aws

Guida per gli sviluppatori

Amazon CloudFront

Amazon CloudFront: Guida per gli sviluppatori

Table of Contents

Che cos'è Amazon CloudFront?

Amazon CloudFront è un servizio web che velocizza la distribuzione dei tuoi contenuti web statici e dinamici, come .html, .css, .js e file di immagine, ai tuoi utenti. CloudFront distribuisce i tuoi contenuti attraverso una rete mondiale di data center denominati edge location. Quando un utente richiede i contenuti che utilizzi CloudFront, la richiesta viene indirizzata all'edge location che offre la latenza (ritardo) più bassa, in modo che i contenuti vengano forniti con le migliori prestazioni possibili.

- Se il contenuto si trova già nell'edge location con la latenza più bassa, lo CloudFront consegna immediatamente.
- Se il contenuto non si trova in quella edge location, lo CloudFront recupera da un'origine che hai definito, ad esempio un bucket Amazon S3, un MediaPackage canale o un server HTTP (ad esempio un server Web) che hai identificato come origine per la versione definitiva dei tuoi contenuti.

Ad esempio, supponiamo che tu stia servendo un'immagine da un server web tradizionale, non da. 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 velocizza la distribuzione dei contenuti indirizzando ogni richiesta utente attraverso la rete AWS backbone verso la posizione periferica più adatta a servire i contenuti. In genere, si tratta di un server CloudFront perimetrale che fornisce la consegna più rapida allo spettatore. L'utilizzo della AWS rete riduce drasticamente il numero di reti attraverso le quali devono passare le richieste degli utenti, il che 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.

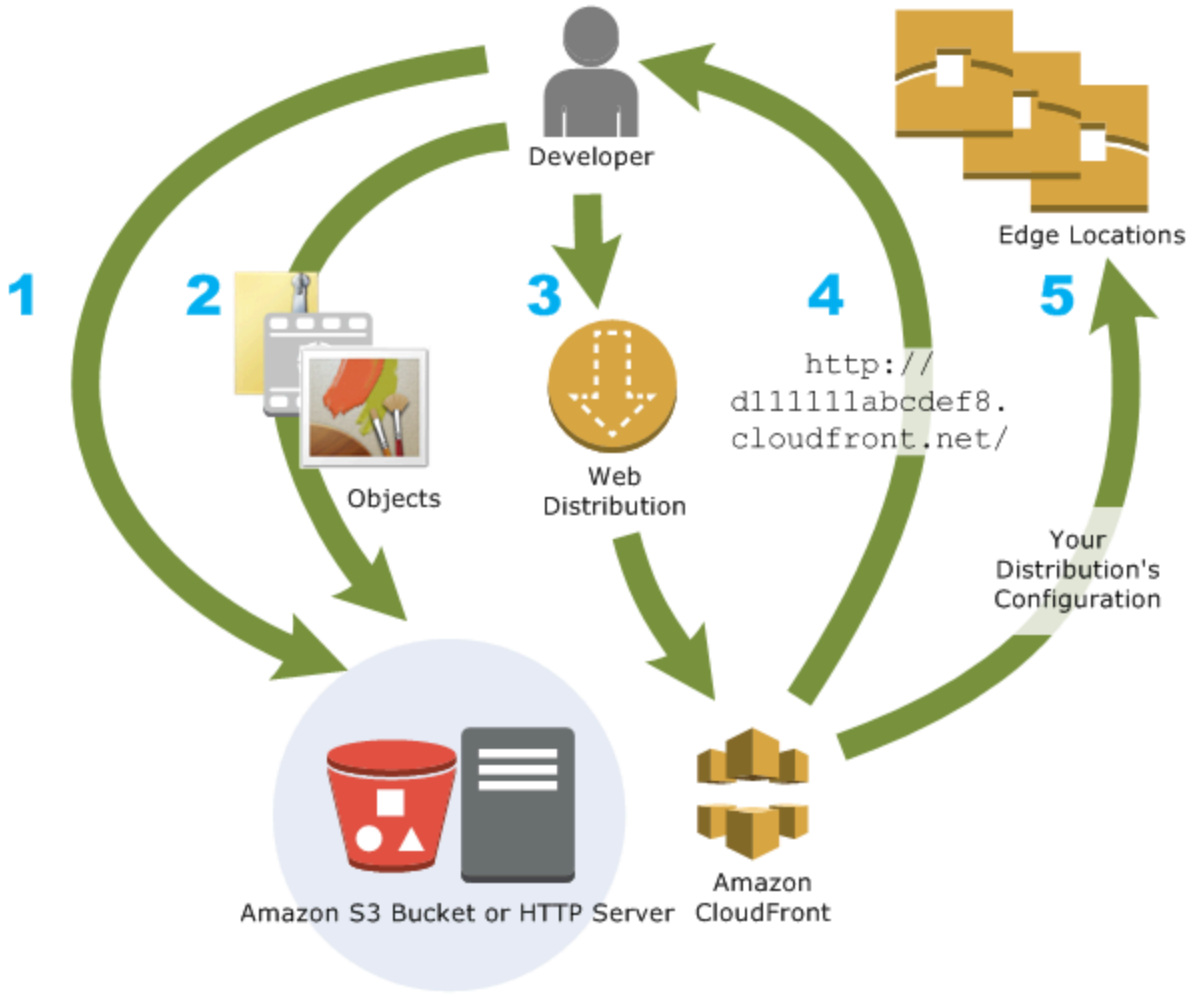
Argomenti

- Come ti configuri CloudFront per distribuire contenuti
- Prezzi

- Modi di utilizzo CloudFront
- Come distribuisce i contenuti CloudFront
- Posizioni e intervalli di indirizzi IP dei server periferici CloudFront
- Utilizzo con un SDK CloudFront AWS
- CloudFront risorse tecniche

Come ti configuri CloudFront per distribuire contenuti

Crei una CloudFront distribuzione per indicare da CloudFront dove desideri che vengano distribuiti i contenuti e i dettagli su come monitorare e gestire la distribuzione dei contenuti. Quindi CloudFront utilizza computer, server periferici, vicini ai tuoi spettatori per distribuire rapidamente i contenuti quando qualcuno desidera vederli o utilizzarli.



