) o un errore del server (il valore del campo `sc-status` è nell'intervallo `5xx`).

  Se il valore del campo `x-edge-result-type` è `Error` e il valore di questo campo non è `Error`, il client è stato disconnesso prima del completamento del download.
- `Redirect` – Il server ha reindirizzato il visualizzatore da HTTP a HTTPS in base alle impostazioni di distribuzione.
- `LambdaExecutionError`— La funzione Lambda @Edge associata alla distribuzione non è stata completata a causa di un'associazione non valida, di un timeout della funzione, di un problema di AWS dipendenza o di un altro problema di disponibilità generale.

24. **`cs-protocol-version`**

    La versione HTTP che il visualizzatore ha specificato nella richiesta. I valori possibili sono `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` e `HTTP/3.0`.

25. **`fle-status`**

    Quando la crittografia a livello di campo è configurata per una distribuzione, questo campo contiene un codice che indica se il corpo della richiesta è stato elaborato correttamente. Quando il server elabora il corpo della richiesta, crittografa valori nei campi specificati e inoltra la richiesta all'origine, il valore di questo campo è `Processed`. Il valore di `x-edge-result-type` in questo caso può ancora indicare un errore lato client o lato server.

    I valori possibili per questo campo sono:

    - `ForwardedByContentType` – Il server ha inoltrato la richiesta all'origine senza analisi o crittografia poiché non è stato configurato alcun tipo di contenuto.

- `ForwardedByQueryArgs`: il server ha inoltrato la richiesta all'origine senza analisi o crittografia in quanto la richiesta contiene un argomento di query che non era nella configurazione per la crittografia a livello di campo.
- `ForwardedDueToNoProfile` – Il server ha inoltrato la richiesta all'origine senza analisi o crittografia in quanto nessun profilo è stato specificato nella configurazione per la crittografia a livello di campo.
- `MalformedContentTypeClientError` – Il server ha rifiutato la richiesta e ha restituito un codice di stato HTTP 400 al visualizzatore perché il valore dell'intestazione `Content-Type` era in un formato non valido.
- `MalformedInputClientError` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché il corpo della richiesta non era in un formato valido.
- `MalformedQueryArgsClientError` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché un argomento di query era vuoto o non era in un formato valido.
- `RejectedByContentType` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché nessun tipo di contenuto è stato specificato nella configurazione per la crittografia a livello di campo.
- `RejectedByQueryArgs` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché nessun argomento di query è stato specificato nella configurazione per la crittografia a livello di campo.
- `ServerError` – Il server di origine ha restituito un errore.

Se la richiesta supera una quota di crittografia a livello di campo (in precedenza definita limite), questo campo contiene uno dei seguenti codici di errore e il server restituisce il codice di stato HTTP 400 al visualizzatore. Per un elenco delle quote correnti della crittografia a livello di campo, consulta Quote della crittografia a livello di campo.

- `FieldLengthLimitClientError` – Un campo configurato per essere crittografato quando viene superata la massima lunghezza.
- `FieldNumberLimitClientError` – Una richiesta che la distribuzione è configurata per crittografare contiene più campi di quelli consentiti.
- `RequestLengthLimitClientError` – La lunghezza del corpo della richiesta supera la lunghezza massima consentita quando è configurata la crittografia a livello di campo.

Se la crittografia a livello di campo non è configurata per la distribuzione, il valore di questo campo è un trattino (-).

26. **`fle-encrypted-fields`**

    Il numero di campi di crittografia a livello di campo che il server ha crittografato e inoltrato all'origine. CloudFront i server trasmettono la richiesta elaborata all'origine mentre crittografano i dati, quindi questo campo può avere un valore anche se il valore di è un errore. `fle-status`

    Se la crittografia a livello di campo non è configurata per la distribuzione, il valore di questo campo è un trattino (-).

27. **`c-port`**

    Il numero di porta della richiesta del visualizzatore.

28. **`time-to-first-byte`**

    Il numero di secondi tra la ricezione della richiesta e la scrittura del primo byte della risposta, misurato sul server.

29. **`x-edge-detailed-result-type`**

    Questo campo contiene lo stesso valore del campo `x-edge-result-type`, tranne nei seguenti casi:

    - Quando l'oggetto è stato servito al visualizzatore dal livello Origin Shield, questo campo contiene `OriginShieldHit`.
    - Quando l'oggetto non era nella CloudFront cache e la risposta è stata generata da una funzione Lambda @Edge di richiesta di origine, questo campo contiene. `MissGeneratedResponse`
    - Quando il valore del campo `x-edge-result-type` è `Error`, questo campo contiene uno dei seguenti valori con ulteriori informazioni sull'errore:
      - `AbortedOrigin` – Il server ha riscontrato un problema con l'origine.
      - `ClientCommError` – La risposta al visualizzatore è stata interrotta a causa di un problema di comunicazione tra il server edge e il visualizzatore.
      - `ClientGeoBlocked`: la distribuzione è configurata per rifiutare le richieste dalla posizione geografica del visualizzatore.
      - `ClientHungUpRequest` — Il visualizzatore si è arrestato prematuramente durante l'invio della richiesta.
      - `Error`: si è verificato un errore per il quale il tipo di errore non si adatta a nessuna delle altre categorie. Questo tipo di errore può verificarsi quando il server edge serve una risposta di errore dalla cache.
      - `InvalidRequest` – Il server ha ricevuto una richiesta non valida dal visualizzatore.

- `InvalidRequestBlocked` — L'accesso alla risorsa richiesta è bloccato.
- `InvalidRequestCertificate`— La distribuzione non corrisponde al SSL/TLS certificato per il quale è stata stabilita la connessione HTTPS.
- `InvalidRequestHeader` —-La richiesta conteneva un'intestazione non valida.
- `InvalidRequestMethod` — La distribuzione non è configurata per gestire il metodo di richiesta HTTP utilizzato. Questo può accadere quando la distribuzione supporta solo le richieste memorizzabili nella cache.
- `OriginCommError` - La richiesta è scaduta durante la connessione a un'origine o durante la lettura di dati da un'origine.
- `OriginConnectError`: il server non è riuscito a connettersi all'origine.
- `OriginContentRangeLengthError`: l'intestazione `Content-Length` nella risposta dell'origine non corrisponde alla lunghezza dell'intestazione `Content-Range`.
- `OriginDnsError`: il server non è riuscito a risolvere il nome di dominio dell'origine.
- `OriginError` — L'origine ha restituito una risposta errata.
- `OriginHeaderTooBigError` - Un'intestazione restituita dall'origine è troppo grande per essere elaborata dal server edge.
- `OriginInvalidResponseError` — L'origine ha restituito una risposta non valida.
- `OriginReadError`: il server non è in grado di leggere dall'origine.
- `OriginWriteError`: il server non è in grado di scrivere sull'origine.
- `OriginZeroSizeObjectError` — Un oggetto di dimensione zero inviato dall'origine ha generato un errore.
- `SlowReaderOriginError` — Il visualizzatore ha letto lentamente il messaggio che ha causato l'errore di origine.

30 **`sc-content-type`**

Il valore dell'intestazione HTTP `Content-Type` della risposta.

31 **`sc-content-len`**

Il valore dell'intestazione HTTP `Content-Length` della risposta.

32 **`sc-range-start`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore iniziale dell'intervallo.

33 **`sc-range-end`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore finale dell'intervallo.

34 **`distribution-tenant-id`**

L'ID del tenant di distribuzione.

35 **`connection-id`**

Un identificatore univoco per la connessione TLS.

È necessario abilitare MTL per le distribuzioni prima di poter ottenere informazioni per questo campo. Per ulteriori informazioni, consulta Visualizzatore TLS reciproco (mTLS).

Di seguito è riportato un esempio di file di log di una distribuzione.

```
#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 - -
```

Analisi dei log

Poiché puoi ricevere più log di accesso all'ora, ti consigliamo di riunire tutti i file di log che ricevi per un determinato periodo di tempo in un unico file. Ciò ti consente di analizzare i dati per quel periodo in modo più accurato e completo.

Per analizzare i log di accesso puoi utilizzare Amazon Athena. Athena è un servizio di interrogazione interattivo che può aiutarti ad analizzare i dati per AWS servizi, tra cui. CloudFront Per ulteriori informazioni, consulta la sezione Querying Amazon CloudFront Logs nella Amazon Athena User Guide.

Inoltre, i seguenti post di AWS blog illustrano alcuni modi per analizzare i log di accesso.

- Amazon CloudFront Request Logging (per contenuti forniti tramite HTTP)
- CloudFront Registri migliorati, ora con stringhe di query

Utilizza i log di accesso in tempo reale

Con i log di accesso CloudFront in tempo reale, puoi ottenere informazioni sulle richieste fatte a una distribuzione in tempo reale (i log vengono consegnati entro pochi secondi dalla ricezione delle richieste). È possibile utilizzare i log di accesso in tempo reale per monitorare, analizzare e intraprendere azioni in base alle prestazioni di distribuzione dei contenuti.

CloudFront i registri di accesso in tempo reale sono configurabili. È possibile scegliere:

- La frequenza di campionamento dei log in tempo reale, ovvero la percentuale di richieste per le quali desideri ricevere i record dei log di accesso in tempo reale.
- I campi specifici che si desidera ricevere nei record di registro.
- I comportamenti specifici della cache (pattern di percorso) per i quali si desidera ricevere i registri in tempo reale.

CloudFront i log di accesso in tempo reale vengono forniti al flusso di dati di tua scelta in Amazon Kinesis Data Streams. Puoi creare il tuo consumer Kinesis Data Stream o utilizzare Amazon Data Firehose per inviare i dati di log ad Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service (Service) o a un OpenSearch servizio di elaborazione dei OpenSearch log di terze parti.

CloudFront costi per i log di accesso in tempo reale, oltre ai costi sostenuti per l'utilizzo di Kinesis Data Streams. Per ulteriori informazioni sui prezzi, consulta i prezzi di Amazon e CloudFront i prezzi di Amazon Kinesis Data Streams.

> **Important**
>
> Ti consigliamo di utilizzare i log per comprendere la natura delle richieste per i tuoi contenuti, non come contabilità completa di tutte le richieste. CloudFront fornisce registri di accesso in tempo reale con il massimo impegno. È possibile che la voce di log per una specifica richiesta venga distribuita molto tempo dopo l'elaborazione effettiva della richiesta e, in rari casi, che non venga distribuita affatto. Quando una voce di registro viene omessa dai registri di accesso in tempo reale, il numero di voci nei registri di accesso in tempo reale non corrisponderà all'utilizzo visualizzato nei report di fatturazione e utilizzo. AWS

Argomenti

Crea e utilizza configurazioni dei registri di accesso in tempo reale

Per ottenere informazioni sulle richieste fatte a una distribuzione in tempo reale, puoi utilizzare configurazioni di log di accesso in tempo reale. I log vengono consegnati entro pochi secondi dalla ricezione delle richieste. È possibile creare una configurazione del registro di accesso in tempo reale nella CloudFront console, con AWS Command Line Interface (AWS CLI) o con l' CloudFront API.

Per utilizzare una configurazione del registro degli accessi in tempo reale, è necessario collegarla a uno o più comportamenti della cache in una CloudFront distribuzione.

Console

Per creare una configurazione del registro di accesso in tempo reale

1. Accedi Console di gestione AWS e apri la pagina dei log nella CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home?#/logs.
2. Scegli la scheda Configurazioni in tempo reale.
3. Scegli Crea configurazione.
4. Per Nome, immetti un nome per la configurazione.
5. Per Frequenza di campionamento, immetti la percentuale di richieste per cui desideri ricevere record di log.
6. Per Fields, scegli i campi da ricevere nei log di accesso in tempo reale.
   - Per includere tutti i campi CMCD per i log, scegli Tutte le chiavi CMCD.
7. Per Endpoint, scegli uno o più flussi di dati Kinesis per ricevere i log di accesso in tempo reale.

   > **Note**
   >
   > CloudFront i log di accesso in tempo reale vengono forniti al flusso di dati specificato in Kinesis Data Streams. Per leggere e analizzare i log di accesso in tempo reale, puoi creare il tuo utente Kinesis Data Stream Consumer. Puoi anche utilizzare Firehose per inviare i dati di registro ad Amazon S3, Amazon Redshift, OpenSearch Amazon Service o a un servizio di elaborazione dei log di terze parti.

8. Per Ruolo IAM, scegli Crea nuovo ruolo di servizio o seleziona un ruolo esistente. È necessario disporre dell'autorizzazione per creare i ruoli IAM.

9. (Facoltativo) Per la distribuzione, scegli un comportamento di CloudFront distribuzione e cache da allegare alla configurazione del log di accesso in tempo reale.
10. Scegli Crea configurazione.

In caso di successo, la console mostra i dettagli della configurazione del registro di accesso in tempo reale appena creata.

Per ulteriori informazioni, consulta Comprendi le configurazioni dei log di accesso in tempo reale.

AWS CLI

Per creare una configurazione del registro di accesso in tempo reale con AWS CLI, usa il aws cloudfront create-realtime-log-config comando. È possibile utilizzare un file di input per fornire i parametri di input del comando, anziché specificare ogni singolo parametro come input della riga di comando.

Per creare una configurazione del registro di accesso in tempo reale (CLI con file di input)

1. Utilizzare il comando seguente per creare un file denominato `rtl-config.yaml` che contiene tutti i parametri di input per il comando create-realtime-log-config.

```
aws cloudfront create-realtime-log-config --generate-cli-skeleton yaml-input >
 rtl-config.yaml
```

2. Aprire il file `rtl-config.yaml` appena creato. Modifica il file per specificare le impostazioni di configurazione del registro di accesso in tempo reale che desideri, quindi salva il file. Tenere presente quanto segue:

   - Per `StreamType`, l'unico valore valido è `Kinesis`.

   Per ulteriori informazioni sulle impostazioni di configurazione di lunga durata in tempo reale, vedere Comprendi le configurazioni dei log di accesso in tempo reale.
3. Utilizzate il comando seguente per creare la configurazione del registro di accesso in tempo reale utilizzando i parametri di input dal `rtl-config.yaml` file.

```
aws cloudfront create-realtime-log-config --cli-input-yaml file://rtl-
config.yaml
```

In caso di successo, l'output del comando mostra i dettagli della configurazione del registro di accesso in tempo reale appena creata.

Per allegare una configurazione del registro di accesso in tempo reale a una distribuzione esistente (CLI con file di input)

1. Utilizzate il comando seguente per salvare la configurazione di distribuzione per la CloudFront distribuzione che desiderate aggiornare. Sostituisci *distribution_ID* con l'ID della distribuzione.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Aprire il file `dist-config.yaml` appena creato. Modifica il file, apportando le seguenti modifiche a ogni comportamento della cache che stai aggiornando per utilizzare una configurazione del registro di accesso in tempo reale.

   - Nel comportamento della cache, aggiungere un campo denominato `RealtimeLogConfigArn`. Per il valore del campo, usa l'ARN della configurazione del log di accesso in tempo reale che desideri allegare a questo comportamento della cache.
   - Rinominare il campo `ETag` in `IfMatch`, ma non modificare il valore del campo.

   Salvare il file al termine.

3. Usa il comando seguente per aggiornare la distribuzione in modo da utilizzare la configurazione del log di accesso in tempo reale. Sostituisci *distribution_ID* con l'ID della distribuzione.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

In caso di successo, l'output del comando mostra i dettagli della distribuzione appena aggiornata.

API

Per creare una configurazione del registro di accesso in tempo reale con l' CloudFront API, utilizza l'operazione CreateRealtimeLogConfigAPI. Per ulteriori informazioni sui parametri

specificati in questa chiamata API, consulta Comprendi le configurazioni dei log di accesso in tempo reale la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato una configurazione del registro di accesso in tempo reale, puoi collegarla a un comportamento della cache, utilizzando una delle seguenti operazioni API:

- Per collegarlo a un comportamento di cache in una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a un comportamento di cache in una nuova distribuzione, usa CreateDistribution.

Per entrambe queste operazioni API, fornisci l'ARN della configurazione del registro di accesso in tempo reale `RealtimeLogConfigArn` sul campo, all'interno di un comportamento di cache. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, Riferimento a tutte le impostazioni di distribuzione consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Comprendi le configurazioni dei log di accesso in tempo reale

Per utilizzare i log di accesso CloudFront in tempo reale, iniziate creando una configurazione dei log di accesso in tempo reale. La configurazione dei log di accesso in tempo reale contiene informazioni sui campi di registro che si desidera ricevere, sulla frequenza di campionamento per i record di log e sul flusso di dati Kinesis a cui si desidera inviare i log.

In particolare, una configurazione dei log di accesso in tempo reale contiene le seguenti impostazioni:

Indice

- Name
- Velocità di campionamento
- Campi
- Endpoint (flusso di dati Kinesis)
- Ruolo IAM

Name

Un nome per identificare la configurazione del registro di accesso in tempo reale.

Velocità di campionamento

La frequenza di campionamento è un numero intero compreso tra 1 e 100 (inclusi) che determina la percentuale di richieste degli spettatori inviate a Kinesis Data Streams come record del registro di accesso in tempo reale. Per includere ogni richiesta di visualizzazione nei log di accesso in tempo reale, specifica 100 per la frequenza di campionamento. Potresti scegliere una frequenza di campionamento inferiore per ridurre i costi, pur continuando a ricevere un campione rappresentativo dei dati delle richieste nei registri di accesso in tempo reale.

Campi

Un elenco dei campi inclusi in ogni record del registro degli accessi in tempo reale. Ogni record di registro può contenere fino a 40 campi ed è possibile scegliere di ricevere tutti i campi disponibili o solo i campi necessari per il monitoraggio e l'analisi delle prestazioni.

L'elenco seguente contiene ogni nome di campo e una descrizione delle informazioni contenute in tale campo. I campi vengono elencati nell'ordine in cui vengono visualizzati nei record di registro che vengono recapitati a Kinesis Data Streams.

I campi 46-63 sono dati comuni dei client multimediali (CMCD) a cui i client dei lettori multimediali possono inviare CDNs con ogni richiesta. Puoi utilizzare questi dati per comprendere ogni richiesta, come il tipo di supporto (audio, video), la velocità di riproduzione e la durata dello streaming. Questi campi verranno visualizzati nei registri di accesso in tempo reale solo se inviati a. CloudFront

1. **`timestamp`**

   Data e ora in cui il server edge ha terminato di rispondere alla richiesta.

2. **`c-ip`**

   L'indirizzo IP del visualizzatore che ha effettuato la richiesta, ad esempio, `192.0.2.183` o `2001:0db8:85a3::8a2e:0370:7334`. Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico (load balancer) per inviare la richiesta, il valore di questo campo è l'indirizzo IP del proxy o del sistema di bilanciamento (load balancer) del carico. Vedere anche il campo `x-forwarded-for`.

3. **`s-ip`**

   L'indirizzo IP del CloudFront server che ha fornito la richiesta, ad esempio, `192.0.2.183` o`2001:0db8:85a3::8a2e:0370:7334`.

4. **`time-to-first-byte`**

Il numero di secondi tra la ricezione della richiesta e la scrittura del primo byte della risposta, misurato sul server.

5. **`sc-status`**

   Il codice di stato HTTP della risposta del server (ad esempio, `200`).

6. **`sc-bytes`**

   Il numero totale di byte che il server ha inviato al visualizzatore in risposta alla richiesta, incluse le intestazioni. Per le connessioni WebSocket e gRPC, questo è il numero totale di byte inviati dal server al client tramite la connessione.

7. **`cs-method`**

   Il metodo di richiesta HTTP ricevuto dal visualizzatore.

8. **`cs-protocol`**

   Protocollo della richiesta del visualizzatore (`http`, `https`, `grpcs`, `ws` o `wss`).

9. **`cs-host`**

   Il valore che il visualizzatore ha incluso nell'intestazione `Host` per questa richiesta. Se utilizzi il nome di CloudFront dominio nel tuo oggetto URLs (ad esempio d111111abcdef8.cloudfront.net), questo campo contiene quel nome di dominio. Se utilizzi nomi di dominio alternativi () nell'oggetto (come www.example.comCNAMEs), questo campo contiene il nome di dominio URLs alternativo.

10. **`cs-uri-stem`**

    L'intero URL della richiesta, inclusa la stringa di query (se presente), ma senza il nome di dominio. Ad esempio, `/images/cat.jpg?mobile=true`.

    > **Note**
    >
    > Nei log standard, il valore `cs-uri-stem` non include la stringa di query.

11. **`cs-bytes`**

    Numero totale di byte di dati che il visualizzatore ha incluso nella richiesta, incluse le intestazioni. Per le connessioni WebSocket e gRPC, questo è il numero totale di byte inviati dal client al server sulla connessione.

12. **`x-edge-location`**

La edge location che ha servito la richiesta. Ogni edge location è identificata da un codice di tre lettere e da un numero assegnato arbitrariamente (ad esempio,). DFW3 Il codice di tre lettere di solito corrisponde al codice aeroportuale della IATA (International Air Transport Association) per l'aeroporto vicino alla posizione geografica della posizione edge. (Queste abbreviazioni potrebbero cambiare in futuro).

13. **`x-edge-request-id`**

    Una stringa opaca che identifica in modo univoco una richiesta. CloudFront invia anche questa stringa nell'intestazione della `x-amz-cf-id` risposta.

14. **`x-host-header`**

    Il nome di dominio della CloudFront distribuzione (ad esempio, d111111abcdef8.cloudfront.net).

15. **`time-taken`**

    Il numero di secondi (al millesimo di secondo, ad esempio 0,082) da quando il server riceve la richiesta del visualizzatore a quando il server scrive l'ultimo byte della risposta alla coda di output, misurato sul server. Dal punto di vista del visualizzatore, il tempo totale per ottenere l'oggetto sarà maggiore di questo valore a causa della latenza di rete e del buffering TCP.

16. **`cs-protocol-version`**

    La versione HTTP che il visualizzatore ha specificato nella richiesta. I valori possibili sono `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` e `HTTP/3.0`.

17. **`c-ip-version`**

    La versione IPv6 IP della richiesta (IPv4 o).

18. **`cs-user-agent`**

    Il valore dell'intestazione `User-Agent` nella richiesta. L'intestazione `User-Agent` identifica l'origine della richiesta, ad esempio il tipo di dispositivo e browser che ha inviato la richiesta e, se la richiesta proveniva da un motore di ricerca, il motore di ricerca.

19. **`cs-referer`**

    Il valore dell'intestazione `Referer` nella richiesta. Questo è il nome del dominio all'origine della richiesta. I referrer comuni includono motori di ricerca, altri siti Web con collegamenti diretti ai tuoi oggetti e il tuo sito Web.

20. **`cs-cookie`**

L'intestazione `Cookie` nella richiesta, incluse le coppie nome-valore e gli attributi associati.

> **Note**
>
> Questo campo viene troncato a 800 byte.

21. **`cs-uri-query`**

L'eventuale parte della stringa di query nell'URL.

22. **`x-edge-response-result-type`**

Il modo in cui il server edge ha classificato la risposta appena prima di restituire la risposta al visualizzatore. Vedere anche il campo `x-edge-result-type`. I valori possibili includono:

- `Hit` – Il server ha servito l'oggetto al visualizzatore dalla cache.
- `RefreshHit` – Il server ha trovato l'oggetto nella cache, ma l'oggetto era scaduto, pertanto il server ha contattato l'origine per verificare che la cache disponesse della versione più recente dell'oggetto.
- `Miss` – La richiesta non poteva essere soddisfatta da un oggetto nella cache, per cui il server ha inoltrato la richiesta al server di origine e ha restituito il risultato al visualizzatore.
- `LimitExceeded`— La richiesta è stata rifiutata perché è stata superata una CloudFront quota (precedentemente denominata limite).
- `CapacityExceeded`: il server ha restituito un errore 503 in quanto non disponeva di capacità sufficiente al momento della richiesta per servire l'oggetto.
- `Error` – In genere, ciò significa che la richiesta ha provocato un errore client (il valore del campo `sc-status` è compreso nell'intervallo `4xx`) o un errore del server (il valore del campo `sc-status` è nell'intervallo `5xx`).

  Se il valore del campo `x-edge-result-type` è `Error` e il valore di questo campo non è `Error`, il client è stato disconnesso prima del completamento del download.
- `Redirect` – Il server ha reindirizzato il visualizzatore da HTTP a HTTPS in base alle impostazioni di distribuzione.
- `LambdaExecutionError`— La funzione Lambda @Edge associata alla distribuzione non è stata completata a causa di un'associazione non valida, di un timeout della funzione, di un problema di AWS dipendenza o di un altro problema di disponibilità generale.

23. **`x-forwarded-for`**

Se il visualizzatore ha utilizzato un proxy HTTP o un sistema di bilanciamento del carico (load balancer) per inviare la richiesta, il valore di questo campo `c-ip` è l'indirizzo IP del proxy o del sistema di bilanciamento (load balancer) del carico. In tal caso, questo campo è l'indirizzo IP del visualizzatore all'origine della richiesta. Questo campo può contenere più indirizzi IP separati da virgole. Ogni indirizzo IP può essere un IPv4 indirizzo (ad esempio,`192.0.2.183`) o un IPv6 indirizzo (ad esempio,). `2001:0db8:85a3::8a2e:0370:7334`

24 **`ssl-protocol`**

Quando la richiesta utilizza HTTPS, questo campo contiene il SSL/TLS protocollo negoziato dal visualizzatore e dal server per trasmettere la richiesta e la risposta. Per un elenco dei valori possibili, consulta i SSL/TLS protocolli supportati in. Protocolli e cifrari supportati tra visualizzatori e CloudFront

25 **`ssl-cipher`**

Quando la richiesta utilizzava HTTPS, questo campo contiene il SSL/TLS codice negoziato dal visualizzatore e dal server per crittografare la richiesta e la risposta. Per un elenco dei valori possibili, consulta i cifrari supportati in. SSL/TLS Protocolli e cifrari supportati tra visualizzatori e CloudFront

26 **`x-edge-result-type`**

Come il server ha classificato la risposta dopo che l'ultimo byte ha lasciato il server. In alcuni casi, il tipo di risultato può variare tra il momento in cui il server è pronto a inviare la risposta e il momento in cui ha finito di inviare la risposta. Vedere anche il campo `x-edge-response-result-type`.

Ad esempio, in streaming HTTP, si supponga che il server trovi un segmento del flusso nella cache. In questo scenario, il valore di questo campo sarebbe normalmente `Hit`. Tuttavia, se il visualizzatore chiude la connessione prima che il server abbia distribuito l'intero segmento, il tipo di risultato finale, e quindi il valore di questo campo, è `Error`.

WebSocket e le connessioni gRPC avranno un valore `Miss` per questo campo perché il contenuto non è memorizzabile nella cache e viene inviato tramite proxy direttamente all'origine.

I valori possibili includono:

- `Hit` – Il server ha servito l'oggetto al visualizzatore dalla cache.

- `RefreshHit` – Il server ha trovato l'oggetto nella cache, ma l'oggetto era scaduto, pertanto il server ha contattato l'origine per verificare che la cache disponesse della versione più recente dell'oggetto.
- `Miss` – La richiesta non è stata soddisfatta da un oggetto nella cache, per cui il server ha inoltrato la richiesta all'origine e ha restituito il risultato al visualizzatore.
- `LimitExceeded`— La richiesta è stata rifiutata perché è stata superata una CloudFront quota (precedentemente denominata limite).
- `CapacityExceeded`: il server ha restituito un codice di stato HTTP 503 in quanto non disponeva di capacità sufficiente al momento della richiesta per servire l'oggetto.
- `Error` – In genere, ciò significa che la richiesta ha provocato un errore client (il valore del campo `sc-status` è compreso nell'intervallo `4xx`) o un errore del server (il valore del campo `sc-status` è nell'intervallo `5xx`). Se il valore del campo `sc-status` è `200`, o se il valore di questo campo è `Error` e il valore del campo `x-edge-response-result-type` non è `Error`, significa che la richiesta HTTP ha avuto esito positivo, ma il client si è disconnesso prima di ricevere tutti i byte.
- `Redirect` – Il server ha reindirizzato il visualizzatore da HTTP a HTTPS in base alle impostazioni di distribuzione.
- `LambdaExecutionError`— La funzione Lambda @Edge associata alla distribuzione non è stata completata a causa di un'associazione non valida, di un timeout della funzione, di un problema di AWS dipendenza o di un altro problema di disponibilità generale.

27. **`fle-encrypted-fields`**

    Il numero di campi di crittografia a livello di campo che il server ha crittografato e inoltrato all'origine. CloudFront i server trasmettono la richiesta elaborata all'origine mentre crittografano i dati, quindi questo campo può avere un valore anche se il valore di è un errore. `fle-status`

28. **`fle-status`**

    Quando la crittografia a livello di campo è configurata per una distribuzione, questo campo contiene un codice che indica se il corpo della richiesta è stato elaborato correttamente. Quando il server elabora il corpo della richiesta, crittografa valori nei campi specificati e inoltra la richiesta all'origine, il valore di questo campo è `Processed`. Il valore di `x-edge-result-type` in questo caso può ancora indicare un errore lato client o lato server.

    I valori possibili per questo campo sono:

- `ForwardedByContentType` – Il server ha inoltrato la richiesta all'origine senza analisi o crittografia poiché non è stato configurato alcun tipo di contenuto.
- `ForwardedByQueryArgs`: il server ha inoltrato la richiesta all'origine senza analisi o crittografia in quanto la richiesta contiene un argomento di query che non era nella configurazione per la crittografia a livello di campo.
- `ForwardedDueToNoProfile` – Il server ha inoltrato la richiesta all'origine senza analisi o crittografia in quanto nessun profilo è stato specificato nella configurazione per la crittografia a livello di campo.
- `MalformedContentTypeClientError` – Il server ha rifiutato la richiesta e ha restituito un codice di stato HTTP 400 al visualizzatore perché il valore dell'intestazione `Content-Type` era in un formato non valido.
- `MalformedInputClientError` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché il corpo della richiesta non era in un formato valido.
- `MalformedQueryArgsClientError` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché un argomento di query era vuoto o non era in un formato valido.
- `RejectedByContentType` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché nessun tipo di contenuto è stato specificato nella configurazione per la crittografia a livello di campo.
- `RejectedByQueryArgs` – Il server ha rifiutato la richiesta e restituito un codice di stato HTTP 400 al visualizzatore poiché nessun argomento di query è stato specificato nella configurazione per la crittografia a livello di campo.
- `ServerError` – Il server di origine ha restituito un errore.

Se la richiesta supera una quota di crittografia a livello di campo (in precedenza definita limite), questo campo contiene uno dei seguenti codici di errore e il server restituisce il codice di stato HTTP 400 al visualizzatore. Per un elenco delle quote correnti della crittografia a livello di campo, consulta Quote della crittografia a livello di campo.

- `FieldLengthLimitClientError` – Un campo configurato per essere crittografato quando viene superata la massima lunghezza.
- `FieldNumberLimitClientError` – Una richiesta che la distribuzione è configurata per crittografare contiene più campi di quelli consentiti.
- `RequestLengthLimitClientError` – La lunghezza del corpo della richiesta supera la lunghezza massima consentita quando è configurata la crittografia a livello di campo.

29 **`sc-content-type`**

Il valore dell'intestazione HTTP `Content-Type` della risposta.

30 **`sc-content-len`**

Il valore dell'intestazione HTTP `Content-Length` della risposta.

31 **`sc-range-start`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore iniziale dell'intervallo.

32 **`sc-range-end`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore finale dell'intervallo.

33 **`c-port`**

Il numero di porta della richiesta del visualizzatore.

34 **`x-edge-detailed-result-type`**

Questo campo contiene lo stesso valore del campo `x-edge-result-type`, tranne nei seguenti casi:

- Quando l'oggetto è stato servito al visualizzatore dal livello Origin Shield, questo campo contiene `OriginShieldHit`.
- Quando l'oggetto non era nella CloudFront cache e la risposta è stata generata da una funzione Lambda @Edge di richiesta di origine, questo campo contiene. `MissGeneratedResponse`
- Quando il valore del campo `x-edge-result-type` è `Error`, questo campo contiene uno dei seguenti valori con ulteriori informazioni sull'errore:
  - `AbortedOrigin` – Il server ha riscontrato un problema con l'origine.
  - `ClientCommError` – La risposta al visualizzatore è stata interrotta a causa di un problema di comunicazione tra il server edge e il visualizzatore.
  - `ClientGeoBlocked`: la distribuzione è configurata per rifiutare le richieste dalla posizione geografica del visualizzatore.
  - `ClientHungUpRequest` — Il visualizzatore si è arrestato prematuramente durante l'invio della richiesta.