Come ti CloudFront configuri per distribuire i tuoi contenuti

1. Devi specificare i server di origine, come un bucket Amazon S3 o il tuo server HTTP, da cui CloudFront ottenere i file che verranno poi distribuiti da CloudFront edge location 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, in modo che chiunque conosca gli CloudFront URL dei tuoi oggetti possa accedervi. Hai anche la possibilità di conservare gli oggetti privati e di controllare chi accede agli stessi. Consulta Offri contenuti privati con URL firmati e cookie firmati.
3. Crei una CloudFront distribuzione che indica CloudFront da quali server di origine recuperare i file quando gli utenti richiedono i file tramite il tuo sito Web o la tua applicazione. Allo stesso tempo, specificate dettagli come se desiderate CloudFront registrare tutte le richieste e se desiderate che la distribuzione sia abilitata non appena viene creata.
4. CloudFront assegna un nome di dominio alla nuova distribuzione che puoi vedere nella CloudFront console o che viene restituito in 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 i contenuti) a tutte le sue edge location o punti di presenza (PoP), ovvero raccolte di server in data center geograficamente distribuiti in cui memorizza nella cache le copie dei file. CloudFront

Durante lo sviluppo del sito Web o dell'applicazione, si utilizza il nome di dominio che fornisce gli URL. CloudFront Ad esempio, se viene CloudFront restituito `d111111abcdef8.cloudfront.net` come nome di dominio per la tua distribuzione, l'URL di logo.jpg nel tuo bucket Amazon S3 (o nella directory principale di un server HTTP) è. `https://d111111abcdef8.cloudfront.net/logo.jpg`

Oppure puoi configurare CloudFront l'utilizzo del tuo nome di dominio con la tua distribuzione. In tal caso, l'URL potrebbe essere `https://www.example.com/logo.jpg`.

Facoltativamente, è possibile configurare il server di origine per aggiungere intestazioni ai file, per indicare per quanto tempo si desidera che i file rimangano nella cache nelle CloudFront edge location. 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 Gestisci la durata della permanenza dei contenuti nella cache (scadenza).

Prezzi

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

Il trasferimento dei dati dall'origine a CloudFront è sempre gratuito quando si utilizzano AWS origini come Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing o Amazon API Gateway. Quando utilizzi le origini, ti viene fatturato solo il trasferimento dei dati in uscita dal CloudFront visualizzatore. AWS

Per ulteriori informazioni, consulta CloudFront i prezzi e le domande frequenti sul pacchetto Billing and Savings Bundle.

Modi di utilizzo CloudFront

L'utilizzo CloudFront può aiutarti a raggiungere una serie di 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 velocizzare la distribuzione di contenuti statici (ad esempio immagini JavaScript, fogli di stile e così via) agli spettatori di tutto il mondo. Utilizzando CloudFront, puoi sfruttare la rete AWS backbone e i server CloudFront periferici per offrire ai tuoi spettatori 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'utilizzo combinato di S3 CloudFront offre una serie di vantaggi, tra cui la possibilità di utilizzare il controllo dell'accesso all'origine per limitare facilmente l'accesso ai contenuti S3.

Per ulteriori informazioni sull'utilizzo di S3 insieme a CloudFront, incluso un AWS CloudFormation modello per aiutarti a iniziare rapidamente, consulta Amazon S3+ CloudFront Amazon: A Match Made in the Cloud.

Esecuzione di video on-demand o in streaming live

CloudFront offre diverse opzioni per lo streaming di contenuti multimediali a spettatori globali, sia file preregistrati che eventi dal vivo.

- Per lo streaming di video on demand (VOD), puoi utilizzarlo CloudFront per lo streaming in formati comuni come MPEG DASH, Apple HLS, Microsoft Smooth Streaming e CMAF, su 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, consulta. CloudFront Video on demand e video in streaming live con CloudFront

Crittografia di campi specifici durante l'elaborazione di sistema

Quando configuri HTTPS con CloudFront, hai già end-to-end connessioni 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 e quindi specifichi il set di campi che desideri crittografare con la chiave. CloudFront 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 aiutare ad autorizzare gli utenti e controllare l'accesso ai tuoi contenuti, prima di CloudFront inoltrare una richiesta all'origine.

L'utilizzo di Lambda @Edge with CloudFront consente una varietà di modi per personalizzare i contenuti distribuiti. CloudFront Per ulteriori informazioni su Lambda @Edge e su come creare e distribuire funzioni conCloudFront, consulta. Personalizzazione all'avanguardia 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

L'uso di Lambda @Edge può aiutarti a configurare la tua CloudFront distribuzione per offrire contenuti privati dalla tua origine personalizzata, oltre a utilizzare URL firmati o cookie firmati.

Per pubblicare contenuti privati utilizzando CloudFront, procedi come segue:

- Richiedere agli utenti (visualizzatori) di accedere ai contenuti utilizzando URL o cookie firmati.
- Limita l'accesso alla tua fonte in modo che sia disponibile solo sui CloudFront server di origine. 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 oppure AWS Firewall Manager, puoi utilizzare l'elenco di prefissi CloudFront gestiti per consentire il traffico in entrata verso la tua origine solo CloudFront dagli indirizzi IP rivolti all'origine.
    - Utilizza un'intestazione HTTP personalizzata per limitare l'accesso solo alle richieste provenienti da. CloudFront Per ulteriori informazioni, consulta the section called “Limita l'accesso ai file su origini personalizzate” e the section called “Aggiungi 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 "Limita l'accesso agli Application Load Balancer".

- Se l'origine personalizzata richiede una logica di controllo degli accessi personalizzata, puoi utilizzare Lambda @Edge per implementarla, come descritto in questo post del blog: Serving Private Content Using Amazon & CloudFront Lambda @Edge.