- `Error`: si è verificato un errore per il quale il tipo di errore non si adatta a nessuna delle altre categorie. Questo tipo di errore può verificarsi quando il server edge serve una risposta di errore dalla cache.
- `InvalidRequest` – Il server ha ricevuto una richiesta non valida dal visualizzatore.
- `InvalidRequestBlocked` — L'accesso alla risorsa richiesta è bloccato.
- `InvalidRequestCertificate`— La distribuzione non corrisponde al SSL/TLS certificato per il quale è stata stabilita la connessione HTTPS.
- `InvalidRequestHeader` —-La richiesta conteneva un'intestazione non valida.
- `InvalidRequestMethod` — La distribuzione non è configurata per gestire il metodo di richiesta HTTP utilizzato. Questo può accadere quando la distribuzione supporta solo le richieste memorizzabili nella cache.
- `OriginCommError` - La richiesta è scaduta durante la connessione a un'origine o durante la lettura di dati da un'origine.
- `OriginConnectError`: il server non è riuscito a connettersi all'origine.
- `OriginContentRangeLengthError`: l'intestazione `Content-Length` nella risposta dell'origine non corrisponde alla lunghezza dell'intestazione `Content-Range`.
- `OriginDnsError`: il server non è riuscito a risolvere il nome di dominio dell'origine.
- `OriginError` — L'origine ha restituito una risposta errata.
- `OriginHeaderTooBigError` - Un'intestazione restituita dall'origine è troppo grande per essere elaborata dal server edge.
- `OriginInvalidResponseError` — L'origine ha restituito una risposta non valida.
- `OriginReadError`: il server non è in grado di leggere dall'origine.
- `OriginWriteError`: il server non è in grado di scrivere sull'origine.
- `OriginZeroSizeObjectError` — Un oggetto di dimensione zero inviato dall'origine ha generato un errore.
- `SlowReaderOriginError` — Il visualizzatore ha letto lentamente il messaggio che ha causato l'errore di origine.

35. **`c-country`**

Codice paese che rappresenta la posizione geografica del visualizzatore, determinata dal relativo indirizzo IP. Per un elenco dei codici paese, vedere ISO 3166-1 alpha-2.

36. **`cs-accept-encoding`**

Il valore dell'intestazione `Accept-Encoding` nella richiesta del visualizzatore.

37. **`cs-accept`**

    Il valore dell'intestazione `Accept` nella richiesta del visualizzatore.

38. **`cache-behavior-path-pattern`**

    Il modello di percorso che identifica il comportamento della cache corrispondente alla richiesta del visualizzatore.

39. **`cs-headers`**

    Le intestazioni HTTP (nomi e valori) nella richiesta del visualizzatore.

    > **Note**
    >
    > Questo campo viene troncato a 800 byte.

40. **`cs-header-names`**

    I nomi delle intestazioni HTTP (non dei valori) nella richiesta del visualizzatore.

    > **Note**
    >
    > Questo campo viene troncato a 800 byte.

41. **`cs-headers-count`**

    Il numero di intestazioni HTTP nella richiesta del visualizzatore.

42. **`primary-distribution-id`**

    Quando è abilitata l'implementazione continua, questo ID identifica quale distribuzione è quella primaria nella distribuzione corrente.

43. **`primary-distribution-dns-name`**

    Quando la distribuzione continua è abilitata, questo valore mostra il nome di dominio primario correlato alla CloudFront distribuzione corrente (ad esempio, d111111abcdef8.cloudfront.net).

44. **`origin-fbl`**

    Il numero di secondi di latenza del primo byte tra e l'origine. CloudFront

45. **`origin-lbl`**

    Il numero di secondi di latenza dell'ultimo byte tra e l'origine. CloudFront

46. **`asn`**

    Il numero di sistema autonomo (ASN) del visualizzatore.

47.

    > **Campi CMCD nei log di accesso in tempo reale**
    >
    > Per ulteriori informazioni su questi campi, consulta il documento CTA Specification Web Application Video Ecosystem - Common Media Client Data CTA-5004.

48. **`cmcd-encoded-bitrate`**

    Il bitrate codificato dell'oggetto audio o video richiesto.

49. **`cmcd-buffer-length`**

    La lunghezza del buffer dell'oggetto multimediale richiesto.

50. **`cmcd-buffer-starvation`**

    Se il buffer è stato esaurito in un momento compreso tra la richiesta precedente e la richiesta dell'oggetto. Ciò può causare una situazione di rebuffering del lettore, che può bloccare la riproduzione video o audio.

51. **`cmcd-content-id`**

    Una stringa univoca che identifica il contenuto corrente.

52. **`cmcd-object-duration`**

    La durata di riproduzione dell'oggetto richiesto (in millisecondi).

53. **`cmcd-deadline`**

    Il termine ultimo dal momento della richiesta entro il quale deve essere disponibile il primo campione di questo oggetto, in modo da evitare uno stato di buffer underrun o altri problemi di riproduzione.

54. **`cmcd-measured-throughput`**

    Il throughput tra client e server, come misurato dal client.

55. **`cmcd-next-object-request`**

Il percorso relativo dell'oggetto successivo richiesto.

56. **`cmcd-next-range-request`**

    Se la richiesta successiva è una richiesta di oggetto parziale, questa stringa indica l'intervallo di byte da richiedere.

57. **`cmcd-object-type`**

    Il tipo di supporto dell'oggetto corrente richiesto.

58. **`cmcd-playback-rate`**

    1 se in tempo reale, 2 se a doppia velocità, 0 se non in riproduzione.

59. **`cmcd-requested-maximum-throughput`**

    Il throughput massimo richiesto che il client ritiene sufficiente per la consegna degli asset.

60. **`cmcd-streaming-format`**

    Il formato di streaming che definisce la richiesta corrente.

61. **`cmcd-session-id`**

    Un GUID che identifica la sessione di riproduzione corrente.

62. **`cmcd-stream-type`**

    Token che identifica la disponibilità del segmento. `v` = tutti i segmenti sono disponibili. `l` = i segmenti diventano disponibili nel tempo.

63. **`cmcd-startup`**

    La chiave è inclusa senza un valore se l'oggetto è necessario con urgenza durante lo startup, la ricerca o il ripristino dopo un evento di buffer vuoto.

64. **`cmcd-top-bitrate`**

    La resa con il bitrate più elevato che il client è in grado di riprodurre.

65. **`cmcd-version`**

    La versione di questa specifica utilizzata per interpretare i nomi e i valori delle chiavi definiti. Se questa chiave viene omessa, il client e il server devono interpretare i valori come definiti dalla versione 1.

66. **`r-host`**

Questo campo viene inviato per le richieste di origine e indica il dominio del server di origine utilizzato per servire l'oggetto. In caso di errori, puoi utilizzare questo campo per trovare l'ultima origine tentata, ad esempio: *cd8jhdejh6a*`.mediapackagev2.us-east-1.amazonaws.com`.

67 **`sr-reason`**

Questo campo fornisce il motivo per cui è stata selezionata l'origine. È vuoto quando una richiesta all'origine primaria ha esito positivo.

Se si verifica un failover dell'origine, il campo conterrà il codice di errore HTTP che ha causato il failover, ad esempio `Failover:403` o `Failover:502`. In caso di failover dell'origine, se anche il nuovo tentativo di richiesta non va a buon fine e non sono state configurate pagine di errore personalizzate, `r-status` indica la risposta della seconda origine. Tuttavia, se sono state configurate pagine di errore personalizzate insieme al failover dell'origine, questa conterrà la risposta della seconda origine se la richiesta non è andata a buon fine ed è stata restituita una pagina di errore personalizzata.

Se non si verifica alcun failover dell'origine ma viene effettuata una selezione dell'origine basata sulla resilienza sensibile alla qualità multimediale (MQAR), ciò verrà registrato come `MediaQuality`. Per ulteriori informazioni, consulta MQAR (Media Quality-Aware Resiliency).

68 **`x-edge-mqcs`**

Questo campo indica il Media Quality Confidence Score (MQCS) (intervallo: 0 - 100) per i segmenti multimediali CloudFront recuperati nelle intestazioni di risposta CMSD dalla v2. MediaPackage Questo campo è disponibile per le richieste che corrispondono a un comportamento della cache con un gruppo di origine abilitato per MQAR. CloudFront registra questo campo per i segmenti multimediali che vengono serviti anche dalla sua cache oltre alle richieste di origine. Per ulteriori informazioni, consulta MQAR (Media Quality-Aware Resiliency).

69 **`distribution-tenant-id`**

L'ID del tenant di distribuzione.

70 **`connection-id`**

Un identificatore univoco per la connessione TLS.

È necessario abilitare MTL per le distribuzioni prima di poter ottenere informazioni per questo campo. Per ulteriori informazioni, consulta Visualizzatore TLS reciproco (mTLS).

Endpoint (flusso di dati Kinesis)

L'endpoint contiene informazioni sul flusso di dati Kinesis a cui si desidera inviare log in tempo reale. Fornisci il Amazon Resource Name (ARN) del flusso di dati.

Per ulteriori informazioni sulla creazione di flussi di dati Kinesis, consulta i seguenti argomenti nella Guida per gli sviluppatori di Flusso di dati Amazon Kinesis.

- Creazione e gestione dei flussi
- Esegui le operazioni di base di Kinesis Data Streams utilizzando il AWS CLI
- Creazione di uno stream (utilizza il) AWS SDK per Java

Quando si crea un flusso di dati, è necessario specificare il numero di partizioni. Utilizzare le seguenti informazioni per stimare il numero di frammenti necessari.

Per stimare il numero di frammenti per il flusso di dati Kinesis

1. Calcola (o stima) il numero di richieste al secondo ricevute dalla distribuzione CloudFront.

   Puoi utilizzare i report CloudFront sull'utilizzo (nella CloudFront console) e le CloudFront metriche (nelle CloudWatch console CloudFront e Amazon) per aiutarti a calcolare le tue richieste al secondo.
2. Determina la dimensione tipica di un singolo record di registro degli accessi in tempo reale.

   In generale, un singolo record di log è di circa 500 byte. Un record di grandi dimensioni che include tutti i campi disponibili è generalmente di circa 1 KB.

   Se non sei sicuro di quale sia la dimensione del record di log, puoi abilitare i log in tempo reale con una bassa frequenza di campionamento (ad esempio, 1%), quindi calcolare la dimensione media del record utilizzando i dati di monitoraggio nei flussi di dati Kinesis (numero totale di byte in ingresso diviso per il numero totale di record).
3. Nella pagina dei prezzi di Amazon Kinesis Data Streams Calcolatore dei prezzi AWS, sotto, scegli Crea subito il tuo preventivo personalizzato.

   - Nella calcolatrice, inserisci il numero di richieste (record) al secondo.
   - Immetti la dimensione media dei record di un singolo record di log.
   - Scegli Mostra calcoli.

Il calcolatore dei prezzi mostra il numero di shard necessari e il costo stimato.

Ruolo IAM

Il ruolo AWS Identity and Access Management (IAM) che consente di CloudFront fornire log di accesso in tempo reale al flusso di dati Kinesis.

Quando crei una configurazione del log di accesso in tempo reale con la CloudFront console, puoi scegliere Crea nuovo ruolo di servizio per consentire alla console di creare il ruolo IAM per te.

Quando crei una configurazione del log di accesso in tempo reale con AWS CloudFormation o l' CloudFront API (AWS CLI o SDK), devi creare tu stesso il ruolo IAM e fornire il ruolo ARN. Per creare autonomamente un ruolo IAM, utilizzare le seguenti policy.

Policy di attendibilità del ruolo IAM

Per utilizzare la seguente policy di fiducia dei ruoli IAM, sostituiscila *111122223333* con il tuo Account AWS numero. L'`Condition`elemento di questa policy aiuta a prevenire il confuso problema del vicesceriffo, in quanto CloudFront può assumere questo ruolo solo per conto di una distribuzione del proprio territorio Account AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
```

```
}
```

Policy di autorizzazioni del ruolo IAM per un flusso di dati non crittografato

Per utilizzare la seguente politica, sostituiscila *arn:aws:kinesis:us-east-2:123456789012:stream/StreamName* con l'ARN del flusso di dati Kinesis.

JSON

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

Policy di autorizzazioni del ruolo IAM per un flusso di dati crittografato

Per utilizzare la seguente policy, sostituiscila *arn:aws:kinesis:us-east-2:123456789012:stream/StreamName* con l'ARN del tuo flusso di dati Kinesis e con *arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-ae03cc73d486* l'ARN del tuo. AWS KMS key

JSON

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

Creazione di un consumer Flussi di dati Kinesis

Per leggere e analizzare i log di accesso in tempo reale, devi creare o utilizzare un consumer Kinesis Data Streams. Quando crei un utente per i log CloudFront in tempo reale, è importante sapere che i campi di ogni record di log di accesso in tempo reale vengono sempre consegnati nello stesso ordine, come indicato nella sezione. Campi Assicurati di creare il tuo consumatore per soddisfare questo ordine fisso.

Ad esempio, si consideri una configurazione dei log di accesso in tempo reale che includa solo questi tre campi: `time-to-first-byte`sc-status, `c-country`. In questo scenario, l'ultimo campo, `c-country`, è sempre il numero di campo 3 in ogni record di registro. Tuttavia, se in un secondo momento si aggiungono campi alla configurazione del registro degli accessi in tempo reale, la posizione di ogni campo in un record può cambiare.

Ad esempio, se si aggiungono i campi `sc-bytes` e `time-taken` alla configurazione del registro degli accessi in tempo reale, questi campi vengono inseriti in ogni record di registro secondo l'ordine mostrato nella Campi sezione. L'ordine risultante di tutti e cinque i campi è `time-to-first-byte`, `sc-status`, `sc-bytes`, `time-taken` e `c-country`. Il campo `c-country` era originariamente il numero 3, ma ora è il campo numero 5. Assicurati che la tua applicazione consumer sia in grado di gestire i campi che cambiano posizione in un record di registro, nel caso in cui aggiungi campi alla configurazione del registro di accesso in tempo reale.

Risolvi i problemi relativi ai log di accesso in tempo reale

Dopo aver creato una configurazione del registro di accesso in tempo reale, potresti scoprire che nessun record (o non tutti i record) viene consegnato a Kinesis Data Streams. In questo caso, è necessario prima verificare che la distribuzione CloudFront stia ricevendo richieste di visualizzatore. In tal caso, è possibile controllare le seguenti impostazioni per continuare la risoluzione dei problemi.

Autorizzazioni del ruolo IAM

Per fornire record di log di accesso in tempo reale al flusso di dati Kinesis, CloudFront utilizza il ruolo IAM nella configurazione dei log di accesso in tempo reale. Assicurarsi che la policy di attendibilità del ruolo e la policy delle autorizzazioni del ruolo corrispondano alle policy mostrate in Ruolo IAM.

Throttling di Kinesis Data Streams

Se CloudFront scrive i record dei log di accesso in tempo reale sul flusso di dati Kinesis più velocemente di quanto il flusso sia in grado di gestire, Kinesis Data Streams potrebbe limitare le richieste da. CloudFront In questo caso, è possibile aumentare il numero di frammenti nel flusso di dati Kinesis. Ogni shard può supportare scritture fino a 1.000 record al secondo, fino a un massimo di 1 MB al secondo in scrittura dei dati.

Registri delle funzioni Edge

Puoi usare Amazon CloudWatch Logs per ottenere i log delle tue funzioni edge, sia Lambda @Edge che Functions. CloudFront Puoi accedere ai log utilizzando la CloudWatch console o l'API Logs. CloudWatch

> **Important**
>
> Ti consigliamo di utilizzare i log per comprendere la natura delle richieste relative ai tuoi contenuti, non come contabilità completa di tutte le richieste. CloudFront fornisce i registri

delle funzioni Edge con la massima diligenza possibile. È possibile che la voce di log per una specifica richiesta venga distribuita molto tempo dopo l'elaborazione effettiva della richiesta e, in rari casi, che non venga distribuita affatto. Quando una voce di log viene omessa dai log delle funzioni edge, il numero di voci nei log delle funzioni edge non corrisponderà all'utilizzo visualizzato nei report di utilizzo e fatturazione di AWS .

Argomenti

Registri di Lambda@Edge

Lambda @Edge invia automaticamente i log delle funzioni ai CloudWatch registri, creando flussi di log nel punto in Regioni AWS cui vengono richiamate le funzioni. Quando crei o modifichi una funzione in AWS Lambda, puoi utilizzare il nome del gruppo di CloudWatch log predefinito o personalizzarlo.

- Il nome predefinito del gruppo di log è `/aws/lambda/<FunctionName>`, dove *`<FunctionName>`* è il nome specificato al momento della creazione della funzione. Quando si inviano i log a CloudWatch, Lambda @Edge aggiungerà automaticamente `us-east-1` il prefisso al nome della funzione, in modo che il nome del gruppo di log sia. `/aws/lambda/us-east-1.<FunctionName>` Questo prefisso corrisponde al luogo in Regione AWS cui è stata creata la funzione. Questo prefisso rimane parte del nome del gruppo di log, anche in altre regioni in cui viene invocata la funzione.
- Se si specifica un nome di gruppo di log personalizzato, come */MyLogGroup*, Lambda@Edge non aggiungerà il prefisso Regione. Il nome del gruppo di log rimane lo stesso in tutte le altre regioni in cui viene invocata la funzione.

> **Note**
>
> Se si crea un gruppo di log personalizzato e si specifica lo stesso nome di quello predefinito `/aws/lambda/<FunctionName>`, Lambda@Edge aggiunge il prefisso `us-east-1` al nome della funzione.

Oltre alla personalizzazione del nome del gruppo di log, le funzioni Lambda@Edge supportano i formati di log JSON e testo normale e il filtraggio a livello di log. Per ulteriori informazioni, consulta Configurazione dei controlli di registrazione di log avanzati per la funzione Lambda nella Guida per gli sviluppatori di AWS Lambda .

> **Note**
>
> Lambda@Edge sottopone a throttling i log in base al volume di richieste e alla dimensione dei log.

È necessario esaminare i file di CloudWatch registro nella regione corretta per visualizzare i file di registro delle funzioni Lambda @Edge. Per vedere le regioni in cui è in esecuzione la funzione Lambda @Edge, visualizza i grafici delle metriche per la funzione nella console. CloudFront I parametri vengono visualizzati per ogni regione . Nella stessa pagina, puoi scegliere una regione e quindi visualizzare i file di registro per tale regione, in modo da analizzare i problemi.

Per ulteriori informazioni su come utilizzare CloudWatch i log con le funzioni Lambda @Edge, consulta i seguenti argomenti:

- Per ulteriori informazioni sulla visualizzazione dei grafici nella sezione Monitoraggio della CloudFront console, consulta. the section called “Monitoraggio delle metriche CloudFront con Amazon CloudWatch”
- Per informazioni sulle autorizzazioni necessarie per inviare dati ai CloudWatch registri, vedere. the section called “Configurazione di autorizzazioni e ruoli IAM”
- Per informazioni sull'aggiunta della registrazione a una funzione Lambda@Edge, consulta Registrazione della funzione AWS Lambda in Node.js o Registrazione della funzione AWS Lambda in Python nella Guida per gli sviluppatori di AWS Lambda .
- Per informazioni sulle quote di CloudWatch Logs (precedentemente note come limiti), consulta Logs CloudWatch quotas nella Amazon Logs User Guide. CloudWatch

CloudFront Registri delle funzioni

Se il codice di una CloudFront funzione contiene `console.log()` istruzioni, CloudFront Functions invia automaticamente queste righe di registro a CloudWatch Logs. Se non ci sono `console.log()` istruzioni, non viene inviato nulla a CloudWatch Logs.

CloudFront Functions crea sempre flussi di log nella regione () degli Stati Uniti orientali (Virginia settentrionaleus-east-1), indipendentemente dalla posizione periferica in cui è stata eseguita la funzione. Il nome del flusso di log è nel formato YYYY/M/D/*UUID*.

Il nome del gruppo di log utilizza il seguente formato:

- Per CloudFront le funzioni a livello di comportamento della cache, il formato è `/aws/cloudfront/function/<FunctionName>`
- Per CloudFront le funzioni a livello di distribuzione (Funzioni di connessione), il formato è `/aws/cloudfront/connection-function/<FunctionName>`

*<FunctionName>*è il nome che hai dato alla funzione quando l'hai creata.

Example Richieste del visualizzatore

Di seguito viene illustrato un esempio di messaggio di registro inviato a CloudWatch Logs. Ogni riga inizia con un ID che identifica in modo univoco una richiesta. CloudFront Il messaggio inizia con una START riga che include l'ID di CloudFront distribuzione e termina con una END riga. Tra le righe START e END vi sono le righe di log generate dalle istruzioni `console.log()` nella funzione.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADAXZZ
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== Example function log output
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

Example Richieste di connessione

Di seguito viene illustrato un esempio di messaggio di registro inviato a CloudWatch Logs. Ogni riga inizia con un ID che identifica in modo univoco una richiesta. CloudFront Il messaggio inizia con una START riga che include l'ID di CloudFront distribuzione e termina con una END riga. Tra le righe START e END vi sono le righe di log generate dalle istruzioni `console.log()` nella funzione.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADA123
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== 1.2.3.4
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

> **Note**
>
> CloudFront Functions invia i log CloudWatch solo per le funzioni nella `LIVE` fase in cui viene eseguita in risposta alle richieste e alle risposte di produzione. Quando testate una funzione, CloudFront non invia alcun registro a. CloudWatch L'output del test contiene informazioni sugli errori, sull'utilizzo del calcolo e sui registri delle funzioni (`console.log()`istruzioni), ma queste informazioni non vengono inviate a. CloudWatch

CloudFront Functions utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) per inviare i log ai registri del tuo account. CloudWatch Un ruolo collegato ai servizi è un tipo univoco di ruolo IAM collegato direttamente a un Servizio AWS. I ruoli collegati al servizio sono predefiniti dal servizio e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti. Servizi AWS CloudFront Functions utilizza il ruolo collegato al servizio. AWSServiceRoleForCloudFrontLogger Per ulteriori informazioni su questo ruolo, consulta the section called “Ruoli collegati ai servizi per Lambda@Edge” (Lambda@Edge utilizza lo stesso ruolo collegato al servizio).

Quando una funzione fallisce a causa di un errore di convalida o di esecuzione, le informazioni vengono registrate nei log standard e nei log di accesso in tempo reale. Per informazioni specifiche sull’errore, consulta i campi `x-edge-result-type`, `x-edge-response-result-type` e `x-edge-detailed-result-type`.

Registrazione di log delle chiamate API Amazon CloudFront utilizzando AWS CloudTrail

CloudFront si integra con AWS CloudTrail, un servizio che offre un record delle azioni eseguite da un utente, un ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API per CloudFront come eventi. Le chiamate acquisite includono le chiamate dalla console CloudFront e le chiamate di codice alle operazioni API CloudFront. Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata a CloudFront, l’indirizzo IP da cui è partita la richiesta, il momento in cui è stata eseguita e altri dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo Account AWS quando create l'account e hai automaticamente accesso alla cronologia degli eventi di CloudTrail. La cronologia degli eventi di CloudTrail fornisce una registrazione visualizzabile, ricercabile, scaricabile e immutabile degli eventi di gestione verificatisi negli ultimi 90 giorni in una Regione AWS. Per ulteriori informazioni, consulta Working with CloudTrail Event history nella Guida per l'utente di AWS CloudTrail. Non sono previsti costi CloudTrail per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi nell'Account AWS oltre i 90 giorni, creare un trail o un datastore di eventi Data Lake CloudTrail.

Trail CloudTrail

Un trail abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Tutti i trail creati utilizzando la Console di gestione AWS sono multi-regione. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. Si consiglia di creare un trail per più Regioni in quanto consente di acquisire l'attività in tutte le Regioni AWS dell'account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail.

Puoi fornire gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 da CloudTrail creando un percorso, tuttavia dovranno essere considerati i costi di archiviazione di Amazon S3. Per maggiori informazioni sui prezzi di CloudTrail, consultare Prezzi di AWS CloudTrail. Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

Datastore di eventi CloudTrail Lake

Data Lake CloudTrail consente di eseguire query SQL sugli eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su Data Lake CloudTrail, consulta Working with AWS CloudTrail Lake nella Guida per l'utente di AWS CloudTrail.

I datastore di eventi e le query di Data Lake CloudTrail comportano costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per maggiori informazioni sui prezzi di CloudTrail, consultare Prezzi di AWS CloudTrail.

> **Note**
>
> CloudFront è un servizio globale. CloudTrail registra eventi per CloudFront nella regione Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni, consulta Eventi dei servizi globali nella Guida per l'utente di AWS CloudTrail.
> Se utilizzi credenziali di sicurezza temporanee utilizzando AWS Security Token Service, le chiamate agli endpoint regionali, ad esempio `us-west-2`, vengono registrate in CloudTrail nella Regione appropriata.
> Per ulteriori informazioni sugli endpoint CloudFront, consulta Endpoint e quote CloudFront nella Riferimenti generali di AWS.

Eventi di dati CloudFront in CloudTrail

Gli eventi di dati forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su una distribuzione CloudFront). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi di dati. La cronologia degli eventi di CloudTrail non registra gli eventi di dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per maggiori informazioni sui prezzi di CloudTrail, consultare Prezzi di AWS CloudTrail.

Puoi registrare gli eventi di dati per il tipo di risorse CloudFront utilizzando la console CloudTrail, AWS CLI o le operazioni API CloudTrail. Per maggiori informazioni su come registrare i log degli eventi di dati, consultare Registrazione di eventi di dati con Console di gestione AWS e Registrazione di eventi di dati con AWS Command Line Interface nella Guida per l'utente di AWS CloudTrail.

La tabella seguente elenca i tipi di risorse CloudFront per i quali è possibile registrare eventi di dati. La colonna Tipo di evento dati (console) mostra il valore da scegli dall'elenco Tipo di evento dati sulla console di CloudTrail. La colonna resources.type value mostra il valore `resources.type`, da specificare quando si configurano selettori di eventi avanzati utilizzando le API AWS CLI o CloudTrail.

La colonna Dati API registrati su CloudTrail mostra le chiamate API registrate su CloudTrail per il tipo di risorsa.

Tipo di evento di dati (console)	Valore resources.type	API sui dati registrate in CloudTrail
KeyValueStore CloudFront	`AWS::CloudFront::KeyValueStore`	• DeleteKeys • DescribeKeyValueStore • GetKey • ListKeys • PutKeys • UpdateKeys

È possibile configurare selettori di eventi avanzati per filtrare i campi `eventName`, `readOnly` e `resources.ARN` per registrare solo gli eventi importanti per l'utente. Per ulteriori informazioni su questi campi, consulta AdvancedFieldSelector in Riferimento API AWS CloudTrail.

Eventi di gestione di CloudFront in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse nell'Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon CloudFront registra tutte le operazioni del piano di controllo (control-plane) CloudFront come eventi di gestione. Per un elenco delle operazioni del piano di controllo (control-plane) di Amazon CloudFront registrate da CloudFront in CloudTrail, consulta Documentazione di riferimento delle API di Amazon CloudFront.

Esempi di eventi CloudFront

Un evento rappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono uno stack trace ordinato delle chiamate API pubbliche, quindi gli eventi non appaiono in un ordine specifico.

Indice

- Ad esempio: UpdateKeys

Ad esempio: UpdateDistribution

L'esempio seguente mostra un evento CloudTrail che illustra l'operazione UpdateDistribution.

Per le chiamate all'API CloudFront, `eventSource` è `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"
}
```

Ad esempio: UpdateKeys

L'esempio seguente mostra un evento CloudTrail che illustra l'operazione UpdateKeys.

Per le chiamate all'API KeyValueStore di CloudFront, `eventSource` è `edgekeyvaluestore.amazonaws.com` invece di `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"
    }
}
```


Per informazioni sui contenuti delle registrazioni CloudTrail, consulta i contenuti delle registrazioni CloudTrail nella Guida per l'utente AWS CloudTrail.

Tieni traccia delle modifiche alla configurazione con AWS Config

Per registrare e valutare le configurazioni delle AWS risorse, è possibile utilizzare AWS Config, che fornisce una visualizzazione dettagliata della configurazione delle distribuzioni. Ciò include il modo in cui le risorse sono correlate tra loro e come sono state configurate in passato, in modo da poter esaminare le modifiche apportate nel tempo.

È inoltre possibile utilizzare AWS Config per registrare le modifiche alla configurazione delle impostazioni di CloudFront distribuzione. Puoi acquisire le modifiche agli stati della distribuzione, alle classi di prezzo, alle origini, alle impostazioni di restrizione geografica e alle configurazioni Lambda@Edge.

> **Note**
>
> AWS Config non registra tag chiave-valore per le distribuzioni CloudFront in streaming.

Indice

Configura con AWS Config CloudFront

Durante la configurazione AWS Config, puoi scegliere di registrare tutte le AWS risorse supportate o registrare solo alcune risorse specifiche, ad esempio registrando le modifiche CloudFront solo per. Per un elenco delle CloudFront risorse supportate, consulta la CloudFront sezione Amazon dell'argomento Supported Resource Types nella AWS Config Developer Guide.

> **Note**
>
> - Per tenere traccia delle modifiche alla configurazione CloudFront della tua distribuzione, devi accedere alla CloudFront console negli Stati Uniti orientali (Virginia settentrionale) Regione AWS.
> - Potrebbe verificarsi un ritardo nella registrazione delle risorse con AWS Config. AWS Config registra le risorse solo dopo averle scoperte.

Console

Per configurare con AWS Config CloudFront

1. Accedi a Console di gestione AWS e apri la AWS Config console.
2. Scegliere Get Started Now (Inizia subito).
3. Nella pagina Impostazioni, per i tipi di risorse da registrare, specifica i tipi di AWS risorse che desideri AWS Config registrare. Se desideri registrare solo le CloudFront modifiche, scegli Tipi specifici e quindi, in, in CloudFront, scegli la distribuzione o la distribuzione in streaming di cui desideri tenere traccia delle modifiche.

Per aggiungere o modificare le distribuzioni da monitorare, scegli Impostazioni a sinistra, dopo aver completato la configurazione iniziale.

4. Specificate le opzioni aggiuntive richieste per AWS Config: impostare una notifica, specificare una posizione per le informazioni di configurazione e aggiungere regole per la valutazione dei tipi di risorse.

Per ulteriori informazioni, consulta Configurazione AWS Config con la console nella Guida per gli AWS Config sviluppatori.

AWS CLI

Per configurare AWS Config l' CloudFront utilizzo di AWS CLI, consulta Configurazione AWS Config con la AWS CLI nella Guida per gli AWS Config sviluppatori.

AWS Config API

Per configurare AWS Config l' CloudFront utilizzo dell' AWS Config API, consulta il funzionamento dell' StartConfigurationRecorderAPI nell'AWS Config API Reference.

Visualizza la cronologia CloudFront delle configurazioni

Dopo aver AWS Config iniziato a registrare le modifiche alla configurazione delle distribuzioni, è possibile ottenere la cronologia di configurazione di qualsiasi distribuzione per CloudFront cui è stata configurata.

Puoi visualizzare le cronologie di configurazione in uno dei seguenti modi:

Console

Per ogni risorsa registrata, puoi visualizzare una pagina della timeline, che fornisce una cronologia dei dettagli di configurazione. Per visualizzare questa pagina, scegli l'icona grigia nella colonna Timeline configurazione della pagina Host dedicati.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli di configurazione nella AWS Config console nella Guida per gli AWS Config sviluppatori.

AWS CLI

Per ottenere un elenco di tutte le distribuzioni, esegui il list-discovered-resourcescomando, come illustrato nell'esempio seguente.