Come distribuisce i contenuti CloudFront

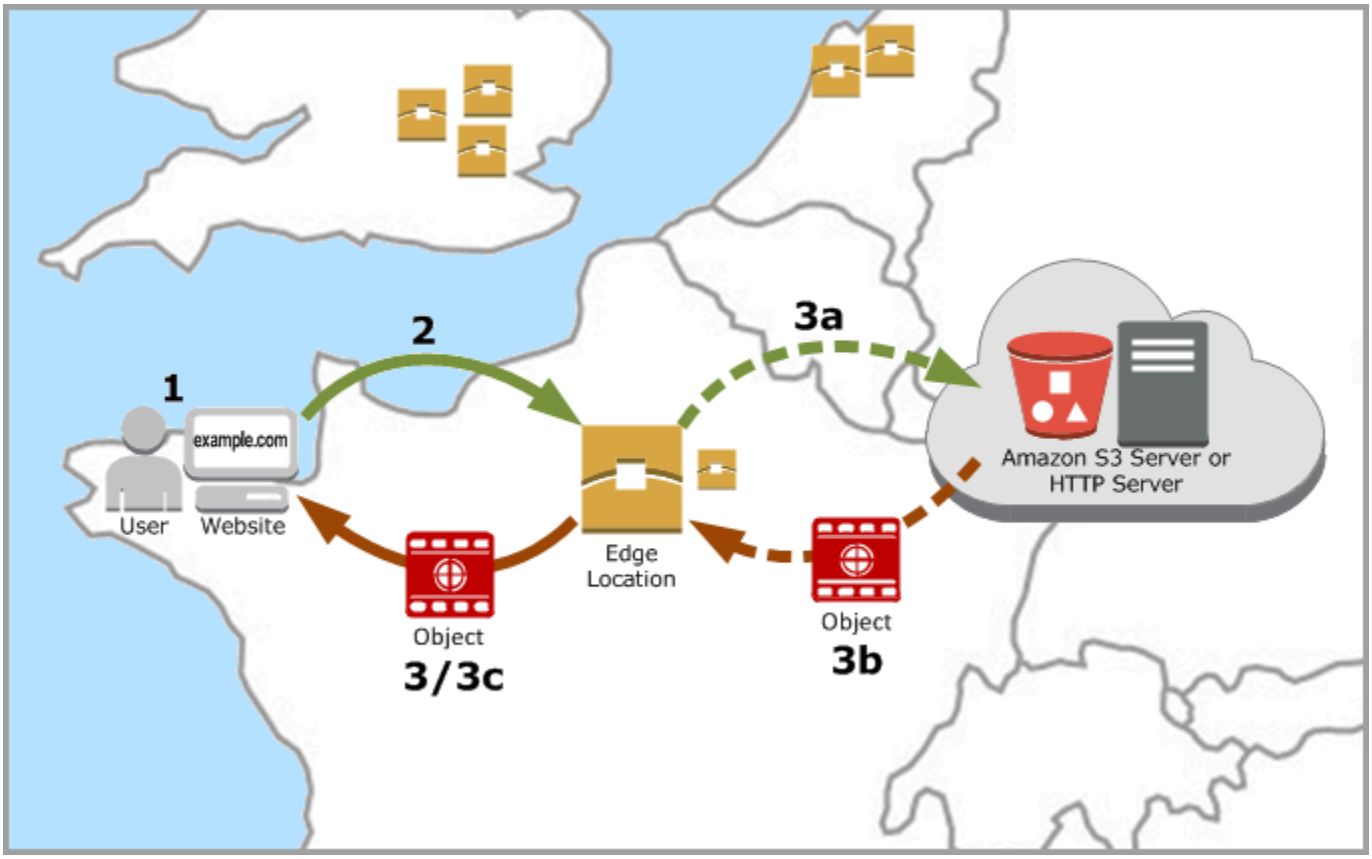
Dopo alcune configurazioni iniziali, CloudFront interagisce con il sito Web o l'applicazione e velocizza la distribuzione dei contenuti. Questa sezione spiega come vengono CloudFront visualizzati i tuoi contenuti quando gli spettatori li richiedono.

Argomenti

In che modo CloudFront fornisce i contenuti ai tuoi utenti

Dopo aver configurato CloudFront la distribuzione dei contenuti, ecco cosa succede quando gli utenti richiedono i tuoi 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. Il DNS indirizza la richiesta al CloudFront POP (edge location) che meglio soddisfa la richiesta, in genere il CloudFront POP più vicino in termini di latenza.
3. CloudFront verifica la presenza dell'oggetto richiesto nella cache. Se l'oggetto è nella cache, lo CloudFront restituisce all'utente. Se l'oggetto non è nella cache, CloudFront effettua le seguenti operazioni:
   a. CloudFront confronta la richiesta con le specifiche della tua distribuzione e inoltra la richiesta al tuo server di origine per l'oggetto corrispondente, ad esempio al tuo bucket Amazon S3 o al tuo server HTTP.
   b. Il server di origine reinvia l'oggetto alla posizione edge.
   c. Non appena il primo byte arriva dall'origine, CloudFront inizia a inoltrare l'oggetto all'utente. CloudFront aggiunge inoltre l'oggetto alla cache per la prossima volta che qualcuno lo richiede.



Come CloudFront funziona con le cache edge regionali

CloudFront i punti di presenza (noti anche come POP o edge location) assicurano che i contenuti più richiesti possano essere distribuiti rapidamente ai tuoi spettatori. CloudFront dispone inoltre di cache periferiche regionali che consentono di avvicinare una maggior parte dei tuoi contenuti ai tuoi spettatori, anche quando i contenuti non sono abbastanza popolari da rimanere in un POP, per contribuire a migliorare le prestazioni di tali contenuti.

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 CloudFront ubicazioni distribuite a livello globale, vicino ai tuoi spettatori. 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. Ciò aiuta a mantenere una maggior parte dei contenuti più vicina agli spettatori, riducendo la necessità di tornare CloudFront al server di origine e migliorando le prestazioni complessive per gli spettatori.

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. Questa posizione è in genere la CloudFront edge location più vicina in termini di latenza. Nel POP, CloudFront verifica la presenza dell'oggetto richiesto nella cache. Se l'oggetto è nella cache, lo CloudFront 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.