```
aws configservice list-discovered-resources --resource-type
 AWS::CloudFront::Distribution
```

Per ottenere i dettagli di configurazione di una distribuzione per un intervallo di tempo specifico, esegui il get-resource-config-historycomando.

Per ulteriori informazioni, consulta l'argomento relativo alla visualizzazione dei dettagli di configurazione mediante la CLI nella Guida per lo sviluppatore di AWS Config .

AWS Config API

Per ottenere un elenco di tutte le tue distribuzioni, usa l'operazione ListDiscoveredResourcesAPI.

Per ottenere i dettagli di configurazione di una distribuzione per un intervallo di tempo specifico, utilizza l'operazione GetResourceConfigHistoryAPI. Per ulteriori informazioni, consulta la documentazione di riferimento dell'API di AWS Config.

Valuta le CloudFront configurazioni con Rules AWS Config

È possibile valutare le configurazioni rispetto alle configurazioni desiderate con Rules. AWS Config Ad esempio, AWS Config Rules consente di valutare se le CloudFront risorse sono conformi alle migliori pratiche di sicurezza comuni. Puoi scegliere regole gestite come la policy del visualizzatore HTTPS, SNI abilitata, OAC abilitata, Origin Failover abilitata, WebACL AWS WAF o le policy AWS Shield Advanced delle risorse da attivare quando la configurazione cambia.

Le regole gestite possono eseguire valutazioni periodicamente, con una frequenza scelta dall'utente. AWS Firewall Manager si affida agli AWS Config avvisi e alle correzioni automatici. Per ulteriori informazioni, consulta Evaluating Resources with AWS Config Rules e List of AWS Config Managed Rules nella Guida per gli sviluppatori.AWS Config

Sicurezza in Amazon CloudFront

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

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per maggiori informazioni sui programmi di conformità applicabili ad Amazon CloudFront, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo CloudFront. I seguenti argomenti mostrano come eseguire la configurazione CloudFront per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere CloudFront le tue risorse.

Argomenti

Protezione dei dati in Amazon CloudFront

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in Amazon CloudFront. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura

globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

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

Amazon CloudFront offre diverse opzioni che puoi utilizzare per proteggere i contenuti che distribuisce:

- Configurazione connessioni HTTPS.
- Configurare la crittografia a livello di campo per fornire una protezione aggiuntiva per dati specifici durante il transito.
- Restrizione dell'accesso ai contenuti in modo che solo determinate persone o persone in un'area specifica siano in grado di visualizzarli.

I seguenti argomenti spiegano le opzioni nel dettaglio.

Argomenti

Crittografia dei dati in transito

Per crittografare i dati durante il transito, configuri Amazon in modo che richieda CloudFront agli utenti di utilizzare HTTPS per richiedere i tuoi file, in modo che le connessioni siano crittografate quando CloudFront comunicano con gli spettatori. Puoi anche configurare l'utilizzo CloudFront di HTTPS per recuperare i file dall'origine, in modo che le connessioni siano crittografate quando CloudFront comunicano con l'origine.

Per ulteriori informazioni, consulta Usa HTTPS con CloudFront.

La crittografia a livello di campo aggiunge un ulteriore livello di sicurezza che, insieme a HTTPS, ti consente di proteggere dati specifici durante l'elaborazione del sistema, di modo che solo alcune applicazioni possano vederli. Configurando la crittografia a livello di campo in CloudFront, puoi caricare in modo sicuro le informazioni sensibili inviate dall'utente sui tuoi server web. Le informazioni sensibili fornite dai tuoi client sono crittografate nella edge location più vicina all'utente e rimangono tali durante l'intero stack di applicazioni. In questo modo, possono essere decrittate solo dalle applicazioni che hanno bisogno di quei dati e che dispongono delle credenziali per farlo.

Per ulteriori informazioni, consulta Utilizzo della crittografia a livello di campo per la protezione dei dati sensibili.

Gli endpoint dell' CloudFront API `cloudfront.amazonaws.com` e `cloudfront-fips.amazonaws.com` accettano solo traffico HTTPS. Ciò significa che quando invii e ricevi

informazioni utilizzando l' CloudFront API, i tuoi dati, incluse le configurazioni di distribuzione, le politiche di cache e le politiche di richiesta di origine, i gruppi di chiavi e le chiavi pubbliche e il codice CloudFront funzionale in Functions, vengono sempre crittografati in transito. Inoltre, tutte le richieste inviate agli endpoint dell' CloudFront API vengono firmate con credenziali e registrate. AWS AWS CloudTrail

Il codice e la configurazione della funzione in CloudFront Functions sono sempre crittografati in transito quando vengono copiati nei punti di presenza di edge location (POPs) e tra altre posizioni di archiviazione utilizzate da. CloudFront

Crittografia dei dati a riposo

Il codice e la configurazione CloudFront delle funzioni in Functions vengono sempre archiviati in un formato crittografato nell'edge location POPs e in altre posizioni di archiviazione utilizzate da CloudFront.

Limitazione dell'accesso ai contenuti

Molte aziende che distribuiscono contenuti tramite Internet vogliono limitare l'accesso a documenti, dati aziendali, flussi multimediali o contenuti destinati a un subset di utenti. Per distribuire questi contenuti in modo sicuro utilizzando Amazon CloudFront, puoi eseguire una o più delle seguenti operazioni:

Utilizza cookie firmati URLs o

> Puoi limitare l'accesso ai contenuti destinati a utenti selezionati, ad esempio utenti che hanno pagato una tariffa, pubblicando questi contenuti privati tramite CloudFront cookie firmati o firmati. URLs Per ulteriori informazioni, consulta Offri contenuti privati con cookie firmati URLs e firmati.

Limitare l'accesso ai contenuti nei bucket Amazon S3

> Se limiti l'accesso ai tuoi contenuti utilizzando, ad esempio, cookie CloudFront firmati URLs o firmati, non vuoi nemmeno che le persone visualizzino i file utilizzando l'URL diretto del file. Invece, vuoi che accedano ai file solo utilizzando l'URL CloudFront , in modo che le protezioni funzionino.
>
> Se utilizzi un bucket Amazon S3 come origine per una CloudFront distribuzione, puoi configurare un controllo di accesso all'origine (OAC) che consente di limitare l'accesso al bucket S3. Per ulteriori informazioni, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

Limitare l'accesso al contenuto gestito da un Application Load Balancer

Quando si utilizza CloudFront un Application Load Balancer in ELB come origine, è possibile configurare in modo da impedire CloudFront agli utenti di accedere direttamente all'Application Load Balancer. Ciò consente agli utenti di accedere all'Application Load Balancer solo tramite CloudFront, assicurandoti di ottenere i vantaggi dell'utilizzo. CloudFront Per ulteriori informazioni, consulta Limitazione dell’accesso ad Application Load Balancer.

Usa il web AWS WAF ACLs

È possibile utilizzare AWS WAF un servizio firewall per applicazioni Web per creare una lista di controllo degli accessi Web (Web ACL) per limitare l'accesso ai contenuti. In base a condizioni specificate, come gli indirizzi IP da cui provengono le richieste o i valori delle stringhe di query, CloudFront risponde alle richieste con il contenuto richiesto o con un codice di stato HTTP 403 (Proibito). Per ulteriori informazioni, consulta Utilizzo di protezioni AWS WAF.

Usa restrizione geografica

Puoi utilizzare la restrizione geografica, nota anche come geoblocking, per impedire agli utenti in specifiche aree geografiche di accedere ai contenuti distribuiti tramite una distribuzione CloudFront. Puoi scegliere tra varie opzioni quando configuri restrizioni geografiche. Per ulteriori informazioni, consulta Limitazione della distribuzione geografica del contenuto.

Identity and Access Management per Amazon CloudFront

AWS Identity and Access Management (IAM) aiuta un Servizio AWS amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. CloudFront IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- AWS politiche gestite per Amazon CloudFront
- Utilizzo dei ruoli collegati ai servizi per CloudFront
- Risolvi i problemi relativi all' CloudFront identità e all'accesso ad Amazon

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risolvi i problemi relativi all' CloudFront identità e all'accesso ad Amazon)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come CloudFront funziona Amazon con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon CloudFront)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste

politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

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

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come CloudFront funziona Amazon con IAM

Prima di utilizzare IAM per gestire l'accesso a CloudFront, scopri con quali funzionalità IAM è disponibile l'uso CloudFront.

Funzionalità IAM che puoi utilizzare con Amazon CloudFront

Funzionalità IAM	CloudFront supporto
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	CloudFront supporto
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	No
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come CloudFront e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per CloudFront

Supporta le policy basate sull'identità: sì

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

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per CloudFront

Per visualizzare esempi di politiche basate sull' CloudFront identità, vedere. Esempi di policy basate sull'identità per Amazon CloudFront

Politiche basate sulle risorse all'interno CloudFront

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per CloudFront

Supporta le operazioni di policy: si

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

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di CloudFront azioni, consulta Azioni definite da Amazon CloudFront nel Service Authorization Reference.

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

```
cloudfront
```

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

```
"Action": [
      "cloudfront:action1",
      "cloudfront:action2"
```

```
        ]
```

Per visualizzare esempi di politiche CloudFront basate sull'identità, vedere. Esempi di policy basate sull'identità per Amazon CloudFront

Risorse politiche per CloudFront

Supporta le risorse relative alle policy: sì

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di CloudFront risorse e relativi ARNs, consulta Resources defined by Amazon CloudFront nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon. CloudFront

Per visualizzare esempi di politiche CloudFront basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon CloudFront

Chiavi relative alle condizioni delle politiche per CloudFront

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

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

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

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

Per visualizzare esempi di politiche CloudFront basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon CloudFront

ACLs in CloudFront

Supporti: No ACLs

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

ABAC con CloudFront

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

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

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

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

CloudFront supporta ABAC solo per le distribuzioni.

Utilizzo di credenziali temporanee con CloudFront

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Sessioni di accesso diretto per CloudFront

Supporta l'inoltro delle sessioni di accesso (FAS): no

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per CloudFront

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

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

Ruoli collegati ai servizi per CloudFront

Supporta i ruoli collegati ai servizi: sì

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

CloudFront utilizza ruoli collegati al servizio per eseguire azioni al posto dell'utente. Per ulteriori informazioni sulla creazione o la gestione di ruoli CloudFront collegati ai servizi, consulta. Utilizzo

dei ruoli collegati ai servizi per CloudFront Per ulteriori informazioni su come creare e gestire i ruoli collegati al servizio di Lambda@Edge, consulta Ruoli collegati ai servizi per Lambda@Edge.

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

Esempi di policy basate sull'identità per Amazon CloudFront

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse CloudFront. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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

Per dettagli sulle azioni e sui tipi di risorse definiti da CloudFront, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon CloudFront nel Service Authorization Reference.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare CloudFront risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti

consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI 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": "*"
        }
    ]
}
```

Autorizzazioni per l'accesso programmatico CloudFront

Di seguito viene illustrata una policy di autorizzazione. Il `Sid`, o ID dichiarazione, è facoltativo.

JSON

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

```
      {
         "Sid": "AllowAllCloudFrontPermissions",
         "Effect": "Allow",
         "Action": ["cloudfront:*"],
         "Resource": "*"
      }
   ]
}
```

La politica concede le autorizzazioni per eseguire tutte le CloudFront operazioni, il che è sufficiente per accedere a livello di codice. CloudFront Se utilizzi la console per accedere, consulta. CloudFront Autorizzazioni necessarie per utilizzare la console CloudFront

Per un elenco di azioni e l'ARN che specifichi per concedere o negare l'autorizzazione a utilizzare ciascuna azione, consulta Azioni, risorse e chiavi di condizione per Amazon CloudFront nel Service Authorization Reference.

Autorizzazioni necessarie per utilizzare la console CloudFront

Per concedere l'accesso completo alla CloudFront console, concedi le autorizzazioni nella seguente politica di autorizzazione:

JSON

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

Di seguito viene descritto perché le autorizzazioni sono necessarie:

`acm:ListCertificates`

Quando crei e aggiorni distribuzioni utilizzando la CloudFront console e desideri configurare CloudFront in modo che richieda HTTPS tra il visualizzatore CloudFront e/o tra CloudFront e l'origine, ti consente di visualizzare un elenco di certificati ACM.

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`cloudfront:*`

Consente di eseguire tutte le CloudFront azioni.

`cloudwatch:DescribeAlarms` e **`cloudwatch:PutMetricAlarm`**

Consente di creare e visualizzare CloudWatch allarmi nella CloudFront console. Consulta anche `sns:ListSubscriptionsByTopic` e `sns:ListTopics`.

Queste autorizzazioni non sono necessarie se non utilizzi la console di CloudFront.

`cloudwatch:GetMetricStatistics`

Consente di CloudFront eseguire il rendering CloudWatch delle metriche nella CloudFront console.

Questa autorizzazione non è richiesta se non si utilizza la CloudFront console.

`elasticloadbalancing:DescribeLoadBalancers`

Durante la creazione e l'aggiornamento delle distribuzioni, consente di visualizzare un elenco di sistemi di bilanciamento del carico ELB nell'elenco delle origini disponibili.

Questa autorizzazione non è richiesta se non si utilizza la console. CloudFront

`iam:ListServerCertificates`

Quando crei e aggiorni distribuzioni utilizzando la CloudFront console e desideri configurare CloudFront in modo che richieda HTTPS tra il visualizzatore CloudFront e/o tra CloudFront e l'origine, ti consente di visualizzare un elenco di certificati nell'archivio certificati IAM.

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`s3:ListAllMyBuckets`

Quando crei e aggiorni distribuzioni, ti consente di eseguire le seguenti operazioni:

- Visualizzare un elenco di bucket S3 nell'elenco di origini disponibili
- Visualizzare un elenco di bucket S3 in cui salvare log di accesso

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`S3:PutBucketPolicy`

Quando crei o aggiorni distribuzioni che limitano l'accesso a bucket S3, consente a un utente di aggiornare le policy di bucket per concedere l'accesso all'identità di accesso origine di CloudFront. Per ulteriori informazioni, consulta the section called “Utilizzo di un’identità di accesso origine (legacy, non consigliata)”.

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`sns:ListSubscriptionsByTopic` e **`sns:ListTopics`**

Quando crei CloudWatch allarmi nella CloudFront console, ti consente di scegliere un argomento SNS per le notifiche.

Queste autorizzazioni non sono necessarie se non utilizzi la console di CloudFront.

`waf:GetWebACL` e **`waf:ListWebACLs`**

Consente di visualizzare un elenco di AWS WAF siti Web ACLs nella CloudFront console.

Queste autorizzazioni non sono necessarie se non utilizzi la console di CloudFront.

Azioni che richiedono solo l'autorizzazione per la console CloudFront

È possibile eseguire le seguenti CloudFront azioni nella pagina CloudFront Security Savings Bundle. Le seguenti azioni API non sono destinate a essere richiamate dal codice e non sono incluse in AWS CLI and AWS SDKs.

Azione	Description
`CreateSavingsPlan`	Concede l'autorizzazione per creare un nuovo Savings Plan.
`GetSavingsPlan`	Concede l'autorizzazione per ottenere un Savings Plan.
`ListRateCards`	Concede l'autorizzazione a inserire le schede CloudFront tariffarie relative all'account.
`ListSavingsPlans`	Concede l'autorizzazione per elencare i Savings Plans nell'account.
`ListUsages`	Concede l'autorizzazione all'utilizzo delle liste CloudFront .
`UpdateSavingsPlan`	Concede l'autorizzazione per aggiornare un Savings Plan.

> **Note**
>
> - Per ulteriori informazioni sui piani di CloudFront risparmio, consulta la sezione CloudFront Security Savings Bundle di Amazon CloudFront FAQs.
> - Se crei un piano di risparmio per CloudFront e poi desideri eliminarlo in un secondo momento, contatta Supporto AWS.

Esempi di policy gestite dal cliente

Puoi creare policy IAM personalizzate per consentire le autorizzazioni per le azioni CloudFront API. È possibile allegare queste policy personalizzate agli utenti o ai gruppi IAM che hanno bisogno delle

autorizzazioni specificate. Queste politiche funzionano quando utilizzi l' CloudFront API AWS SDKs, il o il AWS CLI. I seguenti esempi mostrano autorizzazioni per alcuni casi d'utilizzo comuni. Per la politica che garantisce a un utente l'accesso completo a CloudFront, vediAutorizzazioni necessarie per utilizzare la console CloudFront .

Esempi

- Esempio 1: autorizzazione per accedere in lettura a tutte le distribuzioni
- Esempio 2: autorizzazione per la creazione, l'aggiornamento e l'eliminazione di distribuzioni
- Esempio 3: autorizzazione per creare ed elencare invalidamenti
- Esempio 4: consentire la creazione di una distribuzione

Esempio 1: autorizzazione per accedere in lettura a tutte le distribuzioni

La seguente politica di autorizzazioni concede all'utente le autorizzazioni per visualizzare tutte le distribuzioni nella console: CloudFront

JSON

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

Esempio 2: autorizzazione per la creazione, l'aggiornamento e l'eliminazione di distribuzioni

La seguente politica di autorizzazioni consente agli utenti di creare, aggiornare ed eliminare le distribuzioni utilizzando la console: CloudFront

JSON

```
{
   "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'autorizzazione `cloudfront:ListCloudFrontOriginAccessIdentities` consente agli utenti di concedere automaticamente a un'identità di accesso origine l'autorizzazione ad accedere agli oggetti in un bucket Amazon S3. Se vuoi che gli utenti siano in grado di creare identità di accesso origine, devi concedere anche l'autorizzazione `cloudfront:CreateCloudFrontOriginAccessIdentity`.

Esempio 3: autorizzazione per creare ed elencare invalidamenti

La policy di autorizzazione seguente consente agli utenti di creare ed elencare invalidamenti. Include l'accesso in lettura alle CloudFront distribuzioni perché è possibile creare e visualizzare le invalidazioni visualizzando prima le impostazioni di una distribuzione:

JSON

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

Esempio 4: consentire la creazione di una distribuzione

La seguente politica di autorizzazione concede all'utente l'autorizzazione a creare ed elencare le distribuzioni nella console. CloudFront Per l'azione `CreateDistribution`, specifica il carattere jolly (*) per la `Resource` invece di un carattere jolly per la distribuzione ARN (`arn:aws:cloudfront::123456789012:distribution/*`). Per ulteriori informazioni sull'elemento `Resource`, consulta Elementi della policy JSON di IAM: risorsa nella Guida per l'utente IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "cloudfront:CreateDistribution",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "cloudfront:ListDistributions",
            "Resource": "*"
        }
    ]
```

```
}
```

AWS politiche gestite per Amazon CloudFront

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle autonomamente. La creazione di policy gestite dai clienti IAM che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nell'account Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consultare la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Argomenti

- AWS politica gestita: CloudFrontReadOnlyAccess
- AWS politica gestita: CloudFrontFullAccess
- AWS politica gestita: AWSCloud FrontLogger
- AWS politica gestita: AWSLambda Replicator
- AWS politica gestita: Front AWSCloud VPCOrigin ServiceRolePolicy
- CloudFront aggiornamenti alle politiche AWS gestite

AWS politica gestita: CloudFrontReadOnlyAccess

È possibile allegare la policy CloudFrontReadOnlyAccess alle identità IAM. Questa politica consente autorizzazioni di sola lettura per le risorse. CloudFront Consente inoltre autorizzazioni di sola lettura per altre risorse AWS di servizio correlate CloudFront e visibili nella console. CloudFront

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `cloudfront:Describe*`— Consente ai responsabili di ottenere informazioni sui metadati relativi alle risorse. CloudFront
- `cloudfront:Get*`— Consente ai dirigenti di ottenere informazioni e configurazioni dettagliate per le risorse. CloudFront
- `cloudfront:List*`— Consente ai dirigenti di ottenere elenchi di risorse. CloudFront
- `cloudfront-keyvaluestore:Describe*`: consente ai principali di ottenere informazioni sull'archivio di valori delle chiavi.
- `cloudfront-keyvaluestore:Get*`: consente ai principali di ottenere informazioni dettagliate e configurazioni per l'archivio di valori delle chiavi.
- `cloudfront-keyvaluestore:List*`: consente ai principali di ottenere elenchi di archivi di valori delle chiavi.
- `acm:DescribeCertificate`: consente ai principali di ottenere dettagli su un certificato ACM.
- `acm:ListCertificates`: consente alle entità di ottenere un elenco di certificati ACM.
- `iam:ListServerCertificates`: consente alle entità di ottenere un elenco dei certificati del server archiviati in IAM.
- `route53:List*`: consente alle entità di ottenere elenchi di risorse Route 53.
- `waf:ListWebACLs`— Consente ai presidi di accedere a un elenco di siti Web ACLs . AWS WAF
- `waf:GetWebACL`— Consente ai dirigenti di ottenere informazioni dettagliate sul web ACLs in. AWS WAF
- `wafv2:ListWebACLs`— Consente ai presidi di accedere a un elenco di siti Web ACLs . AWS WAF
- `wafv2:GetWebACL`— Consente ai dirigenti di ottenere informazioni dettagliate sul web ACLs in. AWS WAF
- `pricingplanmanager:GetSubscription`— Consente ai dirigenti l'accesso in sola lettura ai dettagli sugli abbonamenti ai piani tariffari.

- `pricingplanmanager:ListSubscriptions`— Consente ai responsabili l'accesso in sola lettura agli abbonamenti ai piani tariffari di listino.
- `ec2:DescribeIpamPools`— Consente ai responsabili di ottenere informazioni dettagliate sui pool IPAM.
- `ec2:GetIpamPoolCidrs`— Consente ai mandanti di far arrivare il CIDRs provisioning a un pool IPAM.

Per vedere le autorizzazioni per questa policy, consulta CloudFrontReadOnlyAccess nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: CloudFrontFullAccess

È possibile allegare la policy CloudFrontFullAccess alle identità IAM. Questa politica consente autorizzazioni amministrative per le CloudFront risorse. Consente inoltre autorizzazioni di sola lettura per altre risorse di AWS servizio correlate CloudFront e visibili nella console. CloudFront

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `s3:ListAllMyBuckets`: consente alle entità di ottenere un elenco di tutti i bucket Amazon S3.
- `acm:DescribeCertificate`: consente ai principali di ottenere dettagli su un certificato ACM.
- `acm:ListCertificates`: consente alle entità di ottenere un elenco di certificati ACM.
- `acm:RequestCertificate`: consente ai principali di richiedere certificati gestiti da ACM.
- `cloudfront:*`— Consente ai responsabili di eseguire tutte le azioni su tutte le risorse. CloudFront
- `cloudfront-keyvaluestore:*`: consente ai principali di eseguire tutte le azioni sull'archivio di valori delle chiavi.
- `iam:ListServerCertificates`: consente alle entità di ottenere un elenco dei certificati del server archiviati in IAM.
- `waf:ListWebACLs`— Consente ai presidi di accedere a un elenco di siti Web ACLs . AWS WAF
- `waf:GetWebACL`— Consente ai dirigenti di ottenere informazioni dettagliate sul web ACLs in. AWS WAF
- `waf:CreateWebACLs`— Consente ai responsabili di creare un ACL web in. AWS WAF
- `wafv2:ListWebACLs`— Consente ai responsabili di accedere a un elenco di siti Web. ACLs AWS WAF

- `wafv2:GetWebACL`— Consente ai dirigenti di ottenere informazioni dettagliate sul web ACLs in. AWS WAF
- `kinesis:ListStreams`: consente alle entità di ottenere un elenco di flussi Amazon Kinesis.
- `elasticloadbalancing:DescribeLoadBalancers`- Consente ai responsabili di ottenere informazioni dettagliate sui sistemi di bilanciamento del carico in ELB.
- `kinesis:DescribeStream`: consente alle entità di ottenere informazioni dettagliate su un flusso Kinesis.
- `iam:ListRoles`: consente alle entità di ottenere un elenco dei ruoli in IAM.
- `pricingplanmanager:AssociateResourcesToSubscription`- Consente ai responsabili di associare risorse a un abbonamento. In questo modo le risorse possono essere coperte dal piano tariffario dell'abbonamento.
- `pricingplanmanager:CancelSubscription`- Consente ai mandanti di annullare un abbonamento esistente.
- `pricingplanmanager:CancelSubscriptionChange`- Consente ai responsabili di annullare una modifica in sospeso a un abbonamento esistente, ad esempio un aggiornamento del piano, prima che la modifica venga applicata.
- `pricingplanmanager:CreateSubscription`- Consente ai dirigenti di creare un abbonamento a un piano tariffario.
- `pricingplanmanager:DisassociateResourcesFromSubscription`- Consente ai responsabili di rimuovere l'associazione tra le risorse e un abbonamento esistente.
- `pricingplanmanager:UpdateSubscription`- Consente ai mandanti di modificare un abbonamento esistente, ad esempio cambiando il piano tariffario.
- `pricingplanmanager:GetSubscription`— Consente ai responsabili l'accesso in sola lettura ai dettagli sugli abbonamenti ai piani tariffari.
- `pricingplanmanager:ListSubscriptions`— Consente ai responsabili l'accesso in sola lettura agli abbonamenti ai piani tariffari di listino.
- `ec2:DescribeInstances`- Consente ai responsabili di ottenere informazioni dettagliate sulle istanze in Amazon. EC2
- `ec2:DescribeInternetGateways`- Consente ai responsabili di ottenere informazioni dettagliate sui gateway Internet in Amazon. EC2
- `ec2:DescribeIpamPools`— Consente ai responsabili di ottenere informazioni dettagliate sui pool IPAM.

- `ec2:GetIpamPoolCidrs`— Consente ai mandanti di far arrivare il CIDRs provisioning a un pool IPAM.

Per vedere le autorizzazioni per questa policy, consulta CloudFrontFullAccess nella Guida di riferimento sulle policy gestite da AWS .

> **Important**
>
> Se si desidera CloudFront creare e salvare i registri di accesso, è necessario concedere autorizzazioni aggiuntive. Per ulteriori informazioni, consulta Autorizzazioni.

AWS politica gestita: AWSCloud FrontLogger

Non puoi collegare la AWSCloudFrontLoggerpolicy alle tue identità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni CloudFront per tuo conto. Per ulteriori informazioni, consulta the section called “Ruoli collegati ai servizi per Lambda@Edge”.

Questa politica consente di CloudFront inviare file di registro ad Amazon CloudWatch. Per dettagli sulle autorizzazioni incluse in questa policy, consulta the section called “Autorizzazioni relative ai ruoli collegati ai servizi per logger CloudFront”.

Per vedere le autorizzazioni per questa policy, consulta AWSCloudFrontLogger nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSLambda Replicator

Non puoi collegare la policy AWSLambdaReplicator alle tue identità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni CloudFront per conto dell'utente. Per ulteriori informazioni, consulta the section called “Ruoli collegati ai servizi per Lambda@Edge”.

Questa policy consente di CloudFront creare, eliminare e disabilitare funzioni su cui AWS Lambda replicare le funzioni Lambda @Edge. Regioni AWS Per dettagli sulle autorizzazioni incluse in questa policy, consulta the section called “Autorizzazioni del ruolo collegato ai servizi per Lambda Replicator”.

Per visualizzare le autorizzazioni per questa policy, consulta AWSLambdaReplicator nel Managed Policy Reference.AWS

AWS politica gestita: Front AWSCloud VPCOrigin ServiceRolePolicy

Non puoi allegare la VPCOrigin ServiceRolePolicy policy AWSCloudFront alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di CloudFront eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi per CloudFront.

Questa politica consente di CloudFront gestire interfacce di rete EC2 elastiche e gruppi di sicurezza per conto dell'utente. Per dettagli sulle autorizzazioni incluse in questa policy, consulta the section called “Autorizzazioni di ruolo collegate ai servizi per VPC Origins CloudFront ”.

Per visualizzare le autorizzazioni per questa politica, consulta AWSCloudFront VPCOrigin ServiceRolePolicy nel AWS Managed Policy Reference.

CloudFront aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite CloudFront da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei CloudFront documenti.

Modifica	Descrizione	Data
CloudFrontReadOnlyAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per Amazon EC2. Le nuove autorizzazioni consentono ai responsabili di utilizzare le `ec2:DescribeIpamPools` azioni e. `ec2:GetIpamPoolCidrs`	24 novembre 2025
CloudFrontFullAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per Amazon EC2. Le nuove autorizzazioni consentono ai responsabili di utilizzare le `ec2:Descr`	24 novembre 2025

Modifica	Descrizione	Data
	`ibeIpamPools` azioni e. `ec2:GetIpamPoolCidrs`	
CloudFrontFullAccess: aggiornamento a policy esistente	CloudFront ha aggiunto una nuova autorizzazione per creare una risorsa AWS WAF ACL e ha aggiunto le autorizza zioni di creazione, aggiornam ento, eliminazione e lettura a AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontFullAccess: aggiornamento a policy esistente	CloudFront ha aggiunto una nuova autorizzazione per creare una risorsa AWS WAF ACL e ha aggiunto le autorizza zioni di creazione, aggiornam ento, eliminazione e lettura a AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontReadOnlyAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per l'accesso in sola lettura a AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontReadOnlyAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per l'accesso in sola lettura a AWS Pricing Plan Manager.	18 novembre 2025

Modifica	Descrizione	Data
CloudFrontReadOnlyAccess: aggiornamento a policy esistente	CloudFront ha aggiunto una nuova autorizzazione per ACM. La nuova autorizzazione consente ai principali di ottenere i dettagli su un certificato ACM.	28 aprile 2025
CloudFrontFullAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per ACM. Le nuove autorizzazioni consentono ai principali di ottenere dettagli su un certifica to ACM e di richiedere un certificato gestito da ACM.	28 aprile 2025
CloudFrontFullAccess: aggiornamento a policy esistente	CloudFront ha aggiunto nuove autorizzazioni per Amazon EC2 ed ELB. Le nuove autorizzazioni consentono di CloudFront ottenere informazioni dettaglia te sui sistemi di bilanciam ento del carico in ELB e sulle istanze e sui gateway Internet in Amazon. EC2	20 novembre 2024

Modifica	Descrizione	Data
AWSCloudFront: VPCOrigin ServiceRolePolicy Nuova politica	CloudFront ha aggiunto una nuova politica. Questa politica consente di CloudFront gestire interfacce di rete EC2 elastiche e gruppi di sicurezza per conto dell'utente.	20 novembre 2024
CloudFrontReadOnlyAccess e CloudFrontFullAccess: aggiornamenti a due policy esistenti.	CloudFront ha aggiunto nuove autorizzazioni per gli archivi di valori chiave. Le nuove autorizzazioni consentono agli utenti di ottenere informazioni sugli archivi di valori delle chiavi e di effettuare azioni su di essi.	19 dicembre 2023
CloudFrontReadOnlyAccess: aggiornamento di una policy esistente	CloudFront ha aggiunto una nuova autorizzazione per descrivere CloudFront le funzioni. Questa autorizzazione consente all'utente, al gruppo o al ruolo di leggere informazioni e metadati su una funzione, ma non il codice della funzione.	08 settembre 2021
CloudFront ha iniziato a tenere traccia delle modifiche	CloudFront ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	08 settembre 2021

Utilizzo dei ruoli collegati ai servizi per CloudFront

Amazon CloudFront utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. CloudFront I ruoli collegati ai servizi sono predefiniti CloudFront e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione CloudFront perché non è necessario aggiungere manualmente le autorizzazioni necessarie. CloudFront definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. CloudFront Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo proteggi CloudFront le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per VPC Origins CloudFront

CloudFront VPC Origins utilizza il ruolo collegato al servizio denominato AWSServiceRoleForCloudFrontVPCOrigin: consente di gestire interfacce di rete EC2 elastiche e gruppi di sicurezza CloudFront per tuo conto.

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio AWSServiceRoleForCloudFrontVPCOrigin considera attendibili i seguenti servizi:

- `vpcorigin.cloudfront.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSCloud Front VPCOrigin ServiceRolePolicy consente a CloudFront VPC Origins di completare le seguenti azioni sulle risorse specificate:

- Operazione: `ec2:CreateNetworkInterface` su `arn:aws:ec2:*:*:network-interface/*`
- Azione: `ec2:CreateNetworkInterface` su `arn:aws:ec2:*:*:subnet/*` e `arn:aws:ec2:*:*:security-group/*`

- Operazione: `ec2:CreateSecurityGroup` su `arn:aws:ec2:*:*:security-group/*`
- Operazione: `ec2:CreateSecurityGroup` su `arn:aws:ec2:*:*:vpc/*`
- Azione: `ec2:ModifyNetworkInterfaceAttribute`, `ec2:DeleteNetworkInterface`, `ec2:DeleteSecurityGroup`, `ec2:AssignIpv6Addresses` e `ec2:UnassignIpv6Addresses` su `supported AWS resources that have the aws:ResourceTag/aws.cloudfront.vpcorigin tag enabled`
- Azione: `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeInstances`, `ec2:DescribeInternetGateways`, `ec2:DescribeSubnets`, `ec2:DescribeRegions` e `ec2:DescribeAddresses` su `all AWS resources that the actions support`
- Azione: `ec2:CreateTags` su `arn:aws:ec2:*:*:security-group/*` e `arn:aws:ec2:*:*:network-interface/*`
- Azione: `elasticloadbalancing:DescribeLoadBalancers`, `elasticloadbalancing:DescribeListeners` e `elasticloadbalancing:DescribeTargetGroups` su `all AWS resources that the actions support`

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente IAM.

Crea un ruolo collegato ai servizi per VPC Origins CloudFront

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un'origine VPC nella Console di gestione AWS, o nell' AWS API AWS CLI, CloudFront VPC Origins crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un'origine VPC, VPC Origins crea CloudFront nuovamente il ruolo collegato al servizio per te.

Modifica un ruolo collegato al servizio per VPC Origins CloudFront

CloudFront VPC Origins non consente di modificare il ruolo collegato al AWSServiceRoleForCloudFrontVPCOrigin servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile

tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminare un ruolo collegato al servizio per VPC Origins CloudFront

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il CloudFront servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse CloudFront VPC Origins utilizzate da AWSServiceRoleForCloudFrontVPCOrigin

- Elimina le risorse di origine VPC nell'account.
  - Il completamento dell'eliminazione delle risorse dal tuo account potrebbe richiedere del tempo. CloudFront Se non riesci a eliminare immediatamente il ruolo collegato al servizio, attendi e riprova.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForCloudFrontVPCOrigin servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i CloudFront ruoli collegati ai servizi VPC Origins

CloudFront VPC Origins non supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Il ruolo AWSServiceRoleForCloudFrontVPCOrigin può essere utilizzato nelle regioni seguenti.

Nome della Regione	Identità della Regione	Support in CloudFront
Stati Uniti orientali (Virginia settentrionale)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
Stati Uniti occidentali (California settentrionale)	us-west-1 (eccetto AZ usw1-az2)	Sì
Stati Uniti occidentali (Oregon)	us-west-2	Sì
Africa (Città del Capo)	af-south-1	Sì
Asia Pacific (Hong Kong)	ap-east-1	Sì
Asia Pacifico (Giacarta)	ap-southeast-3	Sì
Asia Pacifico (Melbourne)	ap-southeast-4	Sì
Asia Pacifico (Mumbai)	ap-south-1	Sì
Asia Pacifico (Hyderabad)	ap-south-2	Sì
Asia Pacifico (Osaka)	ap-northeast-3	Sì
Asia Pacifico (Seoul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1 (eccetto AZ apne1-az3)	Sì
Canada (Centrale)	ca-central-1 (eccetto AZ cac1-az3)	Sì
Canada occidentale (Calgary)	ca-west-1	Sì
Europa (Francoforte)	eu-central-1	Sì

Nome della Regione	Identità della Regione	Support in CloudFront
Europa (Irlanda)	eu-west-1	Sì
Europa (Londra)	eu-west-2	Sì
Europe (Milan)	eu-south-1	Sì
Europa (Parigi)	eu-west-3	Sì
Europa (Spagna)	eu-south-2	Sì
Europa (Stoccolma)	eu-north-1	Sì
Europa (Zurigo)	eu-central-2	Sì
Israele (Tel Aviv)	il-central-1	Sì
Medio Oriente (Bahrein)	me-south-1	Sì
Medio Oriente (Emirati Arabi Uniti)	me-central-1	Sì
Sud America (San Paolo)	sa-east-1	Sì

Risolvi i problemi relativi all' CloudFront identità e all'accesso ad Amazon

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

Argomenti

- Non sono autorizzato a eseguire un'azione in CloudFront
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie CloudFront risorse

Non sono autorizzato a eseguire un'azione in CloudFront

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

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

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

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

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

Non sono autorizzato a eseguire iam: PassRole

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

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

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

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

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

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

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

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

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

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se CloudFront supporta queste funzionalità, consulta. Come CloudFront funziona Amazon con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Registrazione e monitoraggio in Amazon CloudFront

Il monitoraggio è un elemento importante per mantenere la disponibilità e le prestazioni delle CloudFront tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le CloudFront risorse e le attività e rispondere a potenziali incidenti:

CloudWatch Allarmi Amazon

> Utilizzando gli CloudWatch allarmi, controlli una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, viene inviata una notifica a un argomento o una policy di Amazon SNS. AWS Auto Scaling CloudWatch gli allarmi non richiamano azioni quando una metrica si trova in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato.
>
> Per ulteriori informazioni, consulta Monitoraggio delle metriche CloudFront con Amazon CloudWatch.

AWS CloudTrail registri

CloudTrail fornisce un registro delle azioni API eseguite da un utente, un ruolo o un AWS servizio in CloudFront. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta API a cui è stata effettuata CloudFront, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni, consulta Registrazione di log delle chiamate API Amazon CloudFront utilizzando AWS CloudTrail.

CloudFront registri standard e registri di accesso in tempo reale

CloudFront i registri forniscono registrazioni dettagliate sulle richieste inviate a una distribuzione. Questi log sono utili per molte applicazioni. Ad esempio, le informazioni del log di accesso possono essere utili nei controlli di accesso e di sicurezza.

Per ulteriori informazioni, consultare Registri di accesso (registri standard) e Crea e utilizza configurazioni dei registri di accesso in tempo reale.

Registri delle funzioni Edge

I log generati dalle funzioni edge, sia CloudFront Functions che Lambda @Edge, vengono inviati direttamente ad CloudWatch Amazon Logs e non vengono archiviati da nessuna parte. CloudFront CloudFront Functions utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) per inviare i log generati dal cliente direttamente ai registri del tuo account. CloudWatch

Per ulteriori informazioni, consulta Registri delle funzioni Edge.

CloudFront report della console

La CloudFront console include una varietà di report, tra cui il rapporto sulle statistiche sulla cache, il report sugli oggetti più diffusi e il rapporto sui principali referrer. La maggior parte dei report della CloudFront console si basa sui dati contenuti nei log di CloudFront accesso, che contengono informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Tuttavia, non è necessario attivare i log di accesso per visualizzare i report.

Per ulteriori informazioni, consulta Visualizzazione dei report CloudFront nella console.

Convalida della conformità per Amazon CloudFront

I revisori di terze parti valutano la sicurezza e la conformità di Amazon nell' CloudFront ambito di diversi programmi di AWS conformità. Sono inclusi SOC, PCI e HIPAA.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta AWS Services in Scope by Compliance Program. Per informazioni generali, consulta Programmi di conformità di AWS.

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact.

La vostra responsabilità di conformità durante l'utilizzo CloudFront è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- Architecting for HIPAA Security and Compliance on AWS: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi allo standard HIPAA. AWS

  Il programma di conformità AWS HIPAA include CloudFront (esclusa la distribuzione di contenuti tramite Embedded) come servizio idoneo allo standard HIPAA. CloudFront POPs Se disponi di un Business Associate Addendum (BAA) eseguito con AWS, puoi utilizzare CloudFront (esclusa la distribuzione di contenuti tramite CloudFront Embedded POPs) per fornire contenuti che contengono informazioni sanitarie protette (PHI). Per ulteriori informazioni, consulta Compliance HIPAA.
- AWS Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub CSPM— Questo AWS servizio utilizza controlli di sicurezza per valutare le configurazioni delle risorse e gli standard di sicurezza per aiutarvi a rispettare vari quadri di conformità. Per ulteriori informazioni sull'utilizzo di Security Hub CSPM per valutare CloudFront le risorse, consulta CloudFront i controlli di Amazon nella Guida per l'AWS Security Hub CSPM utente.

CloudFront migliori pratiche di conformità

Questa sezione fornisce le migliori pratiche e consigli per la conformità quando usi Amazon CloudFront per pubblicare i tuoi contenuti.

Se esegui carichi di lavoro conformi a PCI o HIPAA basati sul modello di responsabilitàAWS condivisa, ti consigliamo di registrare i CloudFront dati di utilizzo degli ultimi 365 giorni per scopi di controllo futuri. Per registrare dati di utilizzo, puoi procedere come segue:

- Abilita i log di accesso. CloudFront Per ulteriori informazioni, consulta Registri di accesso (registri standard).
- Acquisisci le richieste inviate all' CloudFront API. Per ulteriori informazioni, consulta Registrazione di log delle chiamate API Amazon CloudFront utilizzando AWS CloudTrail.

Inoltre, consulta quanto segue per i dettagli sulla conformità agli standard PCI DSS e SOC. CloudFront

Payment Card Industry Data Security Standard (PCI DSS)

CloudFront (esclusa la distribuzione di contenuti tramite CloudFront Embedded POPs) supporta l'elaborazione, l'archiviazione e la trasmissione dei dati delle carte di credito da parte di un commerciante o di un fornitore di servizi ed è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (DSS). Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere PCI DSS Level 1.

Come best practice di sicurezza, ti consigliamo di non memorizzare nella cache edge i dati delle carte di credito. CloudFront Ad esempio, puoi configurare la tua origine per includere un'`Cache-Control:no-cache="`*`field-name`*`"`intestazione nelle risposte che contengono i dati della carta di credito, come le ultime quattro cifre del numero di carta di credito e le informazioni di contatto del proprietario della carta.

System and Organization Controls (SOC)

CloudFront (esclusa la distribuzione di contenuti tramite CloudFront Embedded POPs) è conforme alle misure SOC (System and Organization Controls), tra cui SOC 1, SOC 2 e SOC 3. I report SOC sono rapporti di esame indipendenti e di terze parti che dimostrano come AWS raggiungere i controlli e gli obiettivi chiave di conformità. Questi audit assicurano che vengano attuate le adeguate procedure e tutele per proteggersi dai rischi che possono minare sicurezza, riservatezza e

disponibilità dei dati di clienti e aziende. I risultati di questi audit di terze parti sono disponibili sul sito Web AWS SOC Compliance, dove è possibile visualizzare i report pubblicati per ottenere maggiori informazioni sui controlli a supporto AWS delle operazioni e della conformità.

Resilienza in Amazon CloudFront

L'infrastruttura globale di AWS è basata su Regioni e zone di disponibilità AWS. Le Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e con throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni su Regioni e zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Failover di origine CloudFront

Oltre al supporto dell'infrastruttura globale AWS, Amazon CloudFront offre una funzionalità di failover di origine per supportare le esigenze di resilienza dei dati. CloudFront è un servizio globale che fornisce i tuoi contenuti attraverso una rete mondiale di data center denominati edge location o point of presence (POP). Se i contenuti non sono già memorizzati nella cache in una edge location, vengono recuperati da CloudFront da un server di origine che hai identificato come l'origine per la versione definitiva dei contenuti.

Puoi migliorare la resilienza e aumentare la disponibilità per scenari specifici impostando CloudFront con il failover di origine. Per iniziare, crei un gruppo di origine in cui designi un'origine primaria per CloudFront più una seconda origine. CloudFront passa automaticamente alla seconda origine quando l'origine primaria restituisce risposte negative specifiche per il codice di stato HTTP. Per ulteriori informazioni, consulta Ottimizzazione dell'elevata disponibilità con il failover di origine CloudFront.

Sicurezza dell'infrastruttura in Amazon CloudFront

In qualità di servizio gestito, Amazon CloudFront è protetto dalla sicurezza della rete globale AWS. Per informazioni sui servizi di sicurezza AWSe su come AWSprotegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWSutilizzando le best practice per

la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWSWell-Architected Framework.

Utilizza le chiamate API pubblicate da AWS per accedere a CloudFront tramite la rete. I client devono supportare quanto segue:

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

Funzioni CloudFront utilizza una barriera di isolamento altamente sicura tra account AWS, garantendo che gli ambienti dei clienti siano protetti contro attacchi laterali come Spectre e Meltdown. Functions non può accedere a dati che appartengono ad altri clienti o modificarli. Functions viene eseguito in un processo dedicato a thread singolo su una CPU dedicata senza hyperthreading. In un dato POP (point of presence) della edge location CloudFront, CloudFront Functions serve solo un cliente alla volta e tutti i dati specifici del cliente vengono cancellati tra le esecuzioni delle funzioni.

risoluzione dei problemi

Usa questa sezione per risolvere i problemi più comuni che potresti riscontrare durante la configurazione di Amazon CloudFront per la distribuzione dei tuoi contenuti.

Ogni argomento fornisce indicazioni dettagliate sull'identificazione della causa principale dei problemi più comuni e step-by-step istruzioni per risolverli.

Argomenti

Risoluzione di problemi di distribuzione

Usa le informazioni qui per aiutarti a diagnosticare e correggere errori di certificato, problemi di accesso negato o altri problemi comuni che potresti riscontrare durante la configurazione del tuo sito Web o dell'applicazione con le distribuzioni Amazon. CloudFront

Argomenti

CloudFront restituisce un errore Access Denied

Se utilizzi un bucket Amazon S3 come origine per la tua CloudFront distribuzione, potresti visualizzare un messaggio di errore Access Denied (403) negli esempi seguenti.

Indice

- Autorizzazioni IAM mancanti per l'origine Amazon S3
- Utilizzo di credenziali non valide o autorizzazioni insufficienti

Specificato un oggetto mancante dall'origine Amazon S3

Verifica che l'oggetto richiesto nel bucket esista. I nomi degli oggetti fanno distinzione tra maiuscole e minuscole. L'immissione di un nome oggetto non valido può restituire un codice di errore di accesso negato.

Ad esempio, se segui il CloudFront tutorial per creare una distribuzione di base, crei un bucket Amazon S3 come origine e carichi un file di esempio. `index.html`

Nel browser web, se si inserisce `https://d111111abcdef8.cloudfront.net/INDEX.HTML` invece di `https://d111111abcdef8.cloudfront.net/index.html`, potrebbe essere visualizzato un messaggio simile perché il file `index.html` nel percorso URL fa distinzione tra maiuscole e minuscole.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>22Q367AHT7Y1ABCD</RequestId>
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
</Error>
```

Autorizzazioni IAM mancanti per l'origine Amazon S3

Verifica di aver selezionato il bucket Amazon S3 corretto come dominio e nome di origine. L'origine (Amazon S3) deve disporre delle autorizzazioni corrette.

Se non si specificano le autorizzazioni corrette, è possibile che venga visualizzato un messaggio `AccessDenied` per i visualizzatori.

Quando distribuisci contenuti da Amazon S3 e utilizzi anche AWS Key Management Service (AWS KMS) la crittografia lato servizio (SSE-KMS), devi specificare autorizzazioni IAM aggiuntive per la chiave KMS e il bucket Amazon S3. La tua CloudFront distribuzione necessita di queste autorizzazioni per utilizzare la chiave KMS, utilizzata per la crittografia del bucket Amazon S3 di origine.

Le configurazioni della bucket policy di Amazon S3 consentono alla distribuzione di recuperare CloudFront gli oggetti crittografati per la distribuzione dei contenuti.

Come verificare le autorizzazioni del bucket Amazon S3 e della chiave KMS

1. Verifica che la chiave KMS che stai utilizzando sia la stessa chiave utilizzata dal bucket Amazon S3 per la crittografia predefinita. Per ulteriori informazioni, consulta Specifica della crittografia lato server con AWS KMS (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.
2. Verifica che gli oggetti nel bucket siano crittografati con la stessa chiave KMS. Puoi selezionare qualsiasi oggetto dal bucket Amazon S3 e controllare le impostazioni di crittografia lato server per verificare l'ARN della chiave KMS.
3. Modifica la policy del bucket Amazon S3 per concedere l' CloudFront autorizzazione a chiamare l'operazione `GetObject` API dal bucket Amazon S3. Per un esempio di policy di bucket Amazon S3 che utilizza il controllo di accesso origine, consulta Concedi l' CloudFront autorizzazione per accedere al bucket S3.
4. Modifica la politica delle chiavi KMS per concedere l' CloudFront autorizzazione a eseguire le azioni a, e. `Encrypt` `Decrypt` `GenerateDataKey*` Per eseguire l'allineamento con il privilegio minimo, specifica un `Condition` elemento in modo che solo la CloudFront distribuzione specificata possa eseguire le azioni elencate. È possibile personalizzare la politica in base alla politica esistente AWS KMS . Per un esempio di policy della chiave KMS, consulta la SSE-KMS.

Se utilizzi identità di accesso origine (OAI) anziché OAC, le autorizzazioni per il bucket Amazon S3 sono leggermente diverse perché concedi l'autorizzazione a un'identità anziché a un Servizio AWS. Per ulteriori informazioni, consulta Concedere a un'identità di accesso origine l'autorizzazione per leggere i file nel bucket Amazon S3.

Se ancora non riesci a visualizzare i file nella distribuzione, consulta Non posso visualizzare i file nella distribuzione.

Utilizzo di credenziali non valide o autorizzazioni insufficienti

Può apparire un messaggio di errore Accesso negato se utilizzi AWS SCT credenziali errate o scadute (chiave di accesso e chiave segreta) o se al tuo ruolo o utente IAM manca l'autorizzazione necessaria per eseguire un'azione su una CloudFront risorsa. Per ulteriori informazioni sui messaggi di errore di accesso negato, consulta Risoluzione dei problemi relativi ai messaggi di errore di accesso negato nella Guida per l'utente IAM.

Per informazioni su come funziona IAM CloudFront, consulta. Identity and Access Management per Amazon CloudFront

CloudFront restituisce un InvalidViewerCertificate errore quando tento di aggiungere un nome di dominio alternativo

Se CloudFront restituisce un `InvalidViewerCertificate` errore quando tenti di aggiungere un nome di dominio alternativo (CNAME) alla tua distribuzione, consulta le seguenti informazioni per risolvere il problema. Questo errore può indicare che uno dei seguenti problemi devono essere risolti prima che sia possibile aggiungere il nome di dominio alternativo.

I seguenti errori sono elencati nell'ordine in cui viene CloudFront verificata l'autorizzazione all'aggiunta di un nome di dominio alternativo. Questo può aiutarti a risolvere i problemi perché, in base all'errore CloudFront restituito, puoi stabilire quali controlli di verifica sono stati completati correttamente.

Nessun certificato collegato alla distribuzione

> Per aggiungere un nome di dominio alternativo (CNAME), è necessario collegare un certificato valido, attendibile alla distribuzione. Rivedi i requisiti, ottieni un certificato valido che li soddisfa, collegalo alla distribuzione e riprova. Per ulteriori informazioni, consulta Requisiti per l'utilizzo di nomi di dominio alternativi.

La catena di certificati contiene troppi certificati per il certificato che hai collegato.

> Una catena di certificati può contenere un massimo di cinque certificati. Riduci il numero di certificati nella catena e riprova.

La catena di certificati include uno o più certificati che non sono validi per la data corrente.

> La catena di certificati per un certificato che hai aggiunto dispone di uno o più certificati che non sono validi, perché un certificato non è ancora valido o perché un certificato è scaduto. Controlla i campi Not Valid Before (Non valido prima) e Not Valid After (Non valido dopo) nei certificati della catena di certificati per accertarti che tutti i certificati siano validi in base alle date elencate.

Il certificato che hai collegato non è firmato da un'autorità di certificazione (CA) attendibile.

> Il certificato a cui ti alleghi per CloudFront verificare un nome di dominio alternativo non può essere un certificato autofirmato. Deve essere firmato da una CA attendibile. Per ulteriori informazioni, consulta Requisiti per l'utilizzo di nomi di dominio alternativi.

Il certificato che hai collegato non è formattato correttamente

Il formato del nome di dominio e dell'indirizzo IP che sono inclusi nel certificato e il formato del certificato stesso devono seguire lo standard per i certificati.

Si è verificato un errore CloudFront interno.

CloudFront è stato bloccato da un problema interno e non è stato possibile effettuare controlli di convalida per i certificati. In questo scenario, CloudFront restituisce un codice di stato HTTP 500 e indica che esiste un CloudFront problema interno con il collegamento del certificato. Attendi alcuni minuti, quindi riprova ad aggiungere il nome di dominio alternativo al certificato.

Il certificato che hai collegato non include il nome di dominio alternativo che stai tentando di aggiungere.

Per ogni nome di dominio alternativo che aggiungi, è CloudFront necessario allegare un SSL/TLS certificato valido rilasciato da un'autorità di certificazione (CA) affidabile che copre il nome di dominio, per convalidare l'autorizzazione all'utilizzo. Aggiorna il certificato per includere un nome di dominio che include il CNAME che stai tentando di aggiungere. Per ulteriori informazioni ed esempi di utilizzo di nomi di dominio con caratteri jolly, consulta Requisiti per l'utilizzo di nomi di dominio alternativi.

CloudFront restituisce un errore di record DNS configurato in modo errato quando tento di aggiungere un nuovo CNAME

Se esiste una voce DNS con caratteri jolly che punta a una CloudFront distribuzione, se provi ad aggiungere un nuovo CNAME con un nome più specifico, potresti riscontrare il seguente errore:

```
One or more aliases specified for the distribution includes an incorrectly configured
 DNS record that points to another CloudFront distribution. You must update the DNS
 record to correct the problem.
```

Questo errore si verifica perché CloudFront interroga il DNS sul CNAME e la voce DNS con caratteri jolly viene risolta in un'altra distribuzione.

Per risolvere il problema, crea innanzitutto un’altra distribuzione, quindi crea una voce DNS che punti alla nuova distribuzione. Infine, aggiungi il CNAME più specifico. Per ulteriori informazioni su come aggiungere, consulta. CNAMEs Aggiunta di un nome di dominio alternativo

Non posso visualizzare i file nella distribuzione

Se non riesci a visualizzare i file della tua CloudFront distribuzione, consulta gli argomenti seguenti per alcune soluzioni comuni.

Ti sei registrato sia ad Amazon S3 che CloudFront ad Amazon S3?

Per utilizzare Amazon CloudFront con un'origine Amazon S3, devi iscriverti a entrambi CloudFront e ad Amazon S3, separatamente. Per ulteriori informazioni sulla registrazione ad CloudFront Amazon S3, consulta. Configura il tuo Account AWS

Le autorizzazioni per oggetti e il bucket Amazon S3 sono impostati correttamente?

Se utilizzi CloudFront un'origine Amazon S3, le versioni originali dei tuoi contenuti vengono archiviate in un bucket S3. Per offrire i contenuti ai tuoi spettatori, ti consigliamo di utilizzare CloudFront Origin Access Control (OAC) per proteggere l'accesso ai bucket Amazon S3. Ciò significa che il tuo bucket S3 è raggiungibile solo tramite. CloudFront OAC controlla l'accesso dei visualizzatori e la consegna sicura tramite. CloudFront Per ulteriori informazioni su OAC, consulta the section called “Limitazione dell’accesso a un’origine Amazon S3”.

Per ulteriori informazioni sulla gestione dell’accesso al bucket, consulta Blocco dell’accesso pubblico all’archiviazione Amazon S3 nella Guida per l’utente di Amazon S3.

Le proprietà di oggetti e le proprietà di bucket sono indipendenti. È necessario concedere esplicitamente i privilegi per ogni oggetto in un bucket Amazon S3. Gli oggetti non ereditano proprietà dai bucket e le proprietà di oggetto devono essere definite indipendentemente dal bucket.

Il nome di dominio alternativo (CNAME) è configurato correttamente?

Se hai già un record CNAME esistente per il tuo nome di dominio, aggiorna quel record o sostituiscilo con uno nuovo che punti al nome di dominio della tua distribuzione.

Assicurati inoltre che il record CNAME punti al nome di dominio della distribuzione, non al tuo bucket Amazon S3. Puoi confermare che il record CNAME nel sistema DNS punta al nome di dominio della distribuzione. A tale scopo, utilizza uno strumento DNS come dig.

L'esempio seguente mostra una richiesta dig per un nome di dominio denominato `images.example.com` e la parte pertinente della risposta. Sotto `ANSWER SECTION`, esamina la riga che contiene `CNAME`. Il record CNAME per il tuo nome di dominio è impostato correttamente se il valore sul lato destro di CNAME è il nome di dominio della tua CloudFront distribuzione. Se è

il bucket del tuo server di origine Amazon S3 o un altro nome di dominio, il record CNAME non è configurato correttamente.

```
[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.
...
...
```

Per ulteriori informazioni su CNAMEs, consulta. Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs

Stai facendo riferimento all'URL corretto per la tua CloudFront distribuzione?

Assicurati che l'URL a cui fai riferimento utilizzi il nome di dominio (o CNAME) della tua CloudFront distribuzione, non il bucket Amazon S3 o l'origine personalizzata.

Hai bisogno di assistenza per risolvere un problema relativo a un'origine personalizzata?

Se hai bisogno di aiutarti AWS a risolvere i problemi relativi a un'origine personalizzata, probabilmente dovremo controllare le voci di intestazione delle tue richieste. `X-Amz-Cf-Id` Se non hai già registrato queste voci, ti consigliamo di farlo. Per ulteriori informazioni, consulta the section called “Usa Amazon EC2 (o un'altra origine personalizzata)”. Per ulteriore assistenza, consulta il Centro assistenza di AWS.

<certificate-id>Messaggio di errore: Certificato: è usato da CloudFront

Problema: stai cercando di eliminare un certificato SSL/TLS dall'archivio certificati IAM e ricevi il messaggio «Certificate: <certificate-id>is being used by». CloudFront

Soluzione: ogni CloudFront distribuzione deve essere associata al CloudFront certificato predefinito o a un certificato personalizzato per utilizzare il SSL/TLS certificate. Before you can delete an SSL/TLS

certificate, you must either rotate the certificate (replace the current custom SSL/TLS certificate with another custom SSL/TLS certificate) or revert from using a custom SSL/TLS certificato predefinito. CloudFront Per risolvere questo problema, completa le fasi in una delle procedure seguenti:

- Ruota SSL/TLS i certificati
- Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront

Risoluzione dei problemi relativi ai codici di stato della risposta agli errori in CloudFront

Se CloudFront richiede un oggetto dall'origine e l'origine restituisce un codice di stato HTTP 4xx o 5xx, c'è un problema di comunicazione tra CloudFront e l'origine.

Questo argomento include anche i passaggi per la risoluzione dei problemi relativi a questi codici di stato quando si utilizza Lambda @Edge o CloudFront Functions.

Gli argomenti seguenti forniscono spiegazioni dettagliate delle potenziali cause alla base di queste risposte di errore e offrono step-by-step indicazioni su come diagnosticare e risolvere i problemi sottostanti.

Argomenti

- Codice di stato HTTP 400 (richiesta errata)
- Codice di stato HTTP 401 (Non autorizzato)
- Codice di stato HTTP 403 (Metodo non valido)
- Codice di stato HTTP 403 (Autorizzazione negata)
- Codice di stato HTTP 404 (Non trovato)
- Codice di stato HTTP 412 (Precondizione non riuscita)
- Codice di stato HTTP 500 (Errore interno del server)
- Codice di stato HTTP 502 (Gateway non valido)
- Codice stato HTTP 503 (Servizio non disponibile)
- Codice di stato HTTP 504 (Timeout del gateway)

Codice di stato HTTP 400 (richiesta errata)

CloudFront restituisce una richiesta non valida 400 quando il client invia alcuni dati non validi nella richiesta, ad esempio contenuti mancanti o errati nel payload o nei parametri. Questo potrebbe anche rappresentare un errore generico del client.

L'origine Amazon S3 restituisce un errore 400

Se utilizzi un'origine Amazon S3 con la tua CloudFront distribuzione, questa potrebbe inviare risposte di errore con il codice di stato HTTP 400 Bad Request e un messaggio simile al seguente:

L'intestazione di autorizzazione non è valida; la regione '' è sbagliata; è prevista *<AWS Region>* '' *<AWS Region>*

Esempio:

The authorization header is malformed; the region 'us-east-1' is wrong; expecting 'us-west-2' (Intestazione di autorizzazione non corretta; la regione 'us-east-1' è errata; attesa 'us-west-2')

Questo problema può verificarsi nel seguente scenario:

1. L'origine della tua CloudFront distribuzione è un bucket Amazon S3.
2. Hai spostato il bucket S3 da una regione all'altra AWS . Cioè, hai eliminato il bucket S3, quindi successivamente hai creato un nuovo bucket con lo stesso nome di bucket, ma in una AWS regione diversa da quella in cui si trovava il bucket S3 originale.

Per correggere questo errore, aggiorna la CloudFront distribuzione in modo che trovi il bucket S3 nella regione corrente del bucket. AWS

Per aggiornare la tua distribuzione CloudFront

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere la distribuzione che causa questo errore.
3. Scegliere Origins and Origin Groups (Origini e gruppi di origini).
4. Individuare l'origine del bucket S3 spostato. Selezionare la casella di controllo accanto a questa origine, quindi scegliere Edit (Modifica).
5. Seleziona Yes, Edit (Sì, modifica). Non è necessario modificare alcuna impostazione prima di scegliere Yes, Edit (Sì, modifica).

Una volta completati questi passaggi, CloudFront ridistribuisce la distribuzione. Durante l'implementazione della distribuzione, nella colonna Data ultima modifica viene visualizzato lo stato Implementazione in corso. Qualche tempo dopo il completamento dell'implementazione, non si dovrebbero più ricevere risposte di errore `AuthorizationHeaderMalformed`.

L'origine Application Load Balancer restituisce un errore 400

Se utilizzi un'origine Application Load Balancer con la tua CloudFront distribuzione, le possibili cause di un errore 400 includono le seguenti:

- Il client ha inviato una richiesta con un formato errato che non soddisfa le specifiche HTTP.
- L'intestazione della richiesta supera il limite di 16 KB per riga di richiesta, 16 KB per singola intestazione o 64 KB per l'intera intestazione della richiesta.
- Il client ha chiuso la connessione prima di inviare l'intero corpo della richiesta.

Codice di stato HTTP 401 (Non autorizzato)

Un codice di stato della risposta 401 Non autorizzato indica che la richiesta del client non è stata completata perché mancano credenziali di autenticazione valide per la risorsa richiesta. Questo codice di stato viene inviato con un'intestazione di risposta `WWW-Authenticate` HTTP che contiene informazioni su come il client può richiedere nuovamente la risorsa dopo aver eseguito il prompt all'utente delle credenziali di autenticazione. Per ulteriori informazioni, consulta 401 Non autorizzato.

In CloudFront, se l'origine prevede che un'`Authorization`intestazione autentichi le richieste, CloudFront deve inoltrare l'`Authorization`intestazione all'origine per evitare un errore 401 Unauthorized. Quando CloudFront inoltra una richiesta di visualizzazione all'origine, per impostazione predefinita CloudFront rimuove alcune intestazioni del visualizzatore, inclusa l'intestazione. `Authorization` Per assicurarti che l'origine riceva sempre l'intestazione `Authorization` nelle richieste di origine, sono disponibili le seguenti opzioni:

- Aggiungi l'intestazione `Authorization` alla chiave della cache utilizzando una policy della cache. Tutte le intestazioni nella chiave cache vengono incluse automaticamente nelle richieste di origine. Per ulteriori informazioni, consulta Controllo della chiave della cache con una policy.
- Utilizzare una policy di richiesta di origine che inoltra tutte le intestazioni del visualizzatore all'origine. Non puoi inoltrare l'`Authorization`intestazione singolarmente in una policy di richiesta di origine, ma quando inoltri tutte le intestazioni del visualizzatore, CloudFront include l'intestazione nelle richieste dei `Authorization` visualizzatori. CloudFrontfornisce la politica di richiesta di

`AllViewer` origine gestita per questo caso d'uso. Per ulteriori informazioni, consulta Utilizzo delle policy di richiesta origine gestite.

Per ulteriori informazioni, vedi Come posso configurare CloudFront per inoltrare l'intestazione di autorizzazione all'origine?

Codice di stato HTTP 403 (Metodo non valido)

CloudFront restituisce un errore 403 (metodo non valido) se stai cercando di utilizzare un metodo HTTP che non hai specificato nella distribuzione. CloudFront Puoi specificare una delle seguenti opzioni per la distribuzione:

- CloudFront solo `GET` inoltri e richieste. `HEAD`
- CloudFront solo inoltri `GET` e `HEAD` `OPTIONS` richieste.
- CloudFront inoltri`GET`,`HEAD`,`OPTIONS`, `PUT` `PATCH``POST`, e `DELETE` richieste. Se selezioni questa opzione, potrebbe essere necessario limitare l'accesso al bucket Amazon S3 o all'origine personalizzata in modo che gli utenti non possano eseguire operazioni non desiderate. Ad esempio, è possibile che gli utenti non sia autorizzati a eliminare oggetti dall'origine.

Codice di stato HTTP 403 (Autorizzazione negata)

Un errore HTTP 403 indica che il client non è autorizzato ad accedere alla risorsa richiesta. Il client comprende la richiesta, ma non può autorizzare l'accesso del visualizzatore. Di seguito sono riportate le cause più comuni della CloudFront restituzione di questo codice di stato:

Argomenti

- Il CNAME alternativo è configurato in modo errato
- AWS WAF è configurato sulla CloudFront distribuzione o all'origine
- L'origine personalizzata restituisce un errore 403
- L'origine Amazon S3 restituisce un errore 403
- Le restrizioni geografiche restituiscono un errore 403
- La configurazione dell'URL o del cookie firmato restituisce un errore 403
- Le distribuzioni in pila causano un errore 403

Il CNAME alternativo è configurato in modo errato

Verifica di aver specificato il CNAME corretto per la distribuzione. Per utilizzare un CNAME alternativo anziché l'URL predefinito CloudFront :

1. Crea un record CNAME nel tuo DNS per indirizzare il CNAME all'URL di distribuzione. CloudFront
2. Aggiungi il CNAME nella tua configurazione di distribuzione. CloudFront

Se crei il record DNS ma non aggiungi il CNAME nella configurazione di CloudFront distribuzione, la richiesta restituisce un errore 403. Per ulteriori informazioni sulla configurazione di un CNAME personalizzato, consulta Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs.

AWS WAF è configurato sulla CloudFront distribuzione o all'origine

Quando si AWS WAF trova tra il client e CloudFront, non è CloudFront possibile distinguere tra un codice di errore 403 restituito dall'origine e un codice di errore 403 restituito da AWS WAF quando una richiesta viene bloccata.

Per trovare l'origine del codice di stato 403, controlla la regola della lista di controllo degli accessi AWS WAF Web (ACL) per una richiesta bloccata. Per ulteriori informazioni, consulta i seguenti argomenti:

- AWS WAF elenchi di controllo degli accessi web (web) ACLs
- Test e ottimizzazione delle protezioni AWS WAF

L’origine personalizzata restituisce un errore 403

Se utilizzi un’origine personalizzata, potresti ricevere un errore 403 se disponi di una configurazione firewall personalizzata a livello di origine. Per risolvere il problema, invia la richiesta direttamente all’origine. Se riesci a replicare l'errore senza farlo CloudFront, allora l'origine sta causando l'errore 403.

Se l’origine personalizzata causa l’errore, controlla i log dell’origine per identificare la causa dell’errore. Per ulteriori informazioni, consulta i seguenti argomenti relativi alla risoluzione dei problemi:

- Come posso risolvere gli errori HTTP 403 da Gateway API?
- Come posso risolvere gli errori vietati HTTP 403 di Application Load Balancer?

L'origine Amazon S3 restituisce un errore 403

L'errore 403 può essere visualizzato per i seguenti motivi:

- CloudFront non ha accesso al bucket Amazon S3. Questo può accadere se l'identità di accesso origine (OAI) o il controllo di accesso origine (OAC) non sono abilitati per la distribuzione e il bucket è privato.
- Il percorso specificato nell'URL richiesto non è corretto.
- L'oggetto richiesto non esiste.
- L'intestazione dell'host è stata inoltrata con l'endpoint REST API. Per ulteriori informazioni, consulta Specifica del bucket nell'intestazione HTTP Host nella Guida per l'utente di Amazon Simple Storage Service.
- Hai configurato le pagine di errore personalizzate. Per ulteriori informazioni, consulta In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate.

Le restrizioni geografiche restituiscono un errore 403

Se hai abilitato le restrizioni geografiche (note anche come geoblocking) per impedire agli utenti in aree geografiche specifiche di accedere ai contenuti che stai distribuendo tramite una CloudFront distribuzione, gli utenti bloccati ricevono un errore 403.

Per ulteriori informazioni, consulta Limitazione della distribuzione geografica del contenuto.

La configurazione dell'URL o del cookie firmato restituisce un errore 403

Se hai abilitato l'opzione Limita l'accesso degli spettatori per la configurazione del comportamento della tua distribuzione, le richieste che non utilizzano cookie firmati o firmati generano un URLs errore 403. Per ulteriori informazioni, consulta i seguenti argomenti:

- Offri contenuti privati con cookie firmati URLs e firmati
- Come posso risolvere i problemi relativi a un URL firmato o ai cookie registrati? CloudFront

Le distribuzioni in pila causano un errore 403

Se sono presenti due o più distribuzioni all'interno di una catena di richieste all'endpoint di origine, CloudFront restituisce un errore 403. Si sconsiglia di posizionare una distribuzione davanti a un'altra.

Codice di stato HTTP 404 (Non trovato)

CloudFront restituisce un errore 404 (Not Found) quando il client tenta di accedere a una risorsa che non esiste. Se ricevete questo errore con la vostra CloudFront distribuzione, le cause più comuni includono le seguenti:

- La risorsa non esiste.
- L'URL non è corretto.
- Origine personalizzata che restituisce un errore 404.
- Pagine di errore personalizzate che restituiscono un errore 404. Qualsiasi codice di errore potrebbe essere tradotto in 404. Per ulteriori informazioni, consulta In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate.
- Pagina di errore personalizzata eliminata accidentalmente, con conseguente errore 404 perché la richiesta cerca la pagina di errore personalizzata eliminata. Per ulteriori informazioni, consulta Come CloudFront elabora gli errori se non hai configurato pagine di errore personalizzate.
- Percorso di origine errato. Se il percorso di origine è compilato, il relativo valore viene aggiunto al percorso di ciascuna richiesta proveniente dal browser prima che la richiesta venga inoltrata all'origine. Per ulteriori informazioni, consulta Percorso origine.

Codice di stato HTTP 412 (Precondizione non riuscita)

CloudFront restituisce un codice di errore 412 (Precondition Failed) quando l'accesso alla risorsa di destinazione è stato negato. In alcuni casi, un server è configurato per accettare richieste solo dopo che sono state soddisfatte determinate condizioni. Se una delle condizioni specificate non è soddisfatta, il server non consente al client di accedere alla risorsa specificata. Invece, il server risponde con un codice di errore 412.

Le cause più comuni di un errore 412 includono: CloudFront

- Richieste condizionali su metodi diversi da `GET` o `HEAD` quando la condizione definita dalle intestazioni `If-Unmodified-Since` o `If-None-Match` non è soddisfatta. In tal caso, la richiesta, in genere un caricamento o una modifica di una risorsa, non può essere effettuata.
- Una condizione in uno o più campi di richiesta nell'operazione CloudFront UpdateDistributionAPI viene valutata come falsa.

Codice di stato HTTP 500 (Errore interno del server)

Un codice di stato HTTP 500 (Errore interno del server) indica che il server ha riscontrato una condizione imprevista che gli ha impedito di soddisfare la richiesta. Di seguito sono riportate alcune delle cause più comuni di 500 errori in Amazon CloudFront.

Argomenti

Il server Origin restituisce l'errore 500 a CloudFront

Il tuo server di origine potrebbe restituire un errore 500 a CloudFront. Per ulteriori informazioni, consulta i seguenti argomenti relativi alla risoluzione dei problemi:

- Se Amazon S3 restituisce un errore 500, consulta Come faccio a risolvere un errore HTTP 500 o 503 di Amazon S3?
- Se Gateway API restituisce un errore 500, consulta Come posso risolvere gli errori 5xx per REST API di Gateway API?.
- Se ELB restituisce un errore 500, consulta HTTP 500: errore interno del server nella User Guide for Application Load Balancers.

Se l'elenco precedente non risolve l'errore 500, il problema potrebbe riguardare un CloudFront punto di presenza che restituisce un errore interno del server. Puoi contattare Supporto per ricevere assistenza.

Codice di stato HTTP 502 (Gateway non valido)

CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) quando CloudFront non è stato in grado di servire l'oggetto richiesto perché non è riuscito a connettersi al server di origine.

Se utilizzi Lambda@Edge, il problema potrebbe essere un errore di convalida Lambda. Se ricevi un errore HTTP 502 con il codice di `NonS3OriginDnsError` errore, probabilmente c'è un problema di configurazione DNS che CloudFront impedisce la connessione all'origine.

Argomenti

- Il certificato SSL/TLS sull'origine è scaduto, non valido, autofirmato oppure l'ordine della catena di certificati non è corretto
- L'origine non risponde sulle porte specificate nelle impostazioni dell'origine
- Errore di convalida Lambda
- CloudFront errore di convalida della funzione
- Errore DNS (NonS3OriginDnsError)
- Errore 502 dell'origine Application Load Balancer
- Errore 502 dell'origine Gateway API

Errore di negoziazione SSL/TLS tra e un server di origine personalizzato CloudFront

Se utilizzi un'origine personalizzata che richiede HTTPS tra CloudFront e la tua origine, i nomi di dominio non corrispondenti potrebbero causare errori. Il SSL/TLS certificato di origine deve includere un nome di dominio che corrisponda al dominio di origine specificato per la CloudFront distribuzione o all'`Host`intestazione della richiesta di origine.

Se i nomi di dominio non corrispondono, l' SSL/TLS handshake ha esito negativo e CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) e imposta l'`X-Cache`intestazione su. `Error from cloudfront`

Per determinare se i nomi di dominio nel certificato corrispondono a Dominio origine nella distribuzione o nell'intestazione `Host`, puoi utilizzare uno strumento di verifica SSL online o OpenSSL. Se i nomi di dominio non corrispondono, hai due opzioni:

- Ottieni un nuovo SSL/TLS certificato che includa i nomi di dominio applicabili.

  Se utilizzi AWS Certificate Manager (ACM), consulta Richiesta di un certificato pubblico nella Guida per l'AWS Certificate Manager utente per richiedere un nuovo certificato.
- Modifica la configurazione di distribuzione in modo che CloudFront non tenti più di utilizzare SSL per connetterti con la tua origine.

Strumento di verifica SSL online

Per trovare uno strumento di verifica SSL, cerca "online ssl checker" su Internet. In genere, si specifica il nome del dominio e lo strumento restituisce una serie di informazioni sul SSL/TLS certificato. Conferma che il certificato contiene il tuo nome di dominio nel campo Nomi comuni o Nomi alternativi oggetto.

OpenSSL

Per aiutare a risolvere gli errori HTTP 502 di CloudFront, puoi usare OpenSSL per provare a stabilire una connessione al tuo server di origine. SSL/TLS Se OpenSSL non è in grado di effettuare una connessione è possibile che vi sia un problema con la configurazione SSL/TLS del server di origine. Se OpenSSL è in grado di stabilire una connessione, restituisce le informazioni sul certificato del server di origine, inclusi il nome comune (campo `Subject CN`) del certificato e il nome alternativo dell'oggetto (campo `Subject Alternative Name`).

Usa il seguente comando OpenSSL per testare la connessione al tuo server di origine (*origin domain*sostituiscilo con il nome di dominio del server di origine, ad esempio example.com):