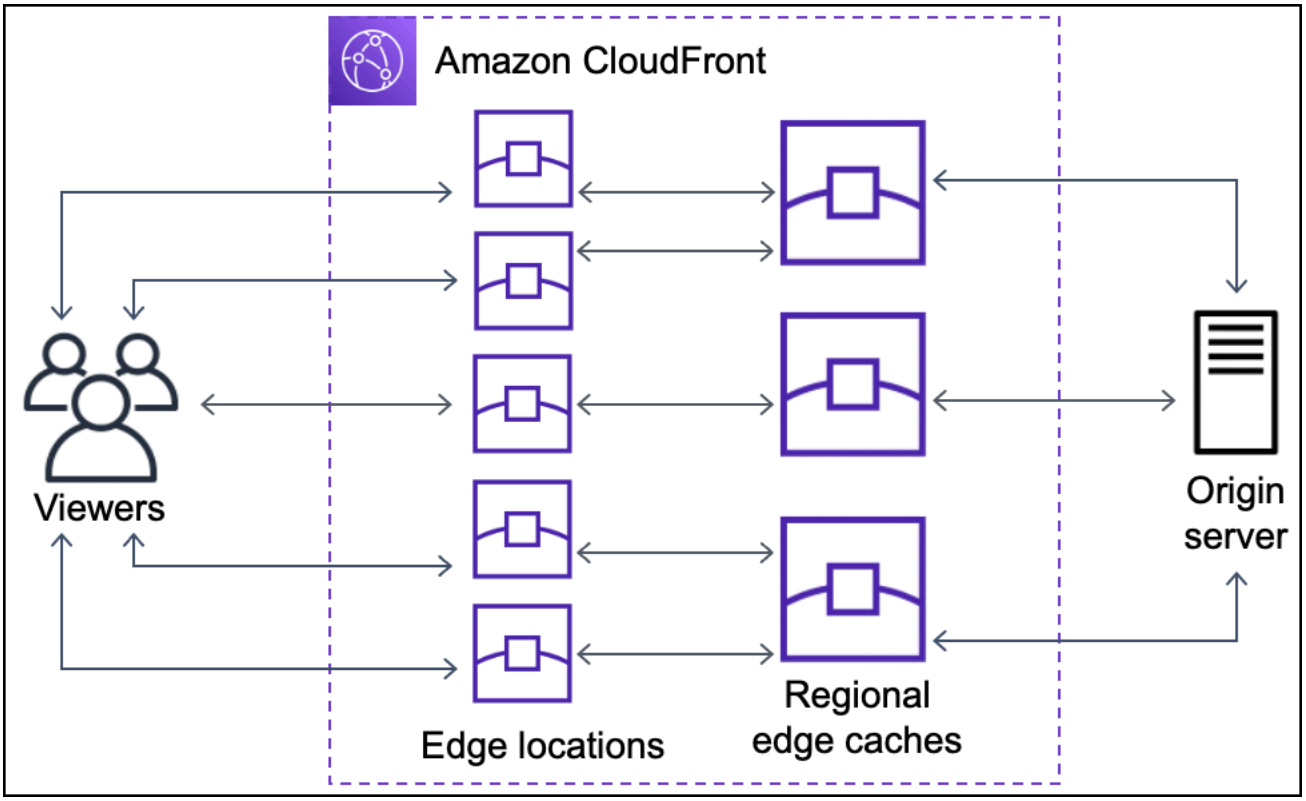
Nella cache edge regionale, controlla CloudFront nuovamente nella cache l'oggetto richiesto. Se l'oggetto è nella cache, lo CloudFront inoltra al POP che lo ha richiesto. Non appena il primo byte arriva dalla cache edge regionale, CloudFront inizia a inoltrare l'oggetto all'utente. CloudFront aggiunge inoltre l'oggetto alla cache del POP per la prossima volta che qualcuno lo richiede.

Per gli oggetti non memorizzati nella cache né nel POP né nella cache edge regionale, CloudFront confronta la richiesta con le specifiche delle distribuzioni e inoltra la richiesta al server di origine. Dopo che il server di origine ha inviato l'oggetto alla cache edge location regionale, questo viene inoltrato al POP e quindi CloudFront all'utente. In questo caso, aggiunge l'oggetto CloudFront anche alla cache nella cache edge location regionale oltre al POP per la successiva richiesta da parte di un visualizzatore. Ciò garantisce che tutti i POP di una regione condividano una cache locale, eliminando le richieste multiple ai server di origine. CloudFront mantiene inoltre connessioni permanenti con i server di origine in modo che gli oggetti vengano recuperati dalle origini il più rapidamente possibile.

> **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 prossima volta che un visualizzatore richiede l'oggetto, CloudFront torna 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 Amazon S3 e la cache edge regionale ottimale della richiesta è nella Regione AWS stessa del bucket S3, il POP salta la cache edge regionale e va direttamente al bucket S3.

Il diagramma seguente illustra come le richieste e le risposte fluiscono attraverso le edge location e le cache edge regionali. CloudFront



Posizioni e intervalli di indirizzi IP dei server periferici CloudFront

Per un elenco delle ubicazioni dei server CloudFront edge, consulta la pagina 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 gli intervalli di indirizzi IP associati ai server CloudFront edge, cerca in ip-ranges.json la seguente stringa:

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

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

Utilizza l'elenco dei prefissi CloudFront gestiti

L'elenco dei prefissi CloudFront gestiti contiene gli intervalli di indirizzi IP di tutti i server rivolti all'origine distribuiti CloudFront a livello globale. Se la tua origine è ospitata AWS e protetta da un gruppo di sicurezza Amazon VPC, puoi utilizzare l'elenco di prefissi CloudFront gestiti per consentire il traffico in entrata verso la tua origine solo dai CloudFront server rivolti all'origine, evitando che qualsiasi traffico diverso raggiunga la tua origine. CloudFront CloudFront mantiene l'elenco dei prefissi gestiti in modo che sia sempre aggiornato con gli indirizzi IP di tutti i server globali rivolti all'origine. CloudFront Con l'elenco dei prefissi CloudFront gestiti, non è necessario leggere o gestire personalmente 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, puoi creare una regola del gruppo di sicurezza che consenta l'accesso HTTPS in entrata dall'elenco dei prefissi CloudFront gestiti. Ciò consente a tutti i server globali rivolti all'origine CloudFront di raggiungere l'istanza. Se rimuovi tutte le altre regole in entrata dal gruppo di sicurezza, impedisci che qualsiasi traffico diverso dal CloudFront traffico raggiunga l'istanza.

L'elenco dei prefissi CloudFront gestiti è denominato com.amazonaws.global.cloudfront.origin-facing. Per ulteriori informazioni, consulta Use an AWS-managed prefix list nella Amazon VPC User Guide.

> **Important**
>
> L'elenco dei prefissi CloudFront gestiti 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 con un SDK CloudFront AWS

AWS I kit di sviluppo software (SDK) sono disponibili per molti 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 for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK for Go	AWS SDK for Go esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Tools for PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS 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.

CloudFront risorse tecniche

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

- AWS re:POST: un sito di domande e risposte basato sulla community in cui gli sviluppatori possono discutere di questioni tecniche relative a. CloudFront
- AWS Support Center: questo sito include informazioni sui casi di assistenza recenti, sui risultati e sui controlli sanitari. AWS Trusted Advisor Fornisce inoltre collegamenti ai forum di discussione, domande frequenti tecniche, al pannello di controllo dello stato del servizio e informazioni sui AWS Support piani.
- AWS Supporto Premium: scopri AWS Premium Support one-on-one, un canale di supporto a risposta rapida che ti aiuta a creare ed eseguire applicazioni su. AWS
- AWS IQ: fatti aiutare da professionisti ed esperti AWS certificati.

Inizia con CloudFront

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

L'Configurazioneargomento 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 di distribuzione di base mostra come configurare il controllo dell'accesso all'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 tuo 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

Configurazione

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 pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.

2. Segui le istruzioni online.

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

   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 procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

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

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. 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 Centro identità IAM.

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

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

Accedi come utente con accesso amministrativo

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

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

Assegna l'accesso ad altri utenti

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

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

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

Scegli come accedere CloudFront

Puoi accedere ad Amazon CloudFront nei seguenti modi:

- AWS Management Console— Le procedure riportate in questa guida spiegano come utilizzarlo AWS Management Console per eseguire attività.
- AWS SDK: se utilizzi un linguaggio di programmazione che AWS fornisce un SDK per, puoi utilizzare un SDK per accedere. CloudFront Gli SDK semplificano l'autenticazione, si integrano facilmente con il tuo ambiente di sviluppo e forniscono l'accesso ai comandi. CloudFront Per ulteriori informazioni, consulta Utilizzo con un SDK CloudFront 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 AWS CLI, consulta Installare o aggiornare alla versione più recente di AWS CLI nella Guida per l'AWS Command Line Interface utente.
- Strumenti per Windows PowerShell: se hai esperienza con Windows PowerShell, potresti preferire utilizzarli AWS Tools for Windows PowerShell. Per ulteriori informazioni, consulta Installazione dell' AWS Tools for Windows PowerShell nella Guida per l'utente dell'AWS Tools for Windows PowerShell .

Inizia con una CloudFront distribuzione di base

Le procedure in questa sezione mostrano come configurare una configurazione CloudFront di base che esegua le seguenti operazioni:

- Crea un bucket da utilizzare come origine di distribuzione.
- Memorizza le versioni originali dei tuoi oggetti in un bucket Amazon Simple Storage Service (Amazon S3).
- Utilizza il controllo dell'accesso all'origine (OAC) per inviare richieste autenticate alla tua origine Amazon S3. OAC invia richieste CloudFront per impedire agli utenti di accedere direttamente al tuo bucket S3. Per ulteriori informazioni su OAC, consulta. Limita l'accesso a un'origine Amazon Simple Storage Service
- Utilizza il nome di CloudFront dominio negli URL per gli 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 delle opzioni è personalizzabile. Per informazioni su come personalizzare le opzioni di CloudFront distribuzione, consultaCreazione di una distribuzione.

Argomenti

- Fase 4: Accedi ai tuoi contenuti tramite CloudFront
- Fase 5: rimozione
- Migliora la tua distribuzione di base CloudFront

Prerequisiti

Prima di iniziare, assicurati di aver completato le fasi in Configurazione.

Fase 1: creazione di 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, crei un bucket S3 con i `hello world` file di esempio forniti che utilizzerai per creare una pagina web di base.

Per creare un bucket

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

Fase 2: Caricamento dei contenuti in un bucket

Dopo aver creato il bucket Amazon S3, carica il contenuto del file decompresso su di esso`hello world`. (Hai scaricato e decompresso questo file). Fase 1: creazione di un bucket Amazon S3

Per caricare i contenuti su Amazon S3

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

Fase 3: creare 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 ti aiuta a inviare in modo sicuro richieste autenticate alla tua origine Amazon S3. Per ulteriori informazioni su OAC, consulta. Limita l'accesso a un'origine Amazon Simple Storage Service

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. Per Origin, dominio Origin, scegli il bucket S3 che hai creato per questo tutorial.
4. Per Origin, Origin access, seleziona le impostazioni del controllo di accesso di Origin (consigliato).
5. Per il controllo degli accessi di Origin, scegli Crea nuovo OAC.
6. Nel riquadro Crea nuovo OAC, mantieni le impostazioni predefinite e scegli Crea.
7. Per Web Application Firewall (WAF), seleziona una delle opzioni.
8. Per tutte le altre sezioni e impostazioni, accettate i valori predefiniti. Per ulteriori informazioni su queste opzioni, consulta Distribution Settings (Impostazioni distribuzione).
9. Scegli Create Distribution (Crea distribuzione).
10. Nel banner The S3 bucket policy deve essere aggiornato, leggi il messaggio e scegli Copia policy.