```
openssl s_client -connect origin domain name:443
```

Se sono vere le seguenti condizioni:

- Il server di origine supporta più nomi di dominio con più certificati SSL/TLS
- La distribuzione è configurata per inoltrare l'intestazione `Host` all'origine

Quindi aggiungi l'`-servername`opzione al comando OpenSSL, come nell'esempio seguente (*CNAME*sostituisci con il CNAME configurato nella tua distribuzione):

```
openssl s_client -connect origin domain name:443 -servername CNAME
```

L'origine non risponde con crittografie/protocolli supportati

CloudFront si connette ai server di origine utilizzando cifrari e protocolli. Per un elenco dei cifrari e dei protocolli supportati CloudFront , vedere. the section called “Protocolli e cifrari supportati tra e l'origine CloudFront ” Se l'origine non risponde con uno di questi codici o protocolli nello scambio SSL/TLS, non riesce a connettersi. CloudFront Puoi verificare che la tua origine supporta protocolli e le crittografie utilizzando un tool online come SSL Labs. Digita il nome di dominio dell'origine nel campo Hostname (Nome host), quindi scegli Submit (Invia). Esamina i campi Common names (Nomi comuni) e Alternative names (Nomi alternativi) del test per sapere se corrispondono al nome di dominio dell'origine. Al termine del test, trova le sezioni Protocols (Protocolli) e Cipher Suites (Pacchetti crittografia) nei risultati del test per sapere quali crittografie o protocolli sono supportati dalla tua origine. Confrontali con l'elenco in the section called “Protocolli e cifrari supportati tra e l'origine CloudFront ”.

Il certificato SSL/TLS sull'origine è scaduto, non valido, autofirmato oppure l'ordine della catena di certificati non è corretto

Se il server di origine restituisce quanto segue, CloudFront interrompe la connessione TCP, restituisce il codice di stato HTTP 502 (Bad Gateway) e imposta l'intestazione su: `X-Cache Error from cloudfront`

- Certificato scaduto
- Certificato non valido
- Certificato autofirmato
- Ordine della catena di certificati non corretto

> **Note**
>
> Se l'intera catena di certificati, incluso il certificato intermedio, non è presente, la connessione TCP viene interrotta CloudFront .

Per informazioni sull'installazione di un SSL/TLS certificato sul server di origine personalizzato, consulta. the section called “Richiesta di HTTPS a un’origine personalizzata”

L'origine non risponde sulle porte specificate nelle impostazioni dell'origine

Quando crei un'origine sulla tua CloudFront distribuzione, puoi impostare le porte con cui CloudFront si connette all'origine per il traffico HTTP e HTTPS. Per impostazione predefinita, queste porte sono TCP 80/443. Hai comunque la possibilità di modificare queste porte. Se la tua origine rifiuta il traffico su queste porte per qualsiasi motivo o se il tuo server di backend non risponde sulle porte, non CloudFront riuscirà a connettersi.

Per risolvere questi problemi, verifica tutti i firewall in esecuzione nell'infrastruttura e assicurati che non blocchino gli intervalli di indirizzi IP. Per ulteriori informazioni, consulta Intervalli di indirizzi IP AWS nella Guida per l’utente di Amazon VPC. Inoltre, verifica se il server Web è in esecuzione sull'origine.

Errore di convalida Lambda

Se utilizzi Lambda@Edge, un codice di stato HTTP 502 può indicare che la risposta della funzione Lambda non è stata correttamente formata o che include contenuti non validi. Per ulteriori

informazioni sulla risoluzione di errori Lambda@Edge, consulta Test e debug delle funzioni Lambda@Edge.

CloudFront errore di convalida della funzione

Se utilizzi CloudFront funzioni, un codice di stato HTTP 502 può indicare che la CloudFront funzione sta tentando di aggiungere, eliminare o modificare un'intestazione di sola lettura. Questo errore non viene visualizzato durante il test, ma verrà visualizzato dopo aver distribuito la funzione ed eseguito la richiesta. Per risolvere questo errore, controlla e aggiorna la tua funzione. CloudFront Per ulteriori informazioni, consulta Aggiornamento delle funzioni.

Errore DNS (**`NonS3OriginDnsError`**)

Un errore HTTP 502 con il codice `NonS3OriginDnsError` di errore indica che esiste un problema di configurazione DNS che CloudFront impedisce la connessione all'origine. Se ricevi questo errore da CloudFront, assicurati che la configurazione DNS dell'origine sia corretta e funzionante.

Quando CloudFront riceve una richiesta per un oggetto scaduto o non presente nella cache, invia una richiesta all'origine per ottenere l'oggetto. Per effettuare una richiesta corretta all'origine, CloudFront esegue una risoluzione DNS sul dominio di origine. Se il servizio DNS per il tuo dominio presenta problemi, non CloudFront riesci a risolvere il nome di dominio per ottenere l'indirizzo IP, generando un errore HTTP 502 (). `NonS3OriginDnsError` Per risolvere il problema, contatta il tuo provider DNS oppure, se utilizzi Amazon Route 53, consulta Perché non riesco ad accedere al mio sito Web che utilizza i servizi DNS di Route 53?

Per risolvere il problema, accertati inoltre che i server dei nomi autorevoli del dominio root o dell'apex di zona dell'origine (ad esempio `example.com`) funzionino correttamente. Puoi usare i seguenti comandi per trovare i server dei nomi per l'origine apex, con uno strumento come dig o nslookup:

```
dig OriginAPEXDomainName NS +short
```

```
nslookup -query=NS OriginAPEXDomainName
```

Quando disponi dei nomi del server dei nomi, utilizza i comandi seguenti per eseguire una query sul nome di dominio dell'origine in base a tali nomi per assicurarti che ognuno risponda:

```
dig OriginDomainName @NameServer
```

```
nslookup OriginDomainName NameServer
```

> **Important**
>
> Assicurati di eseguire questa risoluzione dei problemi DNS utilizzando un computer connesso alla rete Internet pubblica. CloudFront risolve il dominio di origine utilizzando DNS pubblico su Internet, quindi è importante risolvere i problemi in un contesto simile.

Se l'origine è un dominio secondario la cui autorità DNS è delegata a un server di nomi diverso dal dominio principale, assicurati che il record del server dei nomi (`NS`) e il record di origine di autorità (`SOA`) siano configurati correttamente per il dominio secondario. È possibile verificare la presenza di questi record utilizzando comandi simili agli esempi precedenti.

Per ulteriori informazioni sul DNS, consulta i concetti del sistema dei nomi di dominio (DNS) nella documentazione di Amazon Route 53.

Errore 502 dell'origine Application Load Balancer

Se utilizzi Application Load Balancer come origine e ricevi un errore 502, consulta Come posso risolvere i problemi relativi agli errori HTTP 502 del mio Application Load Balancer?.

Errore 502 dell'origine Gateway API

Se utilizzi API Gateway e ricevi un errore 502, vedi Come posso risolvere gli errori HTTP 502 da API Gateway REST con l'integrazione del proxy APIs Lambda? .

Codice stato HTTP 503 (Servizio non disponibile)

Un codice di stato HTTP 503 (Servizio non disponibile) in genere indica un problema di prestazioni sul server di origine. In rari casi, indica che CloudFront temporaneamente non è possibile soddisfare una richiesta a causa di vincoli di risorse in una posizione periferica.

Se utilizzi Lambda @Edge o CloudFront Functions, il problema potrebbe essere un errore di esecuzione o un errore Lambda @Edge in cui è stato superato il limite.

Argomenti

- Il server di origine non dispone di capacità sufficiente per supportare la frequenza delle richieste
- CloudFront ha causato l'errore a causa di vincoli di risorse nell'edge location
- Lambda @Edge o errore di esecuzione CloudFront della funzione

- Limite Lambda@Edge superato

Il server di origine non dispone di capacità sufficiente per supportare la frequenza delle richieste

Quando un server di origine non è disponibile o non è in grado di soddisfare le richieste in arrivo, restituisce un codice di stato HTTP 503 (servizio non disponibile). CloudFront quindi inoltra l'errore all'utente. Per risolvere questo problema, prova le seguenti soluzioni:

- Se utilizzi Amazon S3 come server di origine:
  - Puoi inviare 3.500 PUT/COPY/POST/DELETE or 5,500 GET/HEAD richieste al secondo per prefisso Amazon S3 partizionato. Quando Amazon S3 restituisce una risposta 503 Slow Down, ciò indica in genere un tasso di richieste eccessivo rispetto a un prefisso Amazon S3 specifico.

    Poiché le frequenze di richieste si applicano per prefisso in un bucket S3, gli oggetti devono essere distribuiti su più prefissi. Man mano che la frequenza di richieste sui prefissi aumenta gradualmente, Amazon S3 aumenta verticalmente per gestire separatamente le richieste per ciascuno dei prefissi. Di conseguenza, la frequenza di richieste complessiva gestita dal bucket è un multiplo del numero di prefissi.
  - Per maggiori informazioni, consulta la sezione Ottimizzazione delle prestazioni di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.
- Se utilizzi ELB come server di origine:
  - Assicurati che le istanze di backend siano in grado di rispondere ai controlli dell'integrità.
  - Assicurati che il bilanciatore del carico e le istanze di backend siano in grado di gestire il carico.

  Per ulteriori informazioni, consulta:
  - Come posso risolvere gli errori 503 che ricevo quando utilizzo un Classic Load Balancer?
  - Come posso risolvere gli errori 503 (servizio non disponibile) dal mio Application Load Balancer?
- Se utilizzi un'origine personalizzata:
  - Esamina i log dell'applicazione per accertarti che l'origine disponga di risorse sufficienti, ad esempio CPU, memoria e spazio su disco.
  - Se utilizzi Amazon EC2 come backend, assicurati che il tipo di istanza disponga delle risorse appropriate per soddisfare le richieste in arrivo. Per ulteriori informazioni, consulta i tipi di istanza nella Amazon EC2 User Guide.
- Se utilizzi Gateway API:

- Questo errore è correlato all'integrazione backend quando l'API di Gateway API non è in grado di ricevere una risposta. Il server di backend potrebbe essere:
  - Sovraccaricato oltre la capacità e incapace di elaborare nuove richieste client.
  - In manutenzione temporanea.
- Per risolvere questo errore, esamina i log dell'applicazione Gateway API per determinare se esiste un problema con la capacità backend, l'integrazione o altro.

CloudFront ha causato l'errore a causa di vincoli di risorse nell'edge location

Riceverai questo errore nella rara situazione in cui non è CloudFront possibile indirizzare le richieste alla successiva migliore edge location disponibile e quindi non è in grado di soddisfare una richiesta. Questo errore è comune quando si eseguono test di carico sulle distribuzioni CloudFront. Per impedire che ciò accada, segui le linee guida the section called "Test di carico CloudFront" per evitare gli errori 503 (Capacità superata).

Se ciò dovesse verificarsi nell'ambiente di produzione, contatta Supporto.

Lambda @Edge o errore di esecuzione CloudFront della funzione

Se utilizzi Lambda @Edge o CloudFront Functions, un codice di stato HTTP 503 può indicare che la funzione ha restituito un errore di esecuzione.

Per ulteriori dettagli su come identificare e risolvere gli errori Lambda@Edge, consulta Test e debug delle funzioni Lambda@Edge.

Per ulteriori informazioni sul test delle CloudFront funzioni, consulta. Test delle funzioni

Limite Lambda@Edge superato

Se utilizzi Lambda@Edge, un codice di stato HTTP 503 può indicare che Lambda ha restituito un errore. Questo errore potrebbe essere causato da uno dei seguenti motivi.

- Il numero di esecuzioni di funzioni ha superato una delle quote impostate da Lambda per limitare le esecuzioni in un Regione AWS (esecuzioni simultanee o frequenza di invocazione).
- La funzione ha superato la quota di timeout della funzione Lambda.

Per ulteriori informazioni sulle quote Lambda@Edge, consulta Quote di Lambda@Edge. Per ulteriori dettagli su come identificare e risolvere gli errori Lambda@Edge, consulta the section called "Test

e debug". Puoi anche consultare le Service Quotas Lambda nella Guida per gli sviluppatori di AWS Lambda .

Codice di stato HTTP 504 (Timeout del gateway)

Un codice di stato HTTP 504 (timeout del gateway) indica che quando viene CloudFront inoltrata una richiesta all'origine (poiché l'oggetto richiesto non era nella cache edge), si verificava una delle seguenti situazioni:

- L'origine ha restituito un codice di stato HTTP 504 a. CloudFront
- L'origine non ha risposto prima della scadenza della richiesta.

CloudFront restituirà un codice di stato HTTP 504 se il traffico verso l'origine è bloccato da un firewall o da un gruppo di sicurezza o se l'origine non è accessibile su Internet. Verifica prima se ci sono questi problemi. Quindi, se il problema non è l'accesso, concentrati sui ritardi delle applicazioni e i timeout dei server per identificare e risolvere i problemi.

Argomenti

- Configura il firewall sul tuo server di origine per consentire il traffico CloudFront
- Configura i gruppi di sicurezza sul tuo server di origine per consentire il traffico CloudFront
- Rendere accessibile su Internet il proprio server di origine personale
- Trovare e correggere il ritardo nelle risposte dalle applicazioni sul server di origine

Configura il firewall sul tuo server di origine per consentire il traffico CloudFront

Se il firewall sul server di origine blocca il CloudFront traffico, CloudFront restituisce un codice di stato HTTP 504, quindi è bene assicurarsi che non sia questo il problema prima di verificare la presenza di altri problemi.

Il metodo utilizzato per determinare se si tratta di un problema con il tuo firewall dipende da quale sistema utilizza il tuo server di origine:

- Se utilizzi un IPTable firewall su un server Linux, puoi cercare strumenti e informazioni con IPTables cui lavorare.
- Se utilizzi Windows Firewall su un server Windows, consulta Add or Edit Firewall Rule (Aggiungere o modificare una regola del firewall) nella documentazione Microsoft.

Quando valuti la configurazione del firewall sul tuo server di origine, cerca eventuali firewall o regole di sicurezza che blocchino il traffico proveniente dalle CloudFront edge location, in base all'intervallo di indirizzi IP pubblicato. Per ulteriori informazioni, consulta Ubicazioni e intervalli di indirizzi IP dei server edge di CloudFront.

Se l'intervallo di indirizzi CloudFront IP può connettersi al server di origine, assicurati di aggiornare le regole di sicurezza del server per incorporare le modifiche. È possibile eseguire la sottoscrizione a un argomento Amazon SNS e ricevere notifiche quando il file dell'intervallo di indirizzi IP viene aggiornato. Dopo avere ricevuto la notifica, puoi utilizzare il codice per recuperare il file, analizzarlo e apportare le modifiche necessarie per l'ambiente locale. Per ulteriori informazioni, consulta Abbonarsi alle modifiche degli indirizzi IP AWS pubblici tramite Amazon SNS nel AWS News Blog.

Configura i gruppi di sicurezza sul tuo server di origine per consentire il traffico CloudFront

Se la tua origine utilizza Elastic Load Balancing, esamina i gruppi di sicurezza ELB e assicurati che i gruppi di sicurezza consentano il traffico in entrata da. CloudFront

Puoi anche utilizzarli AWS Lambda per aggiornare automaticamente i tuoi gruppi di sicurezza per consentire il traffico in entrata da. CloudFront

Rendere accessibile su Internet il proprio server di origine personale

Se non CloudFront riesci ad accedere al tuo server di origine personalizzato perché non è disponibile pubblicamente su Internet, CloudFront restituisce un errore HTTP 504.

CloudFront le edge location si connettono ai server di origine tramite Internet. Se l'origine personalizzata si trova su una rete privata, non è CloudFront possibile raggiungerla. Per questo motivo, non puoi utilizzare server privati, compresi i Classic Load Balancer interni, come server di origine con. CloudFront

Per verificare che il traffico Internet possa connettersi al server di origine, esegui i seguenti comandi (*`OriginDomainName`*dov'è il nome di dominio del server):

Per il traffico HTTPS:

- nc -zv 443 *`OriginDomainName`*
- *`OriginDomainName`*telnet 443

Per il traffico HTTP:

- cnc -zv 80 *OriginDomainName*
- telnet 80 *OriginDomainName*

Trovare e correggere il ritardo nelle risposte dalle applicazioni sul server di origine

I timeout del server sono spesso il risultato di un tempo di risposta molto lungo da parte di un'applicazione o di un valore di timeout impostato troppo basso.

Una soluzione rapida per evitare errori HTTP 504 è semplicemente quella di impostare un valore di timeout CloudFront più alto per la distribuzione. Tuttavia, ti consigliamo di verificare innanzitutto come risolvere eventuali problemi di prestazioni e latenza con l'applicazione e il server di origine. Quindi puoi impostare un valore di timeout ragionevole che aiuta a prevenire gli errori HTTP 504 e fornisce una buona reattività agli utenti.

Ecco una panoramica delle fasi che puoi eseguire per individuare i problemi di prestazioni e correggerli:

1. Misura la latenza tipica e a elevato carico (reattività) della tua applicazione Web.
2. Aggiungi risorse aggiuntive, ad esempio CPU o memoria, se necessario. Adotta altre misure per risolvere i problemi, ad esempio il tuning delle query del database in base a scenari a elevato carico.
3. Se necessario, regolate il valore di timeout per la vostra CloudFront distribuzione.

Di seguito sono riportati i dettagli di ciascuna fase.

Misura la latenza tipica e a elevato carico

Per determinare se uno o più server di applicazioni Web back-end riscontri elevata latenza, esegui il seguente comando curl Linux su ciascun server:

```
curl -w "DNS Lookup Time: %{time_namelookup} \nConnect time: %{time_connect}
 \nTLS Setup: %{time_appconnect} \nRedirect Time: %{time_redirect} \nTime to first
 byte: %{time_starttransfer} \nTotal time: %{time_total} \n" -o /dev/null https://
www.example.com/yourobject
```

> **Note**
>
> Se esegui Windows sui server, puoi cercare e scaricare curl per Windows per eseguire un comando simile.

Quando misuri e valuti la latenza di un'applicazione che viene eseguita sul server, tieni presente quanto segue:

- I valori di latenza sono relativi a ogni applicazione. Tuttavia, un Time to First Byte (Tempo per il primo byte) in millisecondi anziché secondi o più, è più sensato.
- Se misuri la latenza dell'applicazione sotto carico normale e non presenta problemi, tieni presente che i visualizzatori potrebbero ancora avere timeout sotto carico elevato. Quando la richiesta è elevata, i server possono avere risposte ritardate o non rispondere affatto. Per prevenire problemi di latenza a causa di un elevato carico, verifica le risorse del server, quali CPU, memoria e letture e scritture sul disco per assicurarti che i server abbiano la capacità di dimensionarsi per un carico elevato.

  Puoi eseguire il seguente comando Linux per verificare la memoria utilizzata dai processi Apache:

  ```
  watch -n 1 "echo -n 'Apache Processes: ' && ps -C apache2 --no-headers | wc -l && free -m"
  ```
- L'elevato utilizzo della CPU sul server può ridurre in modo significativo le prestazioni di un'applicazione. Se utilizzi un' EC2 istanza Amazon per il tuo server di backend, esamina i CloudWatch parametri del server per verificare l'utilizzo della CPU. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide. Oppure, se utilizzi il tuo server, fai riferimento alla documentazione della Guida del server per istruzioni su come verificare l'utilizzo della CPU.
- Verifica la presenza di altri potenziali problemi in presenza di carichi elevati, ad esempio query del database che vengono eseguite lentamente in presenza di un elevato volume di richieste.

Aggiungi le risorse e ottimizza i server e i database

Dopo aver valutato la reattività delle applicazioni e dei server, assicurati di disporre di risorse sufficienti per le situazioni di traffico tipiche e a elevato carico:

- Se disponi di un tuo server, assicurati che abbia CPU, memoria e spazio su disco sufficiente per gestire le richieste del visualizzatore, in base alla tua valutazione

- Se utilizzi un' EC2 istanza Amazon come server di backend, assicurati che il tipo di istanza disponga delle risorse appropriate per soddisfare le richieste in arrivo. Per ulteriori informazioni, consulta i tipi di istanza nella Amazon EC2 User Guide.

Inoltre, considera le seguenti fasi di tuning per evitare timeout:

- Se il valore Time to First Byte (Tempo per il primo byte) restituito dal comando curl sembra alto, adotta le misure necessarie per migliorare le prestazioni dell'applicazione. Il miglioramento della reattività delle applicazioni contribuirà a sua volta a ridurre gli errori di timeout.
- Esegui il tuning delle query del database per assicurarti che siano in grado di gestire volumi di richieste elevate senza rallentare le prestazioni.
- Configura le connessioni keep-alive (persistenti) sul tuo server di back-end. Questa opzione aiuta a evitare le latenze che si verificano quando le connessioni devono essere ristabilite per le richieste o per gli utenti successivi.
- Se utilizzi ELB come origine, le possibili cause dell'errore 504 sono le seguenti:
  - Il bilanciatore del carico non è in grado di stabilire una connessione con la destinazione prima dello scadere del timeout della connessione (10 secondi).
  - Il bilanciatore del carico ha stabilito una connessione con la destinazione, ma la destinazione non ha risposto prima dello scadere del timeout di inattività.
  - La lista di controllo degli accessi alla rete (ACL) nella sottorete non ha consentito il traffico dalle destinazioni ai nodi del bilanciatore del carico sulle porte temporanee (1024-65535).
  - La destinazione ha restituito un'intestazione content-length più grande del corpo dell'entità. Il bilanciatore del carico è scaduto in attesa di byte mancanti.
  - La destinazione è una funzione Lambda e Lambda non ha risposto prima della scadenza del timeout della connessione.

  Per ulteriori informazioni sulla riduzione della latenza, consulta Come posso risolvere i problemi di latenza elevata sul mio ELB Classic Load Balancer?
- Se utilizzi MediaTailor come origine, le possibili cause dell'errore 504 sono le seguenti:
  - Se un parente URLs viene maltrattato, MediaTailor può ricevere dei malformati URLs dai giocatori.
  - Se MediaPackage è l'origine manifesta di MediaTailor, MediaPackage 404 errori manifest possono causare MediaTailor la restituzione di un errore 504.
  - Il completamento della richiesta al server di MediaTailor origine richiede più di 2 secondi.

- Se utilizzi Gateway Amazon API come origine, le seguenti sono le possibili cause di un errore 504:
  - Una richiesta di integrazione richiede più tempo rispetto al parametro di timeout massimo di integrazione della REST API di Gateway API. Per ulteriori informazioni, consulta Come posso risolvere gli errori di timeout con codice di stato HTTP 504 di Gateway API?

Se necessario, modifica il valore di CloudFront timeout

Se hai valutato e risolto rallentamenti di prestazioni delle applicazioni, anomalie nella capacità del server di origine e altri problemi, ma i visualizzatori riscontrano ancora errori HTTP 504, considera la possibilità di modificare il tempo specificato nella distribuzione per il timeout della risposta del server di origine. Per ulteriori informazioni, consulta the section called “Timeout di risposta”.

Test di carico CloudFront

I metodi di test di carico tradizionali non funzionano bene CloudFront perché CloudFront utilizzano il DNS per bilanciare i carichi tra edge location geograficamente distribuite e all'interno di ciascuna edge location. Quando un client richiede contenuti da CloudFront, riceve una risposta DNS che include un set di indirizzi IP. Se esegui il test inviando le richieste a uno solo degli indirizzi IP restituiti dal DNS, stai testando solo un piccolo sottoinsieme delle risorse in un'unica CloudFront edge location, che non rappresenta accuratamente i modelli di traffico effettivi. A seconda del volume di dati richiesto, questo tipo di test può sovraccaricare e ridurre le prestazioni di quel piccolo sottoinsieme di server. CloudFront

CloudFront è progettato per adattarsi a utenti con indirizzi IP client diversi e resolver DNS diversi in più aree geografiche. Per eseguire test di carico che valutino accuratamente le CloudFront prestazioni, ti consigliamo di eseguire tutte le seguenti operazioni:

- Invia le richieste client da diverse regioni geografiche.
- Configura il test in modo che ogni client effettui una richiesta DNS indipendente. Ogni cliente riceverà quindi un diverso set di indirizzi IP dal DNS.
- Per ogni client che esegue le richieste, ripartisci le richieste client in tutto il set di indirizzi IP restituiti dal sistema DNS. Ciò garantisce che il carico venga distribuito su più server in una posizione CloudFront periferica.

Note

- Il test di carico non è consentito sui comportamenti cache con trigger di richiesta visualizzatore o risposta visualizzatore Lambda@Edge.
- Il test di carico non è consentito sulle origini con Origin Shield abilitato.

Quote

Puoi richiedere un aumento della CloudFront quota utilizzando le seguenti opzioni:

- Puoi utilizzare la console Service Quotas o AWS Command Line Interface. Per ulteriori informazioni, consulta i seguenti argomenti:
  - Richiesta di un aumento di quota nella Guida per l'utente di Service Quotas.
  - request-service-quota-increase in Riferimento ai comandi AWS CLI
- Se una CloudFront quota non è disponibile in Service Quotas, utilizza il caso AWS Support Center Console per creare un caso di aumento della quota di servizio.

CloudFront è soggetto alle seguenti quote.

Argomenti

Quote generali

Entità	Quota predefinita
Velocità di trasferimento dati per distribuzione (Questa quota non si applica alle distribuzioni sottoscritte a piani tariffari CloudFront forfettari. Per ulteriori informazioni, consulta.) ???	150 Gbps Richiedi una quota più elevata.
Richieste al secondo per distribuzione (Questa quota non si applica alle distribuzioni sottoscritte a piani CloudFront tariffari forfettari. Per ulteriori informazioni, consulta.) ???	250.000 Richiedi una quota più elevata.
Tag che possono essere aggiunti a una distribuzione	50 Richiedi una quota più elevata.
File che puoi fornire per la distribuzione	Nessuna quota
Lunghezza massima di una richiesta o di una risposta origine, incluse intestazioni e stringhe di query, ma escluso il contenuto del corpo.	20.480 byte
Lunghezza massima di un URL	8,192 byte
Numero massimo di configurazioni di consegna dei log di accesso in tempo reale per Account AWS	150
Numero massimo di associazioni per ACL web	100 Richiedi una quota più elevata.

Quote generali sulle distribuzioni

Entità	Quota predefinita
Nomi di dominio alternativi (CNAMEs) per distribuzione	100

Entità	Quota predefinita
Per ulteriori informazioni, consulta Utilizza la funzionalità personalizzata URLs aggiungendo nomi di dominio alternativi () CNAMEs.	Richiedi una quota più elevata.
Comportamenti cache per distribuzione	75 Richiedi una quota più elevata.
Tentativi di connessione per origine Per ulteriori informazioni, consulta Tentativi di connessione.	1-3
Timeout connessione per origine Per ulteriori informazioni, consulta Timeout di connessione.	1-10 secondi
Timeout di risposta per origine Questo è noto anche come timeout di lettura origine o timeout di richiesta origine. Per ulteriori informazioni, consulta Timeout di risposta.	1-120 secondi Richiedi una quota più elevata.
Timeout keep-alive per origine Per ulteriori informazioni, consulta Timeout keep-alive (solo origini personalizzate e VPC).	1-120 secondi Richiedi una quota più elevata.
Distribuzioni per Account AWS Per ulteriori informazioni, consulta Creazione di una distribuzione.	500 Richiedi una quota più elevata.
Distribuzioni per controllo di accesso origine	100 Richiedi una quota più elevata.
Distribuzioni all’interno della catena di richieste all’endpoint di origine Si sconsiglia di posizionare una distribuzione davanti a un’altra. Il superamento di questa quota comporta un errore 403.	2

Entità	Quota predefinita
Compressione dei file: gamma di dimensioni dei file che CloudFront vengono compressi Per ulteriori informazioni, consulta Distribuzione di file compressi.	Da 1.000 a 10.000.000 byte
Dimensione massima del file memorizzabile nella cache per risposta GET HTTP. Solo le risposte per un GET HTTP vengono memorizzate nella cache. Le risposte per POST o PUT non vengono memorizzate nella cache.	50 GB
Controlli di accesso Origin per Account AWS	100 Richiedi una quota più elevata.
Identità di accesso all'origine per Account AWS	100 Richiedi una quota più elevata.
Origini per distribuzione	100 Richiedi una quota più elevata.
Gruppi di origine per la distribuzione	10 Richiedi una quota più elevata.
Distribuzioni stagionali per Account AWS Per ulteriori informazioni, consulta the section called “Utilizzo dell’implementazione continua per testare in sicurezza le modifiche”.	20 Richiedi una quota più elevata.
Distribuzioni associate alla stessa origine VPC	50

Entità	Quota predefinita
Origini VPC per Account AWS	25 Richiedi una quota più elevata.
Numero massimo di distribuzioni che possono essere associate a un singolo elenco di indirizzi IP statici Anycast.	100 Richiedi una quota più elevata.

Quote generali sulle policy

Entità	Quota predefinita
Politiche di cache personalizzate per Account AWS (Non si applica alle politiche di cache CloudFront gestite)	20 Richiedi una quota più elevata.
Distribuzioni associate allo stesso criterio della cache	100
Stringhe di query per criterio della cache	10 Richiedi una quota più elevata.
Criterio intestazioni per cache	10 Richiedi una quota più elevata.
Cookie per criterio cache	10 Richiedi una quota più elevata.

Entità	Quota predefinita
Lunghezza totale combinata di tutti i nomi di stringhe di query, intestazioni e cookie in una policy della cache	1.024
Politiche di richiesta di origine personalizzate per Account AWS (Non si applica alle politiche di richiesta di origine CloudFront gestita)	20 Richiedi una quota più elevata.
Distribuzioni associate alla stessa policy di richiesta di origine	100
Stringhe di query per criterio di richiesta di origine	10 Richiedi una quota più elevata.
Criterio di richiesta di intestazione per origine	10 Richiedi una quota più elevata.
Criterio di richiesta dei cookie per origine	10 Richiedi una quota più elevata.
Lunghezza totale combinata di tutte le stringhe di query, intestazioni e nomi di cookie in una policy di richiesta di origine	1.024
Politiche di intestazioni di risposta personalizzate per Account AWS (Non si applica alle politiche di CloudFront gestione delle intestazioni di risposta)	20 Richiedi una quota più elevata.
Distribuzioni associate alla stessa policy delle intestazioni di risposta	100 Richiedi una quota più elevata.

Entità	Quota predefinita
Intestazioni personalizzate per policy delle intestazioni di risposta	10 Richiedi una quota più elevata.
Politiche di distribuzione continua per Account AWS	20 Richiedi una quota più elevata.

Quote su MTL e trust store

Entità	Quota predefinita
Trust stores per Account AWS	20 Richiedi una quota più elevata.
Distribuzioni per trust store	25
Dimensioni del pacchetto CA	64 KB Richiedi una quota più elevata.
Dimensione del certificato nel pacchetto CA	16384 Richiedi una quota più elevata.
Numero di certificati nel pacchetto CA	25
Profondità della catena del certificato	4

Quote sulle funzioni CloudFront

Entità	Quota predefinita
Funzioni per Account AWS	100
Dimensione massima della funzione Questa quota non è regolabile. Per memorizzare dati aggiuntivi per CloudFront le tue funzioni, crea un archivio di valori chiave e aggiungi le coppie chiave-valore. Per ulteriori informazioni, consulta Amazon CloudFront KeyValueStore.	10 KB
Memoria massima funzione	2 MB
Distribuzioni associate alla stessa funzione	100

Oltre a queste quote, esistono altre restrizioni quando si utilizzano le funzioni. CloudFront Per ulteriori informazioni, consulta Restrizioni sulle funzioni CloudFront.

Quote sulle funzioni di connessione

Entità	Quota predefinita
Funzioni di connessione per Account AWS Per ulteriori informazioni, consulta Richiedi un aumento della quota della funzione di connessione.	0
Dimensione massima della funzione di connessione Questa quota non è regolabile. Per memorizzare dati aggiuntivi per le funzioni di connessione, create un archivio di valori chiave e aggiunget e le coppie chiave-valore. Per ulteriori informazioni, consulta Amazon CloudFront KeyValueStore.	10 KB
Memoria massima per le funzioni di connessione	2 MB

Entità	Quota predefinita
Distribuzioni associate alla stessa funzione di connessione	100

Oltre a queste quote, esistono altre restrizioni quando si utilizzano le funzioni di connessione. Per ulteriori informazioni, consulta Associare una funzione di CloudFront connessione.

Quote sugli archivi di valori delle chiavi

Entità	Quota predefinita
Dimensione massima di una chiave in una coppia chiave-valore	512 byte
Dimensione massima del valore in una coppia chiave-valore	1 KB
Numero massimo di coppie chiave-valore aggiornabili in una singola richiesta API	50 tasti o un payload di 3 MB, a seconda di quale dei due valori viene raggiunto per primo
Dimensione massima di un singolo archivio di valori delle chiavi	5 MB
Numero massimo di funzioni a cui è possibile associare un singolo archivio di valori delle chiavi	10
Numero massimo di archivi di valori delle chiavi per funzione	1
Numero massimo di archivi di valori delle chiavi per account	50 Richiedi una quota più elevata.

Quote di Lambda@Edge

Quote generali

Entità	Quota predefinita
Le distribuzioni per Account AWS cui possono avere funzioni Lambda @Edge	500 Richiedi una quota più elevata.
Funzioni Lambda@Edge per distribuzione	100 Richiedi una quota più elevata.
Esecuzioni simultanee **Note** • AWS Lambda gestisce le quote di concorrenza per Lambda @Edge. Tutte le funzioni Lambda nella Regione AWS condi vidono questa quota. • Ti consigliamo di rivedere la quota di esecuzioni simultanee in tutte le aree da Regioni AWS cui prevedi che provengano le richieste degli spettatori. Inoltre, ogni istanza della funzione Lambda @Edge può servire fino a 10 richieste al secondo. Il limite totale di invocazioni è 10 volte il limite di concorrenza. Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per gli AWS Lambda sviluppatori: • Comprendere il ridimensionamento delle funzioni Lambda • Richieste API Lambda	1.000 (in ciascuna Regione AWS) Richiedi una quota più elevata.

Entità	Quota predefinita
Distribuzioni associate alla stessa funzione	500
Dimensione compressa massima di una funzione Lambda e delle eventuali librerie incluse	50 MB
Richieste Lambda@Edge al secondo (ciascuna Regione AWS supportata). Per ulteriori informazioni, consulta Quote di concorrenza nella Guida per gli sviluppatori di AWS Lambda .	10.000

Quote che differiscono per tipo di evento

Entità	Eventi di richiesta e risposta del visualizzatore	Eventi di richiesta e risposta origine
Dimensioni memoria della funzione	128 MB	Equivalente a Quote di Lambda.
Timeout della funzione. La funzione può effettuare chiamate di rete a risorse come bucket Amazon S3, tabelle DynamoDB o istanze Amazon in. EC2 Regioni AWS	30 secondi	30 secondi
Dimensione di una risposta generata da una funzione Lambda, inclusi intestazioni e corpo	40 KB	1 MB

Note

- Per un elenco di quote Lambda @Edge aggiuntive che possono essere aumentate da Service Quotas, consulta gli endpoint e le quote di CloudFront Amazon nel. Riferimenti generali di AWS

- Tieni inoltre presente che vi sono alcune altre restrizioni relative all'utilizzo delle funzioni Lambda@Edge. Per ulteriori informazioni, consulta Restrizioni su Lambda@Edge.

Quote sui certificati SSL

Entità	Quota predefinita
I certificati SSL si Account AWS adattano a quando si gestiscono richieste HTTPS utilizzando indirizzi IP dedicati (nessuna quota quando si gestiscono richieste HTTPS tramite SNI) Per ulteriori informazioni, consulta Usa HTTPS con CloudFront.	2 Richiedi una quota più elevata.
Certificati SSL che possono essere associati a una distribuzione CloudFront	1

Se il certificato SSL è specifico per la comunicazione HTTPS tra gli utenti e CloudFront se hai utilizzato AWS Certificate Manager (ACM) o l'archivio certificati IAM per fornire o importare il certificato, si applicano quote aggiuntive. Per ulteriori informazioni, consulta Quote sull'utilizzo di SSL/TLS certificati con CloudFront (HTTPS solo tra visualizzatori e CloudFront solo tra visualizzatori).

Sono previste anche quote sul numero di certificati SSL che puoi importare in AWS Certificate Manager (ACM) o caricare su (IAM). AWS Identity and Access Management Per ulteriori informazioni, consulta Aumento delle quote per certificati SSL/TLS.

Quote degli invalidamenti

Entità	Quota predefinita
Invalidamento dei file: numero massimo di file consentiti in richieste di invalidamento attive, esclusi gli invalidamenti generali Per ulteriori informazioni, consulta Invalidare i file per rimuovere il contenuto.	3.000

Entità	Quota predefinita
Invalidamento dei file: numero massimo di invalidamenti generali attivi consentiti	15
Invalidamento dei file: numero massimo dei file che un invalidamento generale può elaborare	Nessuna quota

Quote sui gruppi di chiavi

Entità	Quota predefinita
Chiavi pubbliche in un unico gruppo di chiavi	5 Richiedi una quota più elevata.
Gruppi di chiavi associati a un singolo comportamento della cache	4 Richiedi una quota più elevata.
Gruppi chiave per Account AWS	10 Richiedi una quota più elevata.
Distribuzioni associate a un singolo gruppo di chiavi	100 Richiedi una quota più elevata.

Quote sulle connessioni WebSocket

Entità	Quota predefinita
Timeout di risposta di origine (timeout di inattività)	10 minuti

Entità	Quota predefinita
	Se CloudFront non ha rilevato alcun byte inviato dall'origine al client negli ultimi 10 minuti, la connessione viene considerata inattiva e viene chiusa.

Quote della crittografia a livello di campo

Entità	Quota predefinita
Lunghezza massima di un campo da crittografare Per ulteriori informazioni, consulta Utilizzo della crittografia a livello di campo per la protezione dei dati sensibili.	16 KB
Numero massimo di campi nel corpo di una richiesta quando la crittografia a livello di campo è configurata	10
Lunghezza massima del corpo di una richiesta quando la crittografia a livello di campo è configurata	1 MB
Numero massimo di configurazioni di crittografia a livello di campo che possono essere associate a una Account AWS	10
Numero massimo di profili di crittografia a livello di campo che possono essere associati a uno Account AWS	10
Numero massimo di chiavi pubbliche che è possibile aggiungere a un Account AWS	10
Numero massimo di campi da crittografare che è possibile specificare in un profilo	10

Entità	Quota predefinita
Numero massimo di CloudFront distribuzioni che possono essere associate a una configurazione di crittografia a livello di campo	20
Numero massimo di mappature di profili di argomento di query che possono essere incluse in una configurazione di crittografia a livello di campo	5

Quote sui cookie (impostazioni della cache legacy)

Queste quote si applicano alle impostazioni CloudFront della cache legacy. Si consiglia di utilizzare una policy della cache o una policy di richiesta origine anziché le impostazioni legacy.

Entità	Quota predefinita
Cookie per il comportamento della cache Per ulteriori informazioni, consulta Caching dei contenuti basati su cookie.	10 Richiedi una quota più elevata.
Numero totale di byte nei nomi dei cookie (non si applica se si configura l'inoltro CloudFront di tutti i cookie all'origine)	512 meno il numero di cookie

Quote sulle stringhe di query (impostazioni della cache legacy)

Queste quote si applicano alle impostazioni CloudFront della cache legacy. Si consiglia di utilizzare una policy della cache o una policy di richiesta origine anziché le impostazioni legacy.

Entità	Quota predefinita
Numero massimo di caratteri in una stringa di query	128 caratteri
Numero massimo totale di caratteri per tutte le stringhe di query nello stesso parametro	512 caratteri
Stringhe di query per il comportamento della cache	10

Entità	Quota predefinita
Per ulteriori informazioni, consulta Memorizzazione nella cache di contenuti basati su parametri delle stringhe di query.	Richiedi una quota più elevata.

Quote delle intestazioni

Entità	Quota predefinita
Intestazioni per il comportamento della cache (impostazioni della cache legacy) Per ulteriori informazioni, consulta the section called “Caching dei contenuti in base alle intestazioni di richiesta”.	10 Richiedi una quota più elevata.
Inoltra intestazioni per il comportamento cache	25 Richiedi una quota più elevata.
Intestazioni personalizzate: numero massimo di intestazioni personalizzate che è possibile configurare CloudFront per l'aggiunta alle richieste di origine Per ulteriori informazioni, consulta the section called “Aggiunta di intestazioni personalizzate alle richieste di origine”.	30 Richiedi una quota più elevata.
Intestazioni personalizzate: numero massimo di intestazioni personalizzate che puoi aggiungere a una policy delle intestazioni di risposta	10 Richiedi una quota più elevata.
Intestazioni personalizzate: lunghezza massima di un nome di intestazione	256 caratteri
Intestazioni personalizzate: lunghezza massima di un valore di intestazione	1,783 caratteri

Entità	Quota predefinita
Intestazioni personalizzate: lunghezza massima di tutti i valori e nomi di intestazione combinati	10.240 caratteri
Massima lunghezza del valore dell'intestazione `Content-Security-Policy`	1,783 caratteri Richiedi una quota più elevata.
Massima lunghezza di un valore dell'intestazione `CORS (Access-Control-Allow-Origin)`	1,783 caratteri

Quote sulle distribuzioni multi-tenant

Entità	Quota predefinita
Numero massimo di tenant di distribuzione per Account AWS	10.000 Richiedi una quota più elevata.
Numero massimo di distribuzioni multi-tenant per Account AWS	20 Richiedi una quota più elevata.
Numero massimo di gruppi di connessione per Account AWS	100 Richiedi una quota più elevata.
Numero massimo di alias per tenant di distribuzione	100 Richiedi una quota più elevata.
Numero massimo di parametri per tenant di distribuzione	5

Entità	Quota predefinita
	Richiedi una quota più elevata.
Numero massimo di parametri per distribuzione multi-tenant	5 Richiedi una quota più elevata.
Numero massimo di parametri in un campo in una distribuzione multi-tenant	2 Richiedi una quota più elevata.
Numero massimo di gruppi di connessioni per elenco IP statici anycast	5 Richiedi una quota più elevata.

Per ulteriori informazioni sulle distribuzione multi-tenant, consulta Comprendere il funzionamento delle distribuzioni multi-tenant.

Informazioni correlate

Per ulteriori informazioni, consulta gli CloudFront endpoint e le quote di Amazon nel. Riferimenti generali di AWS

Esempi di codice per CloudFront l'utilizzo AWS SDKs

I seguenti esempi di codice mostrano come utilizzarlo CloudFront con un kit di sviluppo AWS software (SDK).

Le azioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le azioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica chiamando più funzioni all'interno dello stesso servizio o combinate con altri Servizi AWS.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Eliminare le risorse di CloudFront firma utilizzando SDK AWS
- Inizia con una CloudFront distribuzione di base utilizzando la CLI
- Crea cookie firmati URLs e cookie utilizzando un SDK AWS

- CloudFront Esempi di funzioni per CloudFront
  - Aggiungere intestazioni di sicurezza HTTP a un evento di risposta CloudFront del visualizzatore di funzioni
  - Aggiungere un'intestazione CORS a un evento di risposta del visualizzatore di CloudFront funzioni
  - Aggiungere un'intestazione di controllo della cache a un evento di risposta del visualizzatore di CloudFront funzioni
  - Aggiungere un vero header IP client a un evento di richiesta di CloudFront Functions Viewer
  - Aggiungere un'intestazione di origine a un evento di richiesta del visualizzatore di CloudFront funzioni
  - Aggiungi index.html alla richiesta URLs senza un nome di file in un evento di richiesta del visualizzatore di CloudFront funzioni
  - Normalizza i parametri della stringa di query in una richiesta di CloudFront Functions Viewer
  - Reindirizza a un nuovo URL in un evento di richiesta del visualizzatore di CloudFront funzioni
  - Riscrivi l'URI di una richiesta in base alla KeyValueStore configurazione per un evento di richiesta del visualizzatore di CloudFront funzioni
  - Indirizza le richieste a un'origine più vicina al visualizzatore in un evento di richiesta del visualizzatore di CloudFront funzioni
  - Usa coppie chiave-valore in una CloudFront richiesta di Functions Viewer
  - Convalida un token semplice in una richiesta di CloudFront Functions Viewer

Esempi di base per l' CloudFront utilizzo AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Amazon CloudFront con AWS SDKs.

Esempi

- Azioni per l'utilizzo CloudFront AWS SDKs
  - Utilizzo CreateDistribution con un AWS SDK o una CLI
  - Utilizzare CreateFunction con un SDK AWS

- Utilizzare CreateInvalidation con una CLI
- Utilizzare CreateKeyGroup con un SDK AWS
- Utilizzo CreatePublicKey con un AWS SDK o una CLI
- Utilizzo DeleteDistribution con un AWS SDK o una CLI
- Utilizzare GetCloudFrontOriginAccessIdentity con una CLI
- Utilizzare GetCloudFrontOriginAccessIdentityConfig con una CLI
- Utilizzare GetDistribution con una CLI
- Utilizzo GetDistributionConfig con un AWS SDK o una CLI
- Utilizzare ListCloudFrontOriginAccessIdentities con una CLI
- Utilizzo ListDistributions con un AWS SDK o una CLI
- Utilizzo UpdateDistribution con un AWS SDK o una CLI

Azioni per l'utilizzo CloudFront AWS SDKs

I seguenti esempi di codice mostrano come eseguire singole CloudFront azioni con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Questi estratti richiamano l' CloudFront API e sono estratti di codice di programmi più grandi che devono essere eseguiti nel contesto. È possibile visualizzare le azioni nel contesto in Scenari di utilizzo CloudFront AWS SDKs .

Gli esempi seguenti includono solo le azioni più comunemente utilizzate. Per un elenco completo, consulta Amazon CloudFront API Reference.

Esempi

- Utilizzo CreateDistribution con un AWS SDK o una CLI
- Utilizzare CreateFunction con un SDK AWS
- Utilizzare CreateInvalidation con una CLI
- Utilizzare CreateKeyGroup con un SDK AWS
- Utilizzo CreatePublicKey con un AWS SDK o una CLI
- Utilizzo DeleteDistribution con un AWS SDK o una CLI
- Utilizzare GetCloudFrontOriginAccessIdentity con una CLI
- Utilizzare GetCloudFrontOriginAccessIdentityConfig con una CLI

- Utilizzare GetDistribution con una CLI
- Utilizzo GetDistributionConfig con un AWS SDK o una CLI
- Utilizzare ListCloudFrontOriginAccessIdentities con una CLI
- Utilizzo ListDistributions con un AWS SDK o una CLI
- Utilizzo UpdateDistribution con un AWS SDK o una CLI

Utilizzo **`CreateDistribution`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateDistribution`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nei seguenti esempi di codice:

- Creare una distribuzione multi-tenant e un tenant di distribuzione
- Inizia con CloudFront

CLI

AWS CLI

Esempio 1: creare una distribuzione CloudFront

L'esempio `create-distribution` seguente crea una distribuzione per un bucket S3 denominato `amzn-s3-demo-bucket` e specifica inoltre `index.html` come oggetto root predefinito utilizzando argomenti della riga di comando.

```
aws cloudfront create-distribution \
    --origin-domain-name amzn-s3-demo-bucket.s3.amazonaws.com \
    --default-root-object index.html
```

Output:

```
{
    "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": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.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
        }
    }
}
```

Esempio 2: creare una CloudFront distribuzione utilizzando un file JSON

L'esempio `create-distribution` seguente crea una distribuzione per un bucket S3 denominato `amzn-s3-demo-bucket` e specifica inoltre `index.html` come oggetto root predefinito utilizzando un file JSON.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenuto di `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
```

```
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.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
```

```
}
```

Consulta l'esempio 1 per un output di esempio.

Esempio 3: creare una distribuzione CloudFront multi-tenant con un certificato

L'`create-distribution`esempio seguente crea una CloudFront distribuzione con supporto multi-tenant e specifica un certificato TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenuto di `dist-config.json`:

```
{
    "CallerReference": "cli-example-with-cert",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["HEAD", "GET"],
            "CachedMethods": {
                "Quantity": 2,
```

```
                "Items": ["HEAD", "GET"]
            }
        }
    },
    "Enabled": true,
    "ViewerCertificate": {
        "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/191306a1-db01-49ca-90ef-fc414ee5dabc",
        "SSLSupportMethod": "sni-only"
    },
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Output:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E1HVIAU7UABC",
    "ETag": "E20LT7R1BABC",
    "Distribution": {
        "Id": "E1HVIAU7U12ABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E1HVIAU7U12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:33:31.117000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
```

```
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-with-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
```

```
                    "Quantity": 2,
                    "Items": ["HEAD", "GET"],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": ["HEAD", "GET"]
                    }
                },
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": false,
                "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1.2_2021",
                "Certificate": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "CertificateSource": "acm"
            },
```

```
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Per ulteriori informazioni, consulta Lavorare con le distribuzioni nella Amazon CloudFront Developer Guide.

Esempio 4: creare una distribuzione CloudFront multi-tenant senza certificato

L'`create-distribution`esempio seguente crea una CloudFront distribuzione con supporto multi-tenant ma senza un certificato TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenuto di `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Comment": "CLI example distribution",
```

```
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        }
    },
    "Enabled": true,
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
```

```
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Output:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E2GJ5J9QN12ABC",
    "ETag": "E37YLVVQIABC",
    "Distribution": {
        "Id": "E2GJ5J9QNABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E2GJ5J9QN12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:35:20.565000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-no-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
```

```
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
```

```
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
```

```
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Per ulteriori informazioni, consulta Configurare le distribuzioni nell'Amazon CloudFront Developer Guide.

- Per i dettagli sull'API, consulta CreateDistribution AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

L'esempio seguente utilizza un bucket Amazon Simple Storage Service (Amazon S3) come origine del contenuto.

Dopo aver creato la distribuzione, il codice crea un messaggio CloudFrontWaiterdi attesa che la distribuzione venga distribuita prima di restituirla.

```
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;
        }
}
```

- Per i dettagli sull'API, consulta [CreateDistribution AWS SDK for Java 2.x](#)API Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: crea una CloudFront distribuzione di base, configurata con registrazione e memorizzazione nella cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.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 amzn-s3-demo-logging-bucket.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
```

- Per i dettagli sull'API, vedere CreateDistributionin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: crea una CloudFront distribuzione di base, configurata con registrazione e memorizzazione nella cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.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 amzn-s3-demo-logging-bucket.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
```

- Per i dettagli sull'API, vedere CreateDistributionin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`CreateFunction`** con un SDK AWS

Il seguente esempio di codice mostra come utilizzare`CreateFunction`.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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 "";
    }
}
```

- Per i dettagli sull'API, consulta la CreateFunctionsezione AWS SDK for Java 2.x API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`CreateInvalidation`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateInvalidation`.

CLI

AWS CLI

Per creare un'invalidazione per una distribuzione CloudFront

L'`create-invalidation`esempio seguente crea un'invalidazione per i file specificati nella distribuzione specificata: CloudFront

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --paths "/example-path/example-file.jpg" "/example-path/example-file2.png"
```

Output:

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

Nell'esempio precedente, la AWS CLI generava automaticamente un risultato casuale. `CallerReference` Per specificare i parametri `CallerReference` o per evitare di passare i parametri di invalidazione come argomenti della riga di comando, è possibile utilizzare un file JSON. L'esempio seguente crea un'invalidazione per due file fornendo i parametri di invalidazione in un file JSON denominato `inv-batch.json`:

```
aws cloudfront create-invalidation \
```

```
    --distribution-id EDFDVBD6EXAMPLE \
    --invalidation-batch file://inv-batch.json
```

Contenuto di `inv-batch.json`:

```
{
    "Paths": {
        "Quantity": 2,
        "Items": [
            "/example-path/example-file.jpg",
            "/example-path/example-file2.png"
        ]
    },
    "CallerReference": "cli-example"
}
```

Output:

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

- Per i dettagli sull'API, consulta CreateInvalidation AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo esempio crea una nuova invalidazione per una distribuzione con l'ID EXAMPLENSTXAXE. CallerReference è un ID univoco scelto dall'utente; in questo caso, viene utilizzato un timestamp che rappresenta il 15 maggio 2019 alle 9:00. La variabile $Paths archivia tre percorsi di immagini e file multimediali che l'utente non desidera vengano inseriti nella cache distribuita. Il valore del parametro -Paths_Quantity è il numero totale di percorsi specificati nel parametro -Paths_Item.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Output:

```
Invalidation                          Location

------------                          --------

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Per i dettagli sull'API, vedere CreateInvalidationin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio crea una nuova invalidazione per una distribuzione con l'ID EXAMPLENSTXAXE. CallerReference è un ID univoco scelto dall'utente; in questo caso, viene utilizzato un timestamp che rappresenta il 15 maggio 2019 alle 9:00. La variabile $Paths archivia tre percorsi di immagini e file multimediali che l'utente non desidera vengano inseriti nella cache distribuita. Il valore del parametro -Paths_Quantity è il numero totale di percorsi specificati nel parametro -Paths_Item.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Output:

```
Invalidation                          Location

------------                          --------

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Per i dettagli sull'API, vedere CreateInvalidationin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`CreateKeyGroup`** con un SDK AWS

Il seguente esempio di codice mostra come utilizzare`CreateKeyGroup`.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Un gruppo di chiavi richiede almeno una chiave pubblica utilizzata per verificare i cookie URLs firmati.

```
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;
    }
}
```

- Per i dettagli sull'API, consulta la CreateKeyGroupsezione AWS SDK for Java 2.x API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreatePublicKey`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreatePublicKey`.

CLI

AWS CLI

Per creare una chiave CloudFront pubblica

L'esempio seguente crea una chiave CloudFront pubblica fornendo i parametri in un file JSON denominatopub-key-config.json. Prima di poter utilizzare questo comando, è necessario disporre di una chiave pubblica con codifica PEM. Per ulteriori informazioni, consulta Create an RSA Key Pair nella Amazon CloudFront Developer Guide.

```
aws cloudfront create-public-key \
    --public-key-config file://pub-key-config.json
```

Il file `pub-key-config.json` è un documento JSON nella cartella corrente che contiene quanto segue. Nota che la chiave pubblica è codificata in formato 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"
}
```

Output:

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

- Per i dettagli sull'API, consulta CreatePublicKey AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Il seguente esempio di codice legge una chiave pubblica e la carica su 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);
        }
```

```
    }
}
```

- Per i dettagli sull'API, consulta la sezione AWS SDK for Java 2.x API CreatePublicKeyReference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteDistribution`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DeleteDistribution`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Inizia con CloudFront

CLI

AWS CLI

Per eliminare una distribuzione CloudFront

L'esempio seguente elimina la CloudFront distribuzione con l'ID. `EDFDVBD6EXAMPLE` Prima di eliminare una distribuzione, devi disabilitarla. Per disabilitare una distribuzione, utilizza il comando update-distribution. Per ulteriori informazioni, consulta gli esempi del comando update-distribution.

Quando una distribuzione è disabilitata, è possibile eliminarla. Per eliminare una distribuzione, è necessario utilizzare l'opzione `--if-match` per fornire il tag entità (`ETag`) della distribuzione. Per ottenere il`ETag`, utilizzare il comando get-distribution o. get-distribution-config

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

Se ha esito positivo, questo comando non produce alcun output.

- Per i dettagli sull'API, consulta AWS CLI Command DeleteDistributionReference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

L'esempio di codice seguente aggiorna una distribuzione impostandola su disabled, utilizza un waiter che attende l'implementazione della modifica, quindi elimina la distribuzione.

```
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);
                }
        }
}
```

- Per i dettagli sull'API, consulta la DeleteDistributionsezione AWS SDK for Java 2.x API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`GetCloudFrontOriginAccessIdentity`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetCloudFrontOriginAccessIdentity`.

CLI

AWS CLI

Per ottenere un'identità di accesso all' CloudFront origine

L'esempio seguente ottiene l'identità di accesso di CloudFront origine (OAI) con l'`IDE74FTE3AEXAMPLE`, incluso il relativo ID canonico S3 `ETag` e l'ID canonico S3 associato. L'ID OAI viene restituito nell'output dei comandi -access-identity e -access-identitiescreate-cloud-front-origin. list-cloud-front-origin

```
aws cloudfront get-cloud-front-origin-access-identity --id E74FTE3AEXAMPLE
```

Output:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
    }
}
```

- Per i dettagli sull'API, consulta Command Reference. GetCloudFrontOriginAccessIdentityAWS CLI

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce un'identità di accesso all' CloudFront origine di Amazon specifica, specificata dal parametro -Id. Sebbene il parametro -Id non sia obbligatorio, se non lo si specifica non viene restituito alcun risultato.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Output:

```
     CloudFrontOriginAccessIdentityConfig    Id
    S3CanonicalUserId
     ------------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Per i dettagli sull'API, vedere GetCloudFrontOriginAccessIdentityin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce un'identità di accesso all' CloudFront origine di Amazon specifica, specificata dal parametro -Id. Sebbene il parametro -Id non sia obbligatorio, se non lo si specifica non viene restituito alcun risultato.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Output:

```
     CloudFrontOriginAccessIdentityConfig    Id
    S3CanonicalUserId
     ------------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Per i dettagli sull'API, vedere GetCloudFrontOriginAccessIdentityin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`GetCloudFrontOriginAccessIdentityConfig`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetCloudFrontOriginAccessIdentityConfig`.

CLI

AWS CLI

Per ottenere una configurazione dell'identità di accesso all' CloudFront origine

L'esempio seguente ottiene i metadati sull'identità di accesso all' CloudFront origine (OAI) con l'`IDE74FTE3AEXAMPLE`, incluso il relativo. `ETag` L'ID OAI viene restituito nell'output dei comandi -access-identity e create-cloud-front-origin -access-identities. list-cloud-front-origin

```
aws cloudfront get-cloud-front-origin-access-identity-config --id E74FTE3AEXAMPLE
```

Output:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentityConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example OAI"
    }
}
```

- Per i dettagli sull'API, consulta Command Reference. GetCloudFrontOriginAccessIdentityConfigAWS CLI

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce informazioni di configurazione su una singola identità di accesso di CloudFront origine Amazon, specificata dal parametro -Id. Si verificano errori se non viene specificato alcun parametro -Id.

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Output:

```
     CallerReference                                          Comment
     ---------------                                          -------
     mycallerreference: 2/1/2011 1:16:32 PM                   Caller
reference: 2/1/2011 1:16:32 PM
```

- Per i dettagli sull'API, vedere GetCloudFrontOriginAccessIdentityConfigin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce informazioni di configurazione su una singola identità di accesso di CloudFront origine Amazon, specificata dal parametro -Id. Si verificano errori se non viene specificato alcun parametro -Id.

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Output:

```
     CallerReference                                                Comment
     ---------------                                                -------
     mycallerreference: 2/1/2011 1:16:32 PM                         Caller
reference: 2/1/2011 1:16:32 PM
```

- Per i dettagli sull'API, vedere GetCloudFrontOriginAccessIdentityConfigin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`GetDistribution`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetDistribution`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Inizia con CloudFront

CLI

AWS CLI

Per ottenere una distribuzione CloudFront

L'`get-distribution`esempio seguente ottiene la CloudFront distribuzione con l'`IDEDFDVBD6EXAMPLE`, incluso il relativo`ETag`. L'ID distribuzione viene restituito nei comandi create-distribution e list-distribution.