11. Nello stesso banner, scegli il link Vai alle autorizzazioni del bucket S3 per aggiornare la politica. (Questo ti porta alla pagina dei dettagli del bucket nella console Amazon S3.)
12. Per Policy del bucket scegli Modifica.
13. Nel campo Modifica dichiarazione, incolla la politica che hai copiato nel passaggio 10.
14. Seleziona Salvataggio delle modifiche.
15. Torna alla CloudFront console e consulta la sezione Dettagli relativa alla nuova distribuzione. Al termine della distribuzione, il campo Ultima modifica cambia da Distribuzione a data e ora.
16. 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 tue esigenze specifiche. Per informazioni sulla configurazione dell'accesso in un ambiente di produzione, consulta. Configura l'accesso sicuro e limita l'accesso ai contenuti

Fase 4: Accedi ai tuoi contenuti tramite CloudFront

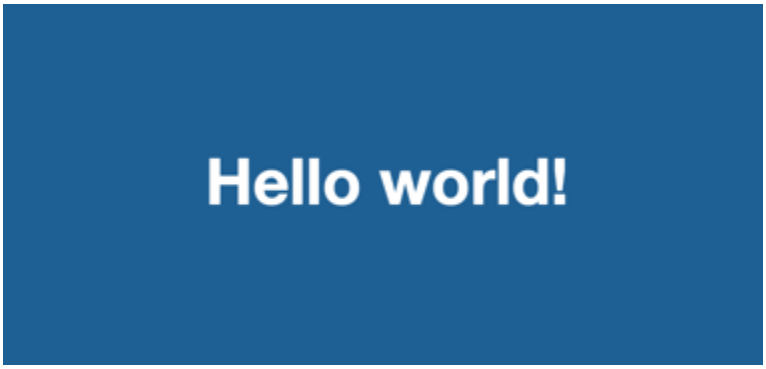
Per accedere ai tuoi contenuti CloudFront, combina il nome di dominio utilizzato per la CloudFront distribuzione con la pagina principale dei tuoi contenuti. (Hai registrato il nome di dominio di distribuzione inFase 3: creare una CloudFront distribuzione che utilizzi un'origine Amazon S3 con OAC.)

- 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 il seguente contenuto:



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`.

Fase 5: rimozione

Se hai creato la distribuzione e il bucket S3 solo come esercizio di apprendimento, eliminali in modo da non addebitare più addebiti. Elimina prima la distribuzione. Per ulteriori informazioni, consulta i collegamenti seguenti:

- Eliminazione di una distribuzione
- Eliminazione di un bucket

Migliora la tua distribuzione di base CloudFront

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

- Per impostazione predefinita, i file (oggetti) nel bucket Amazon S3 sono impostati come privati. Solo chi Account AWS ha creato il bucket ha il permesso di leggere o scrivere i file. Se desideri consentire a chiunque di accedere ai file nel tuo bucket Amazon S3 utilizzando gli CloudFront URL, devi concedere autorizzazioni di lettura pubbliche agli oggetti.
- 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 URL firmati e cookie 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 URL personalizzati.
- Questo tutorial utilizza un'origine Amazon S3 con controllo dell'accesso all'origine (OAC). Tuttavia, non puoi usare OAC se la tua origine è un bucket S3 configurato come endpoint di un sito web. In tal caso, devi configurare il bucket come origine personalizzata. CloudFront Per ulteriori informazioni, consulta Usa un bucket Amazon S3 configurato come endpoint del sito Web. Per ulteriori informazioni su OAC, consulta. Limita l'accesso a un'origine Amazon Simple Storage Service

Inizia con un sito Web statico sicuro

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

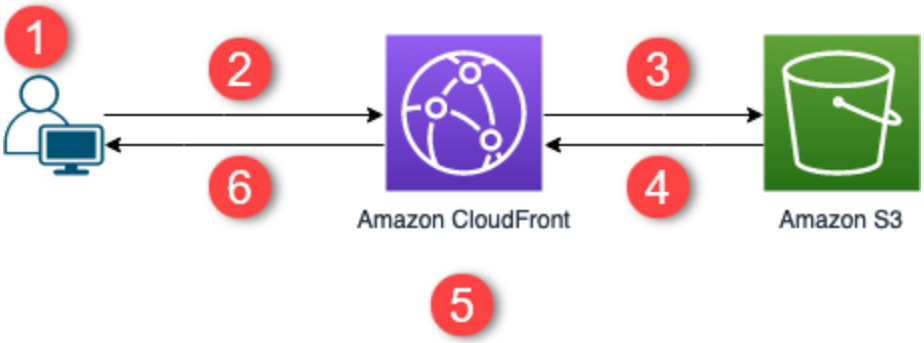
- Utilizza lo storage durevole di Amazon Simple Storage Service (Amazon S3): questa soluzione crea un bucket Amazon S3 per ospitare i contenuti del tuo sito Web statico. Per aggiornare il tuo sito web, basta caricare i nuovi file nel bucket S3.
- È velocizzato dalla rete di distribuzione CloudFront dei contenuti di Amazon: questa soluzione crea una CloudFront distribuzione per servire il tuo sito Web agli spettatori con bassa latenza. La distribuzione è configurata con Origin Access Control (OAC) per garantire 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 SSL/TLS 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 configurata e implementata con AWS CloudFormation: Questa soluzione utilizza un AWS CloudFormation modello per configurare tutti i componenti, in modo da poterti concentrare maggiormente sui contenuti del tuo 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 è memorizzato nella cache, CloudFront restituisce l'oggetto dalla sua cache al visualizzatore.
3. Se l'oggetto non è nella CloudFront cache, lo CloudFront richiede 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 CloudFront edge location vengono servite dalla CloudFront cache.

Implementa la soluzione

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

- Utilizza la AWS CloudFormation console per distribuire la soluzione con contenuti predefiniti, quindi carica i contenuti del tuo sito Web su 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 distribuire 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 nella stessa zona in Account AWS cui viene distribuita 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) autorizzazioni per avviare CloudFormation modelli che creano ruoli IAM e autorizzazioni per creare tutte le AWS risorse della soluzione.

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

Utilizzo della console AWS CloudFormation

Per eseguire la distribuzione utilizzando la console CloudFormation

1. Scegli Avvia su AWS per aprire questa soluzione nella console AWS CloudFormation . Se necessario, accedi al tuo Account AWS.

2. La procedura guidata Create stack si apre nella CloudFormation console, con campi precompilati che specificano il modello di questa soluzione. CloudFormation

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.

   - SubDomain— Inserisci 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.
   - DomainName— Inserisci il tuo nome di dominio, ad esempio *example.com*. Questo dominio deve essere puntato a una zona Route 53 ospitata.
   - HostedZoneId— L'ID della zona ospitata sulla Route 53 del tuo nome di dominio.
   - CreateApex— (Facoltativo) Crea un alias per l'apex del dominio (example.com) nella tua 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 di CloudFormation creare un ruolo IAM che consente l'accesso alle risorse dello stack e di denominare le risorse in modo dinamico.
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 sia memorizzato nella cache in una posizione periferica. CloudFront Per assicurarti che gli spettatori vedano i contenuti aggiornati del tuo sito web, invalida i file per rimuovere le copie memorizzate nella cache dalle edge location. CloudFront Per ulteriori informazioni, consulta Invalida i file per rimuovere il contenuto.

Clonare la soluzione localmente

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. Esegui il AWS CLI comando seguente per creare un bucket Amazon S3 per archiviare gli artefatti della soluzione. Sostituiscilo *example-bucket-for-artifacts*con il tuo nome di bucket.