```
aws cloudfront get-distribution \
    --id EDFDVBD6EXAMPLE
```

Output:

```
{
    "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": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.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
        }
    }
}
```

- Per i dettagli sull'API, consulta GetDistribution AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: recupera le informazioni relative a una distribuzione specifica.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: recupera le informazioni relative a una distribuzione specifica.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetDistributionConfig`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetDistributionConfig`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Inizia con CloudFront

CLI

AWS CLI

Per ottenere una configurazione di CloudFront distribuzione

L'esempio seguente ottiene i metadati sulla CloudFront distribuzione con l'IDEDFDVBD6EXAMPLE, incluso il relativoETag. L'ID distribuzione viene restituito nei comandi create-distribution e list-distribution.

```
aws cloudfront get-distribution-config \
    --id EDFDVBD6EXAMPLE
```

Output:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "DistributionConfig": {
        "CallerReference": "cli-example",
```

```
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.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
    }
}
```

- Per i dettagli sull'API, consulta GetDistributionConfig AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: recupera la configurazione di una distribuzione specifica.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionConfigin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: recupera la configurazione di una distribuzione specifica.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionConfigin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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!")
```

- Per i dettagli sull'API, consulta GetDistributionConfig AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`ListCloudFrontOriginAccessIdentities`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListCloudFrontOriginAccessIdentities`.

CLI

AWS CLI

Per elencare le identità di accesso all' CloudFront origine

L'esempio seguente ottiene un elenco delle identità di accesso di CloudFront origine (OAIs) presenti nel tuo AWS account:

```
aws cloudfront list-cloud-front-origin-access-identities
```

Output:

```
{
    "CloudFrontOriginAccessIdentityList": {
        "Items": [
            {
                "Id": "E74FTE3AEXAMPLE",
                "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
                "Comment": "Example OAI"
            },
            {
                "Id": "EH1HDMBEXAMPLE",
                "S3CanonicalUserId":
 "1489f6f2e6faacaae7ff64c4c3e6956c24f78788abfc1718c3527c263bf7a17EXAMPLE",
                "Comment": "Test OAI"
            },
            {
                "Id": "E2X2C9TEXAMPLE",
                "S3CanonicalUserId":
 "cbfeebb915a64749f9be546a45b3fcfd3a31c779673c13c4dd460911ae402c2EXAMPLE",
                "Comment": "Example OAI #2"
            }
```

```
        ]
    }
}
```

- Per i dettagli sull'API, consulta ListCloudFrontOriginAccessIdentities AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce un elenco di identità di accesso di CloudFront origine di Amazon. Poiché il MaxItem parametro - specifica il valore 2, i risultati includono due identità.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Output:

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Per i dettagli sull'API, vedere ListCloudFrontOriginAccessIdentitiesin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce un elenco di identità di accesso di CloudFront origine di Amazon. Poiché il MaxItem parametro - specifica il valore 2, i risultati includono due identità.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Output:

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
```

```
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Per i dettagli sull'API, vedere ListCloudFrontOriginAccessIdentitiesin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, vedere. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListDistributions`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListDistributions`.

CLI

AWS CLI

Per elencare le distribuzioni CloudFront

L'esempio seguente ottiene un elenco delle CloudFront distribuzioni presenti nel tuo AWS account.

```
aws cloudfront list-distributions
```

Output:

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "E23YS8OEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E23YS8OEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2024-08-05T18:23:40.375000+00:00",
                "DomainName": "abcdefgh12ijk.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
```

```
                    "Items": [
                        {
                            "Id": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            },
                            "ConnectionAttempts": 3,
                            "ConnectionTimeout": 10,
                            "OriginShield": {
                                "Enabled": false
                            },
                            "OriginAccessControlId": "EIAP8PEXAMPLE"
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "TrustedKeyGroups": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
```

```
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "Compress": true,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e886EXAMPLE"
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "SSLSupportMethod": "vip",
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "HTTP2",
            "IsIPV6Enabled": true,
            "Staging": false
        }
```

```
        ]
    }
}
```

- Per i dettagli sull'API, consulta ListDistributions AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce le distribuzioni.

```
Get-CFDistributionList
```

- Per i dettagli sull'API, vedere ListDistributionsin AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce le distribuzioni.

```
Get-CFDistributionList
```

- Per i dettagli sull'API, vedere ListDistributionsin AWS Strumenti per PowerShell Cmdlet Reference (V5).

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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.")
```

- Per i dettagli sull'API, consulta ListDistributions AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`UpdateDistribution`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `UpdateDistribution`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Inizia con CloudFront

CLI

AWS CLI

Esempio 1: aggiornare l'oggetto radice predefinito di una CloudFront distribuzione

L'esempio seguente aggiorna l'oggetto radice predefinito `index.html` per la CloudFront distribuzione con l'ID`EDFDVBD6EXAMPLE`.

```
aws cloudfront update-distribution \
    --id EDFDVBD6EXAMPLE \
    --default-root-object index.html
```

Output:

```
{
    "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
        }
    }
}
```

Esempio 2: aggiornare una CloudFront distribuzione

L'esempio seguente disabilita la CloudFront distribuzione con l'ID `EMLARXS9EXAMPLE` fornendo la configurazione della distribuzione in un file JSON denominato. `dist-config-disable.json` Per aggiornare una distribuzione, è necessario utilizzare l'opzione `--if-match` per fornire il tag entità (`ETag`) della distribuzione. Per ottenere il`ETag`, usa il comando get-distribution o. get-distribution-config Nota che il campo `Enabled` è impostato su `false` nel file JSON.

Dopo aver utilizzato l'esempio seguente per disabilitare una distribuzione, puoi utilizzare il comando delete-distribution per eliminarla.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Contenuto di `dist-config-disable.json`:

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
```

```
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-1574382155-273939",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-
bucket.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
}
```

Output:

```
{
    "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": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
```

```
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-
bucket.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
        }
    }
}
```

- Per i dettagli sull'API, consulta AWS CLI Command UpdateDistributionReference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
        }
    }
}
```

- Per i dettagli sull'API, consulta la UpdateDistributionsezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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!")
```

- Per i dettagli sull'API, consulta UpdateDistribution AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari di utilizzo CloudFront AWS SDKs

I seguenti esempi di codice mostrano come implementare scenari comuni in CloudFront with AWS SDKs. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno

CloudFront o combinandole con altre Servizi AWS. Ogni scenario include un collegamento al codice sorgente completo, dove è possibile trovare le istruzioni su come configurare ed eseguire il codice.

Gli scenari sono relativi a un livello intermedio di esperienza per aiutarti a comprendere le azioni di servizio nel contesto.

Esempi

- Crea un SDK per le risorse di gestione SaaS AWS
- Eliminare le risorse di CloudFront firma utilizzando SDK AWS
- Inizia con una CloudFront distribuzione di base utilizzando la CLI
- Crea cookie firmati URLs e cookie utilizzando un SDK AWS

Crea un SDK per le risorse di gestione SaaS AWS

L'esempio di codice seguente mostra come creare una distribuzione multi-tenant e un tenant di distribuzione con varie configurazioni.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

L'esempio seguente mostra come creare una distribuzione multi-tenant con parametri e un certificato jolly.

```
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.ConnectionMode;
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.HttpVersion;
```

```
import software.amazon.awssdk.services.cloudfront.model.Method;
import software.amazon.awssdk.services.cloudfront.model.SSLSupportMethod;
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 CreateMultiTenantDistribution {
    public static Distribution
 CreateMultiTenantDistributionWithCert(CloudFrontClient cloudFrontClient,
                                                                    S3Client
 s3Client,
                                                                    final String
 bucketName,
                                                                    final String
 certificateArn) {
        // fetch the origin info if necessary
        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.

        CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                .distributionConfig(b1 -> b1
                        .httpVersion(HttpVersion.HTTP2)
                        .enabled(true)
                        .comment("Template Distribution with cert built with
 java")
                        .connectionMode(ConnectionMode.TENANT_ONLY)
                        .callerReference(Instant.now().toString())
                        .viewerCertificate(certBuilder -> certBuilder
                                .acmCertificateArn(certificateArn)
                                .sslSupportMethod(SSLSupportMethod.SNI_ONLY))
                        .origins(b2 -> b2
                                .quantity(1)
                                .items(b3 -> b3
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
```

```
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
                                                        "")))))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
                                        .items(Method.HEAD, Method.GET)))
                ));

        final Distribution distribution = createDistResponse.distribution();
        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"));
        }
        return distribution;
    }

    public static Distribution
 CreateMultiTenantDistributionNoCert(CloudFrontClient cloudFrontClient,
                                                                S3Client s3Client,
                                                                final String
 bucketName) {
        // fetch the origin info if necessary
```

```
        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.

        CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                .distributionConfig(b1 -> b1
                        .httpVersion(HttpVersion.HTTP2)
                        .enabled(true)
                        .comment("Template Distribution with cert built with
 java")
                        .connectionMode(ConnectionMode.TENANT_ONLY)
                        .callerReference(Instant.now().toString())
                        .origins(b2 -> b2
                                .quantity(1)
                                .items(b3 -> b3
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
                                                        ""))))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
                                        .items(Method.HEAD, Method.GET)))
```

```
                ));

        final Distribution distribution = createDistResponse.distribution();
        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"));
        }
        return distribution;
    }
}
```

L'esempio seguente mostra come creare un tenant di distribuzione associato al modello, incluso l'utilizzo del parametro dichiarato sopra. Nota che non è necessario aggiungere informazioni sul certificato in questo esempio perché il dominio è già coperto dal modello principale.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantNoCert(CloudFrontClient cloudFrontClient,
```

```
                                                                Route53Client
route53Client,
                                                                String
distributionId,
                                                                String
domain,
                                                                String
hostedZoneId) {
        CreateDistributionTenantResponse createResponse =
cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("no-cert-tenant")
        );

        final DistributionTenant distributionTenant =
createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
distribution tenant
        // We fetch the RoutingEndpoint to point to via the default connection
group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

.value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
```

```
                ));
        return distributionTenant;
    }

}
```

Se il certificato del visualizzatore è stato omesso dal modello principale, è invece necessario aggiungere le informazioni sul certificato nei tenant associati. L'esempio seguente mostra come eseguire questa operazione tramite l'ARN di un certificato ACM che interessa il dominio necessario per il tenant.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantWithCert(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId,
                                                                    String
 certificateArn) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
```

```
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .enabled(false)
                .name("tenant-with-cert")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .customizations(b3 -> b3
                        .certificate(b4 -> b4
                                .arn(certificateArn))) // NOTE: Cert must be in
 Us-East-1 and cover the domain provided in this request

        );

        final DistributionTenant distributionTenant =
 createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
 distribution tenant
        // We fetch the RoutingEndpoint to point to via the default connection
 group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
 cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

 .value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));
        return distributionTenant;
    }

}
```

L'esempio seguente mostra come eseguire questa operazione con una richiesta di certificato gestita CloudFront -hosted. Questa soluzione è ideale se non è già stato generato traffico verso il dominio. In questo caso, creiamo un file ConnectionGroup per generare un. RoutingEndpoint Quindi lo usiamo RoutingEndpoint per creare record DNS che verificano la proprietà del dominio e puntano a CloudFront. CloudFront utilizzerà quindi automaticamente un token per convalidare la proprietà del dominio e creare un certificato gestito.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantCfHosted(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId) throws InterruptedException {
        CreateConnectionGroupResponse createConnectionGroupResponse =
 cloudFrontClient.createConnectionGroup(builder -> builder
                .ipv6Enabled(true)
                .name("cf-hosted-connection-group")
                .enabled(true));
```

```
        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("cf-hosted domain validation record")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type(RRType.CNAME)
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

 .value(createConnectionGroupResponse.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));

        // Give the R53 record time to propagate, if it isn't being returned by
 servers yet, the following call will fail
        Thread.sleep(60000);

        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))

 .connectionGroupId(createConnectionGroupResponse.connectionGroup().id())
                .enabled(false)
                .name("cf-hosted-tenant")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .managedCertificateRequest(b3 -> b3
                        .validationTokenHost(ValidationTokenHost.CLOUDFRONT)
                )
        );

        return createResponse.distributionTenant();
    }

}
```

L'esempio seguente mostra come eseguire questa operazione con una richiesta di certificato gestita con hosting autonomo. Questa soluzione è ideale se è stato generato traffico verso il dominio e non possono essere sostenuti tempi di inattività durante una migrazione. Alla fine di questo esempio, il tenant verrà creato in uno stato in attesa della convalida del dominio e della configurazione DNS. Segui i passaggi [qui] (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/managed-cloudfront-certificates.html#complete-domain-ownership) per completare la configurazione quando sei pronto per la migrazione del traffico.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantSelfHosted(CloudFrontClient cloudFrontClient,
                                                                    String
 distributionId,
                                                                    String
 domain) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("self-hosted-tenant")
                .managedCertificateRequest(b3 -> b3
```

```
                        .validationTokenHost(ValidationTokenHost.SELF_HOSTED)
                        .primaryDomainName(domain)
                )
        );

        return createResponse.distributionTenant();
    }

}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dell'API AWS SDK for Java 2.x .
  - CreateDistribution
  - CreateDistributionTenant

Per un elenco completo delle guide per sviluppatori SDK e degli esempi di codice, consulta. AWS Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Eliminare le risorse di CloudFront firma utilizzando SDK AWS

L'esempio di codice seguente mostra come eliminare le risorse utilizzate per accedere a contenuti con restrizioni in un bucket Amazon Simple Storage Service (Amazon S3).

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice 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);
        }
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dell'API AWS SDK for Java 2.x .
  - DeleteKeyGroup
  - DeleteOriginAccessControl
  - DeletePublicKey

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Inizia con una CloudFront distribuzione di base utilizzando la CLI

L'esempio di codice seguente mostra come:

- Creare un bucket Amazon S3 per l'archiviazione dei contenuti
- Caricare contenuti di esempio nel bucket S3
- Creare un controllo di accesso origine (OAC) per un accesso sicuro a S3
- Crea una CloudFront distribuzione con S3 come origine
- Aggiorna la policy del bucket S3 per consentire l'accesso CloudFront
- Attendere l'implementazione della distribuzione e verificare l'accesso ai contenuti
- Eseguire la pulizia delle risorse, tra cui distribuzione, controllo di accesso origine (OAC) e bucket S3

Bash

AWS CLI con lo script Bash

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri come eseguire la configurazione e l'esecuzione nel repository dei tutorial sugli esempi di codice per gli sviluppatori.

```
#!/bin/bash

# CloudFront Getting Started Tutorial Script
# This script creates an S3 bucket, uploads sample content, creates a CloudFront
 distribution with OAC,
# and demonstrates how to access content through CloudFront.

# Set up logging
LOG_FILE="cloudfront-tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting CloudFront Getting Started Tutorial at $(date)"

# Function to handle errors
handle_error() {
    echo "ERROR: $1"
    echo "Resources created before error:"
    if [ -n "$BUCKET_NAME" ]; then
        echo "- S3 Bucket: $BUCKET_NAME"
    fi
    if [ -n "$OAC_ID" ]; then
        echo "- CloudFront Origin Access Control: $OAC_ID"
    fi
    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "- CloudFront Distribution: $DISTRIBUTION_ID"
    fi

    echo "Attempting to clean up resources..."
    cleanup
    exit 1
}
```

```
# Function to clean up resources
cleanup() {
    echo "Cleaning up resources..."

    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "Disabling CloudFront distribution $DISTRIBUTION_ID..."

        # Get the current configuration and ETag
        ETAG=$(aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" --
query 'ETag' --output text)
        if [ $? -ne 0 ]; then
            echo "Failed to get distribution config. Continuing with cleanup..."
        else
            # Create a modified configuration with Enabled=false
            aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" | \
            jq '.DistributionConfig.Enabled = false' > temp_disabled_config.json

            # Update the distribution to disable it
            aws cloudfront update-distribution \
                --id "$DISTRIBUTION_ID" \
                --distribution-config file://<(jq '.DistributionConfig'
 temp_disabled_config.json) \
                --if-match "$ETAG"

            if [ $? -ne 0 ]; then
                echo "Failed to disable distribution. Continuing with cleanup..."
            else
                echo "Waiting for distribution to be disabled (this may take
 several minutes)..."
                aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"

                # Delete the distribution
                ETAG=$(aws cloudfront get-distribution-config --id
 "$DISTRIBUTION_ID" --query 'ETag' --output text)
                aws cloudfront delete-distribution --id "$DISTRIBUTION_ID" --if-
match "$ETAG"
                if [ $? -ne 0 ]; then
                    echo "Failed to delete distribution. You may need to delete
 it manually."
                else
                    echo "CloudFront distribution deleted."
                fi
            fi
```

```
        fi
    fi

    if [ -n "$OAC_ID" ]; then
        echo "Deleting Origin Access Control $OAC_ID..."
        OAC_ETAG=$(aws cloudfront get-origin-access-control --id "$OAC_ID" --
query 'ETag' --output text 2>/dev/null)
        if [ $? -ne 0 ]; then
            echo "Failed to get Origin Access Control ETag. You may need to
 delete it manually."
        else
            aws cloudfront delete-origin-access-control --id "$OAC_ID" --if-match
 "$OAC_ETAG"
            if [ $? -ne 0 ]; then
                echo "Failed to delete Origin Access Control. You may need to
 delete it manually."
            else
                echo "Origin Access Control deleted."
            fi
        fi
    fi

    if [ -n "$BUCKET_NAME" ]; then
        echo "Deleting S3 bucket $BUCKET_NAME and its contents..."
        aws s3 rm "s3://$BUCKET_NAME" --recursive
        if [ $? -ne 0 ]; then
            echo "Failed to remove bucket contents. Continuing with bucket
 deletion..."
        fi

        aws s3 rb "s3://$BUCKET_NAME"
        if [ $? -ne 0 ]; then
            echo "Failed to delete bucket. You may need to delete it manually."
        else
            echo "S3 bucket deleted."
        fi
    fi

    # Clean up temporary files
    rm -f temp_disabled_config.json
    rm -rf temp_content
}

# Generate a random identifier for the bucket name
```

```
RANDOM_ID=$(openssl rand -hex 6)
BUCKET_NAME="cloudfront-${RANDOM_ID}"
echo "Using bucket name: $BUCKET_NAME"

# Create a temporary directory for content
TEMP_DIR="temp_content"
mkdir -p "$TEMP_DIR/css"
if [ $? -ne 0 ]; then
    handle_error "Failed to create temporary directory"
fi

# Step 1: Create an S3 bucket
echo "Creating S3 bucket: $BUCKET_NAME"
aws s3 mb "s3://$BUCKET_NAME"
if [ $? -ne 0 ]; then
    handle_error "Failed to create S3 bucket"
fi

# Step 2: Create sample content
echo "Creating sample content..."
cat > "$TEMP_DIR/index.html" << 'EOF'
<!DOCTYPE html>
<html>
<head>
    <title>Hello World</title>
    <link rel="stylesheet" type="text/css" href="css/styles.css">
</head>
<body>
    <h1>Hello world!</h1>
</body>
</html>
EOF

cat > "$TEMP_DIR/css/styles.css" << 'EOF'
body {
    font-family: Arial, sans-serif;
    margin: 40px;
    background-color: #f5f5f5;
}
h1 {
    color: #333;
    text-align: center;
}
EOF
```

```
# Step 3: Upload content to the S3 bucket
echo "Uploading content to S3 bucket..."
aws s3 cp "$TEMP_DIR/" "s3://$BUCKET_NAME/" --recursive
if [ $? -ne 0 ]; then
    handle_error "Failed to upload content to S3 bucket"
fi

# Step 4: Create Origin Access Control
echo "Creating Origin Access Control..."
OAC_RESPONSE=$(aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
$BUCKET_NAME",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=

if [ $? -ne 0 ]; then
    handle_error "Failed to create Origin Access Control"
fi

OAC_ID=$(echo "$OAC_RESPONSE" | jq -r '.OriginAccessControl.Id')
echo "Created Origin Access Control with ID: $OAC_ID"

# Step 5: Create CloudFront distribution
echo "Creating CloudFront distribution..."

# Get AWS account ID for bucket policy
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
if [ $? -ne 0 ]; then
    handle_error "Failed to get AWS account ID"
fi

# Create distribution configuration
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-tutorial-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-$BUCKET_NAME",
                "DomainName": "$BUCKET_NAME.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
```

```
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-$BUCKET_NAME",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for tutorial",
    "Enabled": true,
    "WebACLId": ""
}
EOF

DIST_RESPONSE=$(aws cloudfront create-distribution --distribution-config file://
distribution-config.json)
if [ $? -ne 0 ]; then
    handle_error "Failed to create CloudFront distribution"
fi

DISTRIBUTION_ID=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.Id')
DOMAIN_NAME=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.DomainName')

echo "Created CloudFront distribution with ID: $DISTRIBUTION_ID"
echo "CloudFront domain name: $DOMAIN_NAME"

# Step 6: Update S3 bucket policy
```

```
echo "Updating S3 bucket policy..."
cat > bucket-policy.json << EOF
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::$BUCKET_NAME/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::
$ACCOUNT_ID:distribution/$DISTRIBUTION_ID"
                }
            }
        }
    ]
}
EOF

aws s3api put-bucket-policy --bucket "$BUCKET_NAME" --policy file://bucket-
policy.json
if [ $? -ne 0 ]; then
    handle_error "Failed to update S3 bucket policy"
fi

# Step 7: Wait for distribution to deploy
echo "Waiting for CloudFront distribution to deploy (this may take 5-10
 minutes)..."
aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"
if [ $? -ne 0 ]; then
    echo "Warning: Distribution deployment wait timed out. The distribution may
 still be deploying."
else
    echo "CloudFront distribution is now deployed."
fi

# Step 8: Display access information
echo ""
echo "===== CloudFront Distribution Setup Complete ====="
```

```
echo "You can access your content at: https://$DOMAIN_NAME/index.html"
echo ""
echo "Resources created:"
echo "- S3 Bucket: $BUCKET_NAME"
echo "- CloudFront Origin Access Control: $OAC_ID"
echo "- CloudFront Distribution: $DISTRIBUTION_ID"
echo ""

# Ask user if they want to clean up resources
read -p "Do you want to clean up all resources created by this script? (y/n): "
 CLEANUP_RESPONSE
if [[ "$CLEANUP_RESPONSE" =~ ^[Yy] ]]; then
    cleanup
    echo "All resources have been cleaned up."
else
    echo "Resources will not be cleaned up. You can manually delete them later."
    echo "To access your content, visit: https://$DOMAIN_NAME/index.html"
fi

echo "Tutorial completed at $(date)"
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dei comandi della AWS CLI .
  - CreateDistribution
  - CreateOriginAccessControl
  - DeleteDistribution
  - DeleteOriginAccessControl
  - GetDistribution
  - GetDistributionConfig
  - GetOriginAccessControl
  - UpdateDistribution
  - WaitDistributionDeployed

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Crea cookie firmati URLs e cookie utilizzando un SDK AWS

Il seguente esempio di codice mostra come creare cookie firmati URLs e cookie che consentono l'accesso a risorse con restrizioni.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Usa la CannedSignerRequestclasse per firmare URLs o cookie con una politica predefinita.

```
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();
    }
}
```

Usa la CustomSignerRequestclasse per firmare URLs o cookie con una politica personalizzata. I metodi `activeDate` e `ipRange` sono facoltativi.

```
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)
                // .resourceUrlPattern("https://*.example.com/*")  // Optional.
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expireDate)
                .activeDate(activeDate) // Optional.
                // .ipRange("192.168.0.1/24") // Optional.
                .build();
```

```
    }
}
```

L'esempio seguente dimostra l'uso della CloudFrontUtilitiesclasse per produrre cookie firmati e URLs. Visualizza questo esempio di codice su. 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;
    }
}
```

- Per i dettagli sull'API, consulta la CloudFrontUtilitiessezione AWS SDK for Java 2.x API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di CloudFront con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

CloudFront Esempi di funzioni per CloudFront

I seguenti esempi di codice mostrano come utilizzare CloudFront con AWS SDKs.

Esempi

- Aggiungere intestazioni di sicurezza HTTP a un evento di risposta CloudFront del visualizzatore di funzioni
- Aggiungere un'intestazione CORS a un evento di risposta del visualizzatore di CloudFront funzioni

- Aggiungere un'intestazione di controllo della cache a un evento di risposta del visualizzatore di CloudFront funzioni
- Aggiungere un vero header IP client a un evento di richiesta di CloudFront Functions Viewer
- Aggiungere un'intestazione di origine a un evento di richiesta del visualizzatore di CloudFront funzioni
- Aggiungi index.html alla richiesta URLs senza un nome di file in un evento di richiesta del visualizzatore di CloudFront funzioni
- Normalizza i parametri della stringa di query in una richiesta di CloudFront Functions Viewer
- Reindirizza a un nuovo URL in un evento di richiesta del visualizzatore di CloudFront funzioni
- Riscrivi l'URI di una richiesta in base alla KeyValueStore configurazione per un evento di richiesta del visualizzatore di CloudFront funzioni
- Indirizza le richieste a un'origine più vicina al visualizzatore in un evento di richiesta del visualizzatore di CloudFront funzioni
- Usa coppie chiave-valore in una CloudFront richiesta di Functions Viewer
- Convalida un token semplice in una richiesta di CloudFront Functions Viewer

Aggiungere intestazioni di sicurezza HTTP a un evento di risposta CloudFront del visualizzatore di funzioni

Il seguente esempio di codice mostra come aggiungere intestazioni di sicurezza HTTP a un evento di risposta del visualizzatore CloudFront Functions.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async 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'; 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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Aggiungere un'intestazione CORS a un evento di risposta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come aggiungere un'intestazione CORS a un evento di risposta del visualizzatore CloudFront Functions.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async function handler(event)  {
    var request = event.request;
```

```
    var 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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Aggiungere un'intestazione di controllo della cache a un evento di risposta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come aggiungere un'intestazione di controllo della cache a un evento di risposta del visualizzatore CloudFront Functions.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async function handler(event) {
    var response = event.response;
    var headers = response.headers;
```

```
    if (response.statusCode >= 200 && response.statusCode < 400) {
        // Set the cache-control header
        headers['cache-control'] = {value: 'public, max-age=63072000'};
    }

    // Return response to viewers
    return response;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Aggiungere un vero header IP client a un evento di richiesta di CloudFront Functions Viewer

Il seguente esempio di codice mostra come aggiungere un'intestazione IP true client a un evento di richiesta del visualizzatore di CloudFront funzioni.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Aggiungere un'intestazione di origine a un evento di richiesta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come aggiungere un'intestazione di origine a un evento di richiesta del visualizzatore di CloudFront funzioni.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async 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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Aggiungi index.html alla richiesta URLs senza un nome di file in un evento di richiesta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come aggiungere index.html alla richiesta URLs senza un nome di file in un evento di richiesta del visualizzatore di CloudFront funzioni.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async 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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Normalizza i parametri della stringa di query in una richiesta di CloudFront Functions Viewer

Il seguente esempio di codice mostra come normalizzare i parametri della stringa di query in una richiesta di CloudFront Functions Viewer.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Reindirizza a un nuovo URL in un evento di richiesta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come reindirizzare a un nuovo URL in un evento di richiesta del visualizzatore di CloudFront funzioni.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
async 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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Riscrivi l'URI di una richiesta in base alla KeyValueStore configurazione per un evento di richiesta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come riscrivere l'URI di una richiesta in base alla KeyValueStore configurazione per un evento di richiesta del visualizzatore di CloudFront funzioni.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
import cf from 'cloudfront';

// (Optional) Replace KVS_ID with actual KVS ID
const kvsId = "KVS_ID";
// enable stickiness by setting a cookie from origin or using another edge
 function
const stickinessCookieName = "appversion";
// set to true to enable console logging
const loggingEnabled = false;

// function rewrites the request uri based on configuration in KVS
// example config in KVS in key:value format
// "latest": {"a_weightage": .8, "a_url": "v1", "b_url": "v2"}
// given above key and value in KVS the request uri will be rewritten
// for example http(s)://domain/latest/something/else will be rewritten as
 http(s)://domain/v1/something/else or http(s)://domain/v2/something/else
 depending on weightage
// if no configuration is found, then the request is returned as is
async 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.
    const request = event.request;
    const pathSegments = request.uri.split('/');
    const key = pathSegments[1];

    // if empty path segment or if there is valid stickiness cookie
    // then skip call to KVS and let the request continue.
    if (!key || hasValidStickinessCookie(request.cookies[stickinessCookieName],
 key)) {
        return event.request;
    }

    try {
        // get the prefix replacement from KVS
        const replacement = await getPathPrefixByWeightage(key);
        if (!replacement) {
            return event.request;
        }
        //Replace the first path with the replacement
        pathSegments[1] = replacement;
        log(`using prefix ${pathSegments[1]}`)
        const newUri = pathSegments.join('/');
        log(`${request.uri} -> ${newUri}`);
        request.uri = newUri;

        return request;
    } catch (err) {
        // No change to the path if the key is not found or any other error
        log(`request uri: ${request.uri}, error: ${err}`);
    }
    // no change to path - return request
    return event.request;
}

// function to get the prefix from KVS
async function getPathPrefixByWeightage(key) {
    const kvsHandle = cf.kvs(kvsId);
    // get the weightage config from KVS
    const kvsResponse = await kvsHandle.get(key);
    const weightageConfig = JSON.parse(kvsResponse);
    // no configuration - return null
    if (!weightageConfig || !isFinite(weightageConfig.a_weightage)) {
        return null;
```

```
    }
    // return the url based on weightage
    // return null if no url is configured
    if (Math.random() <= weightageConfig.a_weightage) {
        return weightageConfig.a_url ? weightageConfig.a_url: null;
    } else {
        return weightageConfig.b_url ? weightageConfig.b_url : null;
    }
}

// function to check if the stickiness cookie is valid
function hasValidSticknessCookie(stickinessCookie, pathSegment) {
    // if the value exists and it matches pathSegment
    return (stickinessCookie && stickinessCookie.value === pathSegment)
}

function log(message) {
    if (loggingEnabled) {
        console.log(message);
    }
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Indirizza le richieste a un'origine più vicina al visualizzatore in un evento di richiesta del visualizzatore di CloudFront funzioni

Il seguente esempio di codice mostra come indirizzare le richieste a un'origine più vicina al visualizzatore in un evento di richiesta del visualizzatore CloudFront Functions.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
import cf from 'cloudfront';

function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const country = headers['cloudfront-viewer-country'] &&
        headers['cloudfront-viewer-country'].value;

    //List of Regions with S3 buckets containing content
    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'
    };

    const DEFAULT_REGION = 'us-east-1';

    const selectedRegion = (country && countryToRegion[country]) ||
 DEFAULT_REGION;

    const domainName =
        `cloudfront-functions-demo-bucket-in-${selectedRegion}.s3.
${selectedRegion}.amazonaws.com`;

    cf.updateRequestOrigin({
        "domainName": domainName,
        "originAccessControlConfig": {
            "enabled": true,
            "region": selectedRegion,
```

```
            "signingBehavior": "always",
            "signingProtocol": "sigv4",
            "originType": "s3"
        },
    });

    return request;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Usa coppie chiave-valore in una CloudFront richiesta di Functions Viewer

Il seguente esempio di codice mostra come utilizzare le coppie chiave-valore in una richiesta di CloudFront Functions Viewer.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
import cf from 'cloudfront';

// This fails if there is no key value store associated with the function
const kvsHandle = cf.kvs();

// Remember to associate the KVS with your function before referencing KVS in
 your code.
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
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;
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Convalida un token semplice in una richiesta di CloudFront Functions Viewer

Il seguente esempio di codice mostra come convalidare un token semplice in una richiesta di CloudFront Functions Viewer.

JavaScript

JavaScript runtime 2.0 per Functions CloudFront

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri come configurarlo ed eseguirlo nell'archivio degli esempi di CloudFront Functions.

```
import crypto from 'crypto';
import cf from 'cloudfront';
```

```
//Response when JWT is not valid.
const response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

// Remember to associate the KVS with your function before calling the const
 kvsKey = 'jwt.secret'.
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
const kvsKey = 'jwt.secret';
// set to true to enable console logging
const loggingEnabled = false;


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 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;
    }

    let xor = 0;
    for (let 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')
}

async function handler(event) {
    let request = event.request;

    //Secret key used to verify JWT token.
    //Update with your own key.
    const secret_key = await getSecret()

    if(!secret_key) {
        return response401;
    }

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        log("Error: No JWT in the querystring");
        return response401;
    }

    const jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, secret_key);
    }
    catch(e) {
        log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    log("Valid JWT token");
    return request;
}

// get secret from key value store
async function getSecret() {
    // initialize cloudfront kv store and get the key value
    try {
        const kvsHandle = cf.kvs();
        return await kvsHandle.get(kvsKey);
    } catch (err) {
```

```
        log(`Error reading value for key: ${kvsKey}, error: ${err}`);
        return null;
    }

}

function log(message) {
    if (loggingEnabled) {
        console.log(message);
    }
}
```

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di CloudFront con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Cronologia dei documenti

La tabella seguente descrive le importanti modifiche apportate alla documentazione. CloudFront Per ricevere le notifiche sugli aggiornamenti, è possibile effettuare la sottoscrizione al feed RSS.

Modifica	Descrizione	Data
È stato aggiunto il TLS reciproco (visualizzatore)	CloudFront supporta TLS reciproco (visualizzatore).	24 novembre 2025
È stato aggiunto un campo di registro per i registri di accesso	È stato aggiunto il `connection-id` campo per i registri di accesso (registri standard) e i registri di accesso in tempo reale.	24 novembre 2025
Registri di connessione aggiunti	Sono stati aggiunti i log di connessione come nuova funzionalità di registrazione per Mutual TLS (viewer).	24 novembre 2025
Funzioni di connessione aggiunte	CloudFront supporta le funzioni di connessione per TLS reciproco (visualizzatore).	24 novembre 2025
Aggiungete il supporto per CloudFront utilizzare IPAM con il vostro indirizzo IP	CloudFront supporta l'inserimento dei propri IPv4 indirizzi tramite BYOIP di IPAM per servizi globali.	24 novembre 2025
AWS aggiornamento della politica gestita	Le politiche `CloudFrontReadOnlyAccess` e `CloudFrontFullAccess` IAM ora supportano `ec2:DescribeIpamPools` e `ec2:GetIpamPoolCidrs` agiscono.	24 novembre 2025

Aggiornamenti alle funzioni CloudFront	Questa versione aggiunge parametri per i metodi di supporto per la modifica dell'origine in CloudFront Functions. È possibile utilizzare i `originOverrides` parametri `hostHeader sni`,`allowedCertificateNames` , e.	20 novembre 2025
Aggiornamenti alle funzioni CloudFront	Aggiunto il supporto CBOR Web Tokens (CWT) per le funzioni. CloudFront	20 novembre 2025
Aggiornamenti alle funzioni CloudFront	Aggiunti metodi di supporto generali per CloudFront le funzioni.	20 novembre 2025
Politica AWS gestita aggiornata	Aggiornato `CloudFrontFullAccess` per consentire l'autorizzazione alla creazione di una risorsa AWS WAF Web ACL e l'accesso a AWS Pricing Plan Manager per creare, aggiornare, eliminare e leggere.	18 novembre 2025
Politica AWS gestita aggiornata	Aggiornato `CloudFrontReadOnlyAccess` per consentire l'autorizzazione di sola lettura a AWS Pricing Plan Manager.	18 novembre 2025

Politica AWS gestita aggiornata	Aggiornato `CloudFrontFullAccess` per consentire l'autorizzazione alla creazione di una risorsa AWS WAF Web ACL e l'accesso a AWS Pricing Plan Manager per creare, aggiornare, eliminare e leggere.	18 novembre 2025
Politica AWS gestita aggiornata	Aggiornato `CloudFrontReadOnlyAccess` per consentire l'autorizzazione di sola lettura a AWS Pricing Plan Manager.	18 novembre 2025
CloudFront supporta piani tariffari forfettari	Ora puoi abbonare le tue distribuzioni a un CloudFront piano tariffario forfettario.	18 novembre 2025
Anycast statico IPs	Ora puoi scegliere tra solo IPv4 indirizzi o entrambi IPv4 e IPv6 indirizzi (dualstack).	5 novembre 2025
Aggiunto il supporto per la condivisione delle origini VPC tra Account AWS	Puoi creare una condivisione di risorse e aggiungervi origini VPC. Ciò consente di mantenere separate le origini e le CloudFront distribuzioni del VPC Account AWS, consentendo all'organizzazione di mantenere i requisiti per più account. Altri Account AWS possono associare le origini VPC condivise per le proprie CloudFront distribuzioni.	5 novembre 2025

Aggiunta policy di sicurezza visualizzatore	È stata aggiunta la politica di TLSv1 sicurezza .2_2025. • Protocolli e cifrari supportati tra visualizzatori e CloudFront • Politica di sicurezza (versione minima) SSL/TLS	10 ottobre 2025
Aggiunti algoritmi di scambio di chiavi post-quantistico (PQ)	Aggiunti due nuovi algoritmi di scambio di chiavi PQ alle CloudFront politiche TLS.	4 settembre 2025
IPv6 richieste di origine	Quando utilizzi un'origin e personalizzata (escluse le origini Amazon S3 e VPC), puoi personalizzare le impostazioni di origine per la tua distribuzione per scegliere come CloudFront connettersi alla tua origine utilizzando o gli indirizzi. IPv4 IPv6	3 settembre 2025
Aggiunta nuova policy di richiesta origine gestita	Aggiunta nuova policy di richiesta origine gestita `HostHeaderOnly` .	29 agosto 2025
CloudFront gli endpoint pubblici ora supportano IPv6	Consulta gli CloudFront endpoint e le quote Amazon in Riferimenti generali di AWSe il relativo Servizi AWS supporto IPv6 nella Amazon VPC User Guide.	21 agosto 2025

Aggiunta policy di sicurezza visualizzatore	Aggiunta TLSv1 .3_2025, una nuova policy di sicurezza solo per TLS 1.3.	7 agosto 2025
Aggiunte nuove impostazioni di timeout di origine	Aggiunto il timeout di completamento della risposta per tutte le origini e aggiunto il timeout di risposta (timeout di lettura dell'origine) per le origini S3.	30 luglio 2025
Aggiunte impostazioni preconfigurate della distribuzione standard	Aggiunte impostazioni preconfigurate per la distribuzione standard.	17 giugno 2025
Aggiunto nuovo flusso di lavoro della console per la configurazione del dominio di distribuzione standard	Aggiunto nuovo flusso di lavoro della console per la configurazione del dominio di distribuzione standard.	17 giugno 2025
Parametri di esempio aggiunti	Aggiunti esempi per l'utilizzo dei parametri con nomi di dominio e percorsi di origine nei tenant di distribuzione.	17 giugno 2025
Aggiunto supporto CloudFront alle funzioni per CloudFront SaaS Manager	Aggiunte le funzioni di assistente di gestione e il campo `endpoint` per l'oggetto `context`.	2 maggio 2025
Aggiornamenti alla registrazione standard (v2)	Aggiunta la variabile di partizione `{distributionid}` per supportare l'invio dei log di accesso ad AWS Glue.	1 maggio 2025

Aggiornamenti alle politiche CloudFront gestite	Aggiunte autorizzazioni ACM alle policy gestite `CloudFrontReadOnlyAccess` e `CloudFrontFullAccess` .	28 aprile 2025
Aggiunto il supporto per la distribuzione multi-tenant e i tenant di distribuzione	Puoi creare una distribuzione multi-tenant per impostare parametri di distribuzione comuni in base al tipo di origine. Quindi, puoi riutilizzare la distribuzione multi-tenant per creare più tenant di distribuzione che condividono tali impostazioni. Poi quindi personalizzare specifici tenant di distribuzione man mano che aggiungi ulteriori siti Web o applicazioni.	28 aprile 2025
Aggiornamenti per le funzioni Lambda@Edge	Le funzioni Lambda @Edge ora supportano controlli di registrazione avanzati e la personalizzazione del nome del CloudWatch gruppo di log.	7 aprile 2025
Anycast statico IPs	Puoi usare Anycast static IPs per abilitare il routing dei domini apex direttamente alle tue distribuzioni. CloudFront	4 aprile 2025
Aggiunti ulteriori metodi di supporto per la modifica dell'origine	Sono stati aggiunti i metodi di supporto and `selectRequestOriginById()` Functions. `createRequestOriginGroup()` CloudFront	2 aprile 2025

Aggiornamenti alla registrazione standard (v2)	Aggiunta la variabile di partizione `{accountid}` e percorsi suffisso di esempio per la consegna di log di accesso ad Amazon S3.	14 febbraio 2025
Aggiunti campi aggiuntivi di registro degli accessi in tempo reale per la registrazione standard (v2)	È possibile specificare i campi del registro degli `c-country` accessi `cache-behavior-path-pattern` in tempo reale quando si abilita la registrazione standard (v2).	31 gennaio 2025
Lambda@Edge supporta le versioni di runtime più recenti	Lambda @Edge ora supporta le funzioni Lambda con il runtime Node.js 22.	22 novembre 2024
Supporto alla resilienza sensibile alla qualità dei media per CloudFront	È possibile utilizzare la funzionalità Media Quality-Aware Resiliency (MQAR) in modo che scelga CloudFront automaticamente l'origine in un gruppo di origini con il punteggio di qualità multimediale più elevato.	21 novembre 2024
Metodo di assistente di gestione per la modifica dell'origine	Aggiunto un nuovo metodo di supporto CloudFront Functions per la modifica dell'origine.	21 novembre 2024
VPC Origins	Utilizza le origini CloudFront VPC per limitare l'accesso a un'origine di Application Load Balancer, Network Load Balancer o istanza. EC2	20 novembre 2024

Aggiornamenti alla policy gestita	È stata aggiornata la policy gestita `CloudFrontFullAccess` .	20 novembre 2024
Anycast statico IPs	Puoi richiedere Anycast static IPs da utilizzare con CloudFront le tue distribuzioni.	20 novembre 2024
Aggiunto supporto per la registrazione di log standard	CloudFront supporta la registrazione standard (v2) e l'invio dei log ad Amazon CloudWatch Logs, Amazon Data Firehose e Amazon Simple Storage Service (Amazon S3).	20 novembre 2024
Aggiunto il supporto per gRPC	CloudFront ora supporta le richieste gRPC per la tua distribuzione.	20 novembre 2024
Aggiunta una nuova policy gestita per VPC Origins	Aggiunta nuova policy gestita `AWSCloudFrontVPCOriginServiceRolePolicy` .	20 novembre 2024
Lambda@Edge supporta le versioni di runtime più recenti	Lambda @Edge ora supporta le funzioni Lambda con il runtime Python 3.13.	13 novembre 2024
AWS Config Valuta con regole	Valuta le tue CloudFront configurazioni con AWS Config Rules.	20 settembre 2024
Aggiunti ulteriori contenuti relativi alla risoluzione dei problemi	Aggiunti ulteriori contenuti relativi alla risoluzione dei problemi per i codici di stato di risposta di errore HTTP 4xx e 5xx.	26 agosto 2024

Aggiunte nuove policy della cache gestite	Aggiunte nuove policy della cache gestite `UseOriginCacheControlHeaders` e `UseOriginCacheControlHeaders-QueryStrings` .	24 maggio 2024
Aggiunto supporto per il controllo di accesso origine	Ora puoi creare un controllo di accesso all'origine (OAC) per AWS Elemental MediaPackage V2 e AWS Lambda l'URL della funzione.	11 aprile 2024
Campi di registro degli accessi in tempo reale per CMCD	Aggiunti 18 campi Common Media Client Data (CMCD) per i log di accesso in tempo reale.	9 aprile 2024
Iniziare con una distribuzione CloudFront standard	Tutorial aggiornato per una distribuzione standard che utilizza un'origine Amazon S3 con controllo di accesso origine (OAC).	18 marzo 2024
Esempi di codice per l' CloudFront utilizzo AWS SDKs	Sono stati aggiunti esempi di codice che mostrano come utilizzarlo CloudFront con un kit di sviluppo AWS software (SDK). Gli esempi sono suddivisi in estratti di codice che mostrano come richiamare le singole funzioni di servizio ed esempi che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.	16 febbraio 2024

AWS policy gestita	Le policy IAM `CloudFrontReadOnlyAccess` e `CloudFrontFullAccess` ora supportano le operazioni `KeyValueStore` .	19 dicembre 2023
JavaScript runtime 2.0	Aggiunte funzionalità JavaScript di runtime 2.0 per CloudFront Functions.	21 novembre 2023
CloudFront KeyValueStore	Amazon CloudFront ora supporta CloudFront KeyValueStore. Questa funzionalità è un datastore di valori chiave sicuro, globale e a bassa latenza che consente l'accesso in lettura dall'interno di Functions. CloudFront È possibile abilitare una logica personalizzabile avanzata nelle postazioni periferiche. CloudFront	21 novembre 2023
Lambda@Edge supporta le versioni di runtime più recenti	Lambda@Edge ora supporta le funzioni Lambda con il runtime Node.js 20.	15 novembre 2023
Dashboard di sicurezza	CloudFront crea una dashboard di sicurezza quando si crea una distribuzione. Abilita AWS WAF, gestisci le restrizioni geografiche e visualizza dati di alto livello per richieste, bot e log.	8 novembre 2023

Ordinamento delle stringhe di query nelle funzioni	CloudFront ora supporta l'ordinamento delle stringhe di query utilizzando Functions. CloudFront	3 ottobre 2023
AWS WAF raccomandazioni di sicurezza	Amazon CloudFront ora mostra i consigli AWS WAF di sicurezza sulla CloudFront console.	26 settembre 2023
Supporto per la distribuzione di contenuti della cache non aggiornati (scaduti)	CloudFront supporta le direttive di controllo `Stale-While-Revalidate` e `Stale-If-Error` cache.	15 maggio 2023
Abilita AWS WAF le protezioni con un clic	Un metodo semplificato per aggiungere protezioni AWS WAF di sicurezza alle distribuzioni. CloudFront	10 maggio 2023
Abilita ACLs i nuovi bucket S3 utilizzati per i log standard	Sono stati aggiunti una nota e collegamenti per gestire l'impostazione ACL predefinita per i nuovi bucket S3.	11 aprile 2023
Creazione di un'origine utilizzando Lambda per oggetti Amazon S3	Puoi utilizzare un alias del punto di accesso Lambda per oggetti Amazon S3 come un'origine per la tua distribuzione.	31 marzo 2023
Personalizza lo stato e il corpo dell'HTTP utilizzando le funzioni CloudFront	È possibile utilizzare CloudFront Functions per aggiornare il codice di stato della risposta del visualizzatore e sostituire o rimuovere il corpo della risposta.	29 marzo 2023

Aggiunte opzioni con caratteri jolly per le intestazioni CORS per porte	È ora possibile includere configurazioni con caratteri jolly per porte in intestazioni di controllo degli accessi CORS.	20 marzo 2023
È stato aggiunto un nuovo collegamento per la Guida per AWS Security Hub CSPM l'utente	Lingua aggiornata e collegamento aggiunto ai CloudFront controlli Amazon riorganizzati nella Guida per l'AWS Security Hub CSPM utente.	9 marzo 2023
CloudFront ora supporta gli elenchi di blocco («tutti tranne») nelle politiche di Origin Request	Utilizza gli elenchi di blocco nelle politiche di richiesta di origine per includere tutte le stringhe di query, le intestazioni HTTP o i cookie, ad eccezione di quelli specificati, nelle richieste CloudFront inviate all'origine.	22 febbraio 2023
CloudFront aggiunge una nuova politica di richiesta di origine gestita per inoltrare tutte le intestazioni dei visualizzatori tranne l'intestazione Host	Utilizza CloudFront la nuova politica di richiesta di origine gestita per includere tutte le intestazioni della richiesta del visualizzatore, ad eccezione dell'`Host`intestazione, nelle richieste CloudFront inviate all'origine.	22 febbraio 2023
Restrizioni aggiornate su Lambda@Edge	Lambda@Edge supporta le configurazioni di gestione del runtime Lambda impostate su Auto.	16 febbraio 2023

È stata aggiornata la guida IAM per CloudFront	Guida aggiornata per l'allinea mento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	15 febbraio 2023
Sicurezza migliorata con il controllo degli accessi dell'orig ine	Ora puoi proteggere MediaStore le origini autorizza ndo l'accesso solo alle CloudFront distribuzioni designate.	9 febbraio 2023
Nuove intestazioni per determinare la struttura dell'intestazione del visualizz atore	Ora è possibile aggiunger e l'ordine e il numero delle intestazioni per identificare il visualizzatore in base alle intestazioni che invia.	13 gennaio 2023
Lambda@Edge supporta le versioni di runtime più recenti	Lambda@Edge ora supporta le funzioni Lambda con il runtime Node.js 18.	12 gennaio 2023
Rimozione delle intestazioni di risposta utilizzando una policy delle intestazioni di risposta	Ora puoi utilizzare una politica di intestazioni di CloudFront risposta per rimuovere dall'orig ine le intestazioni CloudFron t ricevute nella risposta. Le intestazioni specifica te non sono incluse nella risposta CloudFront inviata agli spettatori.	3 gennaio 2023
Implementazione continua per testare in sicurezza le modifiche alla configurazione	È ora possibile implementare le modifiche alla configura zione CDN eseguendo test con un sottoinsieme del traffico di produzione.	18 novembre 2022

Rilascio dell'intestazione `CloudFront-Viewer-JA3-Fingerprint`	Ora puoi usare l' JA3 impronta digitale per determinare se la richiesta proviene da un client noto.	16 novembre 2022
Aggiunte opzioni con caratteri jolly per le intestazioni CORS	È ora possibile utilizzare varie configurazioni con caratteri jolly in alcune intestazioni di controllo degli accessi CORS.	11 novembre 2022
Metriche aggiuntive per le distribuzioni CloudFront	Support per `MonitoringSubscription` l' CloudFront API e CloudFormation.	3 ottobre 2022
Sicurezza migliorata con il controllo degli accessi dell'origine	Ora puoi proteggere le origini di Amazon S3 permettendo l'accesso solo alle distribuzioni designate. CloudFront	24 agosto 2022
Supporto HTTP/3 per le distribuzioni CloudFront	Ora puoi scegliere HTTP/3 per la tua distribuzione. CloudFront	15 agosto 2022
Aggiungi i dettagli dell'handshake all'intestazione CloudFront-Viewer-TLS	È possibile visualizzare nuovamente le informazioni sull' SSL/TLS handshake utilizzato.	27 giugno 2022
Nuova metrica nell'intestazione Server-Timing	Aggiunta la nuova metrica `cdn-downstream-fbl` alle intestazioni `Server-Timing` .	13 giugno 2022

Nuova intestazione per ottenere informazioni sulla versione e sulla cifratura TLS	È ora possibile utilizzare l'`CloudFront-Viewer-TLS` intestazione per ottenere informazioni sulla versione di TLS (o SSL) e sul codice utilizzato per la connessione tra il visualizzatore e. CloudFront	23 maggio 2022
Nuova metrica per le funzioni FunctionThrottles CloudFront	Con Amazon CloudWatch, ora puoi monitorare il numero di volte in cui una CloudFront funzione è stata limitata in un determinato periodo di tempo.	4 maggio 2022
CloudFront supporta la funzione Lambda URLs	Se crei un'applicazione web serverless utilizzando le funzioni Lambda con URLs funzione, ora puoi CloudFront aggiungere una serie di vantaggi.	6 aprile 2022
Intestazione Server-Timing nelle risposte HTTP	Ora puoi abilitare l'`Server-Timing` intestazione nelle risposte HTTP inviate da CloudFront per visualizzare le metriche che possono aiutarti a ottenere informazioni sul comportamento e le prestazioni di. CloudFront	30 marzo 2022
Usa AWS-managed prefix list per limitare il traffico in entrata	Ora puoi limitare il traffico HTTP e HTTPS in entrata alle tue origini solo dagli indirizzi IP che appartengono ai server rivolti all' CloudFrontorigine.	7 febbraio 2022

Nuova funzionalità	CloudFront aggiunge il supporto per le politiche relative alle intestazioni di risposta, che consentono di specificare le intestazioni HTTP da CloudFront aggiungere alle risposte HTTP inviate ai visualizzatori (browser Web o altri client). È possibile specificare le intestazioni desiderate (e i relativi valori) senza apportare modifiche all'origine o scrivere alcun codice. Per ulteriori informazioni, consulta Aggiungere o rimuovere intestazioni HTTP nelle risposte. CloudFront	2 novembre 2021
Nuova intestazione della richiesta `CloudFront-Viewer-Address`	CloudFront aggiunge il supporto per una nuova intestazione`CloudFront-Viewer-Address` , che contiene l'indirizzo IP del visualizzatore a cui ha inviato la richiesta HTTP. CloudFront Per ulteriori informazioni, consulta Aggiungere intestazioni di CloudFront richiesta.	25 ottobre 2021
Lambda @Edge supporta la nuova versione di runtime	Lambda@Edge ora supporta le funzioni Lambda con runtime Python 3.9. Per ulteriori informazioni, consulta Runtime supportati.	22 settembre 2021

AWS aggiornamento gestito delle politiche	CloudFront ha aggiornato la CloudFrontReadOnly Accesspolitica. Per ulteriori informazioni, consulta CloudFront gli aggiornamenti delle politiche AWS gestite.	08 settembre 2021
Nuova funzionalità	CloudFront ora supporta i certificati ECDSA per le connessioni HTTPS rivolte agli spettatori. Per ulteriori informazioni, consulta Protocolli e cifrari supportati tra i visualizzatori e CloudFront Requisiti per l'utilizzo dei certificati con. SSL/TLS CloudFront	14 luglio 2021
Nuova funzionalità	CloudFront ora supporta più modi per spostare un nome di dominio alternativo da una distribuzione all'altra, senza contattare. Supporto Per ulteriori informazioni, consulta Spostamento di un nome di dominio alternativo su un'altra distribuzione.	7 luglio 2021
Nuova politica di sicurezza	CloudFront ora supporta una nuova politica di sicurezza, TLSv1.2_2021, con un set più piccolo di cifrari supportati. Per ulteriori informazioni, consulta Protocolli e cifrari supportati tra visualizzatori e. CloudFront	23 giugno 2021

Nuova funzionalità	Amazon CloudFront ora supporta CloudFront Functions , una funzionalità nativa CloudFront che consente di scrivere funzioni leggere per personalizzazioni CDN JavaScript su larga scala e sensibili alla latenza. Per ulteriori informazioni, consulta Personalizzazione all'edge con Functions. CloudFront	3 maggio 2021
Lambda @Edge supporta versioni di runtime più recenti	Lambda@Edge ora supporta le funzioni Lambda con il runtime Node.js 14. Per ulteriori informazioni, consulta Runtime supportati.	29 aprile 2021
Rimuovi la documentazione per le distribuzioni RTMP	Amazon ha CloudFront dichiarato obsolete le distribuzioni RTMP (Real-Time Messaging Protocol) il 31 dicembre 2020. La documentazione per le distribuzioni RTMP è ora rimossa dalla Amazon CloudFront Developer Guide.	10 febbraio 2021
Nuova opzione di prezzo	Amazon CloudFront introduce il CloudFront Security Savings Bundle, un modo semplice per risparmiare fino al 30% sugli CloudFront addebiti in bolletta AWS . Per ulteriori informazioni, consulta il Savings Bundle. FAQs	5 febbraio 2021

Nuovo tutorial	L'Amazon CloudFront Developer Guide ora include un tutorial per usare Amazon CloudFront per limitare l'accesso a un Application Load Balancer in ELB. Per ulteriori informazioni, consulta Limitazione dell'accesso ai servizi di Application Load Balancer.	18 dicembre 2020
Nuova opzione per la gestione delle chiavi pubbliche	CloudFront ora supporta la gestione delle chiavi pubbliche per i cookie firmati URLs e firmati tramite la CloudFron t console e l'API, senza richiedere l'accesso all'utent e Account AWS root. Per ulteriori informazioni, consulta Specificare i firmatari che possono creare cookie firmati URLs e firmati.	22 ottobre 2020
Nuova funzionalità: Origin Shield	CloudFront ora supporta CloudFront Origin Shield, un livello aggiuntivo dell'infr astruttura di CloudFront caching che aiuta a ridurre al minimo il carico dell'origine, a migliorarne la disponibilità e a ridurne i costi operativi. Per ulteriori informazioni, consulta Usare Amazon CloudFront Origin Shield.	20 ottobre 2020

Nuovo formato di compressione	CloudFront ora supporta la formazione di compressione Brotli quando si configura CloudFront per comprimere oggetti in CloudFront posizioni periferiche. È inoltre possibile configurare CloudFront la memorizzazione nella cache degli oggetti Brotli utilizzando un'intestazione normalizzata. `Accept-Encoding` Per ulteriori informazioni, consulta Fornitura di file compressi e Supporto della compressione.	14 settembre 2020
Nuovo protocollo TLS	CloudFront ora supporta il protocollo TLS 1.3 per le connessioni HTTPS tra visualizzatori e distribuzioni. CloudFront TLS 1.3 è abilitato per impostazione predefinita in tutte le politiche di sicurezza. CloudFront Per ulteriori informazioni, consulta Protocolli e cifrari supportati tra visualizzatori e. CloudFront	3 settembre 2020

Nuovi registri di accesso in tempo reale	CloudFront ora supporta registri di accesso configura bili in tempo reale. Con i log di accesso in tempo reale, è possibile ottenere informazi oni sulle richieste effettuate a una distribuzione in tempo reale. È possibile utilizzare i log di accesso in tempo reale per monitorare, analizzare e intraprendere azioni in base alle prestazioni di distribuz ione dei contenuti. Per ulteriori informazioni, consulta Log in tempo reale.	31 agosto 2020
Supporto API per metriche aggiuntive	CloudFront ora supporta l'abilitazione di otto metriche aggiuntive in tempo reale con l' CloudFront API. Per ulteriori informazioni, consulta Attivazio ne di metriche aggiuntive.	28 agosto 2020
Nuove intestazioni CloudFront HTTP	CloudFront sono state aggiunte intestazioni HTTP aggiuntive per determinare le informazioni sul visualizz atore come il tipo di dispositi vo, la posizione geografica e altro. Per ulteriori informazioni, consulta Aggiungere intestazi oni di CloudFront richiesta.	23 luglio 2020

Nuova funzionalità	CloudFront ora supporta i criteri di cache e i criteri di richiesta di origine, che offrono un controllo più granulare sulla chiave della cache e sulle richieste di origine per le distribuzioni. CloudFron t Per ulteriori informazioni, consulta Controllo della chiave della cache e Controllo delle richieste origine.	22 luglio 2020
Nuova politica di sicurezza	CloudFront ora supporta una nuova politica di sicurezza, TLSv1.2_2019, con un set più piccolo di cifrari supportati. Per ulteriori informazioni, consulta Protocolli e cifrari supportati tra visualizzatori e. CloudFront	8 luglio 2020
Nuove impostazioni per controllare i timeout e i tentativi di origine	CloudFront ha aggiunto nuove impostazioni che controllano i timeout e i tentativi di origine. Per ulteriori informazioni, consulta Controllo dei timeout e dei tentativi di origine.	5 giugno 2020
Nuova documentazione per iniziare a creare un CloudFront sito Web statico sicuro	Inizia CloudFront creando un sito Web statico sicuro utilizzando Amazon S3, CloudFront Lambda @Edge e altro, tutti implementati con. CloudFormation Per ulteriori informazioni, consulta Guida introduttiva a un sito Web statico protetto.	2 giugno 2020

Lambda @Edge supporta versioni di runtime più recenti	Lambda@Edge ora supporta le funzioni Lambda con runtime Node.js 12 e Python 3.8. Per ulteriori informazioni, consulta Runtime supportati.	27 febbraio 2020
Nuove metriche in tempo reale in CloudWatch	Amazon CloudFrontnow offre otto parametri aggiuntivi in tempo reale su Amazon CloudWatch. Per ulteriori informazioni, consulta Attivazione di metriche di CloudFront distribuzione aggiuntive.	19 dicembre 2019
Nuovi campi nei log di accesso	CloudFront aggiunge sette nuovi campi ai log di accesso. Per ulteriori informazioni, consulta Campi dei file di log standard.	12 dicembre 2019
AWS WordPress plugin	Puoi utilizzare il AWS WordPress plug-in per offrire ai visitatori del tuo WordPress sito Web un'esperienza di visualizzazione accelerata utilizzando CloudFront. (Aggiornamento: a partire dal 30 settembre 2022, il WordPress plugin AWS for è obsoleto.)	30 ottobre 2019

Politiche di autorizzazione IAM basate su tag e a livello di risorsa	CloudFront ora supporta due modi aggiuntivi per specifica re le politiche di autorizza zione IAM: autorizzazioni basate su tag e autorizza zioni a livello di risorsa. Per ulteriori informazioni, consulta Gestione dell'accesso alle risorse.	8 agosto 2019
Support per il linguaggio di programmazione Python	Ora puoi utilizzare il linguaggi o di programmazione Python per sviluppare funzioni in Lambda@Edge, oltre a Node.js. Per funzioni di esempio che coprono diversi scenari, consulta Funzioni di esempio Lambda@Edge.	1 agosto 2019
Grafici di monitoraggio aggiornati	Aggiornamenti dei contenuti per descrivere nuovi modi per monitorare le funzioni Lambda associate alle CloudFron t distribuzioni direttamente dalla CloudFront console per tracciare ed eseguire più facilmente il debug degli errori. Per ulteriori informazi oni, consulta Monitoraggio di CloudFront.	20 giugno 2019

Contenuti di sicurezza consolidati	Un nuovo capitolo sulla sicurezza consolida le informazioni sulle CloudFront funzionalità e sull'implementazione della protezione dei dati, dell'IAM, della registrazione, della conformità e altro ancora. Per ulteriori informazioni, consulta Sicurezza.	24 maggio 2019
La convalida del dominio è ora richiesta	CloudFront ora richiede l'utilizzo di un certificato SSL per verificare di disporre dell'autorizzazione a utilizzare un nome di dominio alternativo con una distribuzione. Per ulteriori informazioni, consulta Utilizzo di HTTPS e di nomi di dominio alternativi.	9 aprile 2019
Nome file PDF aggiornato	Il nuovo nome di file per l'Amazon CloudFront Developer Guide è: AmazonCloudFront _. DevGuide Il nome precedente era: cf-dg.	7 gennaio 2019

Nuove funzionalità	CloudFront ora supporta WebSocket un protocollo basato su TCP utile quando sono necessarie connessioni di lunga durata tra client e server. Ora puoi anche configurare CloudFront con Origin Failover per scenari che richiedono un'elevata disponibilità. Per ulteriori informazioni, consulta Utilizzo WebSocket con le CloudFront distribuzioni e Ottimizzazione dell'alta disponibilità con CloudFront Origin Failover.	20 novembre 2018
Nuova funzionalità	CloudFront ora supporta la registrazione dettagliata degli errori per le richieste HTTP che eseguono funzioni Lambda. È possibile archiviare i log CloudWatch e utilizzarli per risolvere gli errori HTTP 5xx quando la funzione restituisce una risposta non valida. Per ulteriori informazioni, consulta CloudWatch Metriche e CloudWatch registri per le funzioni Lambda.	8 Ottobre 2018

Nuova funzionalità	Ora puoi fare in modo che Lambda@Edge esponga il corpo in una richiesta per metodi HTTP con possibilità di scrittura (POST, PUT, DELETE e così via), in modo che tu possa accedervi dalla tua funzione Lambda. È possibile scegliere le autorizzazioni di accesso in sola lettura, oppure è possibile specificare che sarà possibile sostituire il corpo. Per ulteriori informazioni, consulta Accesso al corpo della richiesta scegliendo l'opzione Includi corpo.	14 agosto 2018
Nuova funzionalità	CloudFront ora supporta la pubblicazione di contenuti compressi utilizzando brotli o altri algoritmi di compressione, in aggiunta o al posto di gzip. Per ulteriori informazioni, consulta Distribuzione di file compressi.	25 luglio 2018
Riorganizzazione	L'Amazon CloudFront Developer Guide è stata riorganizzata per semplificare la ricerca di contenuti correlati e migliorare la scansionabilità e la navigazione.	28 giugno 2018

Nuova funzionalità	Lambda@Edge ora consente di personalizzare ulteriormente la distribuzione di contenuti archiviati in un bucket Amazon S3, permettendo di accedere a ulteriori intestazioni, tra cui le intestazioni personalizzate, dagli eventi di origine. Per ulteriori informazioni, consulta questi esempi che mostrano la personalizzazione dei contenuti in base alla posizione del visualizzatore e al tipo di dispositivo del visualizzatore.	20 marzo 2018
Nuova funzionalità	Ora puoi usare Amazon CloudFront per negoziare connessioni HTTPS alle origini utilizzando Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA utilizza chiavi più piccole che sono più veloci, ma altrettanto sicure quanto il precedente algoritmo RSA. Per ulteriori informazioni, consulta SSL/TLS Protocolli e cifrari supportati per la comunicazione tra e l'origine e Informazioni sui cifrari RSA CloudFront ed ECDSA.	15 marzo 2018

Nuova funzionalità	Lambda @Edge ti consente di personalizzare le risposte agli errori dalla tua origine, consentendoti di eseguire funzioni Lambda in risposta agli errori HTTP che Amazon CloudFrontreceives ha generato dalla tua origine. Per ulteriori informazioni, consulta questi esempi che mostrano i reindirizzamenti a un'altra posizione e la generazione della risposta con codice di stato 200 (OK).	21 dicembre 2017
Nuova funzionalità	Una nuova CloudFront funzionalità, la crittografia a livello di campo, consente di migliorare ulteriormente la sicurezza dei dati sensibili , come i numeri di carta di credito o le informazioni di identificazione personale (PII) come i numeri di previdenza sociale. Per ulteriori informazioni, consulta Utilizzo della crittografia a livello di campo per proteggere dati sensibili.	14 dicembre 2017
Cronologia dei documenti archiviata	La cronologia documenti più vecchia è stata archiviata.	1° dicembre 2017

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.