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

5. Esegui il AWS CLI comando seguente per impacchettare gli artefatti della soluzione come modello. CloudFormation Sostituiscilo *example-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 example-bucket-for-artifacts \
    --output-template-file packaged.template
```

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

   - *your- CloudFormation -stack-name — Sostituisci con un nome* per lo stack. CloudFormation
   - *example.com*: sostituisci con il nome di dominio. Questo dominio deve essere indirizzato a una zona ospitata sulla Route 53 all'interno della stessa. 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*: sostituiscilo con l'ID della zona ospitata Route 53 del tuo 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 distribuire lo stack con un apex di dominio, esegui 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. Attendi che lo CloudFormation stack finisca di creare. 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 log di accesso per la CloudFront distribuzione. 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. Scegli 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 log di accesso. CloudFront

Configurare le 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.

Scegli tra le seguenti impostazioni di configurazione:

- 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.
- 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 di origine: 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 in tempo reale che mostrino l'attività degli spettatori.

Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.

Per il numero massimo attuale di distribuzioni che puoi creare per ogni account, consulta. AWS Quote 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 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 AWS CloudFormation stack. Per ulteriori informazioni, consulta Offri video in streaming live 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

Creazione di una distribuzione

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

Panoramica sulla creazione di una distribuzione

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 server Amazon EC2 o un'altra origine personalizzata, consulta Usa 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. Puoi rendere i tuoi oggetti leggibili pubblicamente oppure puoi utilizzare URL CloudFront firmati per limitare l'accesso ai tuoi contenuti.

   > **Important**
   >
   > È tua responsabilità garantire la protezione del tuo server di origine. Devi assicurarti che CloudFront disponga dell'autorizzazione per 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, consultaCreazione di una distribuzione.
   - Per informazioni sulla creazione di una distribuzione utilizzando l' CloudFront API, CreateDistributionconsulta Amazon CloudFront API Reference.

4. (Facoltativo) Se usi 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 Per aggiornare una distribuzione CloudFront .

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

6. Sviluppa il tuo sito Web o l'applicazione per accedere ai tuoi contenuti utilizzando il nome di dominio CloudFront restituito dopo aver creato la 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 (CNAME) alla creazione della distribuzione, puoi utilizzare il tuo nome di dominio. In tal caso, l'URL per `image.jpg` potrebbe essere `https://www.example.com/image.jpg`.

Tieni presente quanto segue:

- Se desideri utilizzare URL firmati per limitare l'accesso al tuo contenuto, consulta Offri contenuti privati con URL firmati e cookie firmati.
- Se desideri servire contenuto compresso, consulta Servire 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

Per creare una distribuzione (console)

1. Accedi a AWS Management Console 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. Specifica le impostazioni per la distribuzione. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.
4. Salvare le modifiche.
5. Dopo aver CloudFront creato la distribuzione, il valore della colonna Stato relativa alla distribuzione cambierà da Deploying alla data e all'ora di distribuzione della distribuzione. Se hai scelto di abilitare la distribuzione, questa sarà pronta per l'elaborazione delle richieste in questo momento.

   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 URL personalizzati aggiungendo nomi di dominio alternativi (CName)

6. Una volta implementata la distribuzione, conferma di poter accedere ai contenuti utilizzando il nuovo CloudFront URL o CNAME. Per ulteriori informazioni, consulta Prova una distribuzione.

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, gli AWS account con una coppia di CloudFront key pair attiva e che possono essere utilizzati per creare URL firmati validi, non sono attualmente 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, ad esempio. `EDFDVBD6EXAMPLE` Non puoi modificare l'ID distribuzione di una distribuzione.

Distribuzione e stato

Quando si distribuisce una distribuzione, viene visualizzato lo stato di distribuzione nella colonna Ultima modifica. Attendi che la distribuzione finisca la distribuzione e assicurati che la colonna Stato indichi Enabled. 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.

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 CloudFront dominio per la tua distribuzione. Per ulteriori informazioni sugli CloudFront URL per i collegamenti ai tuoi oggetti, consultaPersonalizza il formato URL per i file in CloudFront.

Se hai specificato uno o più nomi di dominio alternativi (CName), puoi utilizzare i tuoi nomi di dominio per i collegamenti ai tuoi oggetti anziché utilizzare il CloudFront nome di dominio. Per ulteriori informazioni sui CNAME, consulta Nomi di dominio alternativi (CNAME).

> **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.

Collegamenti aggiuntivi

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

- Per informazioni su come creare una distribuzione che utilizzi un'origine bucket Amazon Simple Storage Service (Amazon S3) con controllo dell'accesso all'origine (OAC), consulta. Inizia con una CloudFront distribuzione di base
- Per informazioni sull'utilizzo delle CloudFront API per creare una distribuzione, consulta CreateDistributionAmazon CloudFront API Reference.
- Per informazioni sull'aggiornamento di una distribuzione (ad esempio, per aggiungere o modificare i comportamenti della cache), 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.

Riferimento alle impostazioni di distribuzione

Quando si utilizza la CloudFrontconsole per creare una nuova distribuzione o aggiornare una distribuzione esistente, si specificano i seguenti valori.

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

Argomenti

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

Il dominio di origine è il nome di dominio DNS del bucket Amazon S3 o del server HTTP da cui CloudFront desideri ottenere oggetti per questa origine, ad esempio:

- Bucket Amazon S3 – `DOC-EXAMPLE-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. La propagazione del nome del bucket S3 in tutte le regioni può richiedere fino a 24 ore. 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 – `DOC-EXAMPLE-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
- Istanza Amazon EC2 – *ec2-203-0-113-25*.compute-1.amazonaws.com
- Sistema di bilanciamento del carico Elastic Load Balancing – *example-load-balancer-1234567890*.*us-west-2*.elb.amazonaws.com
- Il tuo server web – https://www.example.com

Scegli il nome di dominio nel campo Origin Domain Name (Nome dominio origine) o digita il nome. Il nome di dominio non fa distinzione tra maiuscole e minuscole.

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 “Usa un bucket Amazon S3 configurato come 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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.

> **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. Finché le richieste dei visualizzatori nell'applicazione non sono state modificate, CloudFront continua a servire gli oggetti che si trovano già in una cache edge fino alla scadenza del TTL su ciascun oggetto o fino alla rimozione degli oggetti richiesti raramente.

Protocollo (solo origini personalizzate)

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

La politica del protocollo che desideri utilizzare CloudFront per recuperare oggetti dall'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 certificato SSL/TLS sul server di origine deve corrispondere al nome di dominio specificato per Origin domain. 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 dei certificati SSL/TLS con 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 protocollo TLS/SSL 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 protocollo TLS/SSL da utilizzare, non puoi impostare CloudFront un protocollo minimo. Devi invece specificare tutti i protocolli TLS/SSL che CloudFront puoi utilizzare con la tua origine. Per ulteriori informazioni, OriginSslProtocolsconsulta Amazon CloudFront API Reference.

Origin Path (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 **`DOC-EXAMPLE-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. `DOC-EXAMPLE-BUCKET/production/index.html`

Quando un utente entra `example.com/acme/index.html` in un browser, CloudFront invia una richiesta ad Amazon S3 per. `DOC-EXAMPLE-BUCKET/production/acme/index.html`

Nome

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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.

Per informazioni su come richiedere agli utenti di accedere agli oggetti su un'origine personalizzata utilizzando solo CloudFront URL, consulta. the section called “Limita l'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 “Aggiungi 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 dello scudo di origine”.

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 (solo origini personalizzate)”.

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 falliscono 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 (solo origini personalizzate)

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 keep-alive origine (solo origini personalizzate)

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 di timeout di risposta e keep-alive

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

- Per il timeout di risposta, l'impostazione predefinita è 30 secondi.
- Per il timeout keep-alive, l'impostazione predefinita è 5 secondi.
- Per entrambe le quote, è possibile specificare un valore compreso tra 1 e 60 secondi. Per richiedere un aumento, crea un caso nel campo AWS Support Center Console/.

Dopo aver richiesto 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 di timeout keep-alive che desideri. Un aumento della quota per il tuo account non aggiorna automaticamente le tue origini. Ad esempio, se utilizzi una funzione Lambda @Edge per impostare un timeout keep-alive di 90 secondi, la tua origine deve già avere un timeout keep-alive di 90 secondi o più. In caso contrario, l'esecuzione della funzione Lambda @Edge potrebbe non riuscire.

Per ulteriori informazioni sulle quote di distribuzione, 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 relativo alla cache potrebbe applicarsi a tutti `.jpg` i file nella `images` directory su un server Web per il quale state utilizzando come server di origine 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 gli utenti devono utilizzare URL firmati per accedere ai file specificati
- 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 che l'origine aggiunge 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 si crea un comportamento di cache, si specifica l'unica origine da cui si desidera 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)
- 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

- Restrict Viewer Access (Use Signed URLs or Signed Cookies) (Limita accesso visualizzatore (usa URL o cookie firmati))
- Firmatari fidati
- Account AWS numeri
- Compress Objects Automatically (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 cache non richiede URL firmati, contrariamente al secondo. 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 Pubblica 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 predefinito della cache.

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

Example Esempio

Specificate i `/a*` percorsi `/a/b*` e per il comportamento della cache.

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

Per aggirare la normalizzazione dei percorsi, puoi aggiornare i percorsi delle richieste o il modello di percorso per il comportamento della cache.

Origine o gruppo di origini

Questa impostazione si applica solo quando si crea o si aggiorna un comportamento della 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: È possibile utilizzarli CloudFront solo per recuperare oggetti dall'origine, ottenere le intestazioni degli oggetti o recuperare un elenco delle opzioni supportate dal server di origine.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE: è possibile utilizzarli 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**
>
> 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 Limita l'accesso a un'origine Amazon Simple Storage Service.
- 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.

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. Contenuto della cache in base alle intestazioni delle richieste

Intestazioni elenco consentiti

Queste impostazioni si applicano solo quando si sceglie Allowlist for Cache Based on Selected Request Headers.

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 Gestisci la durata della 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.

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

Maximum TTL (TTL massimo)

Specificate il tempo massimo, in secondi, durante il quale 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 Gestisci la durata della 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 che specifichi per Default TTL (TTL di default) 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 Gestisci la durata della 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 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 Contenuto della cache basato sui 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`*

Dove ognuno dei tuoi utenti ha un valore univoco per *`member-number`*. Desiderate CloudFront memorizzare nella cache una versione separata dell'oggetto per ogni membro. Puoi farlo inoltrando tutti i cookie all'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 Contenuto della cache in base ai parametri della stringa di query.

Elenco consentiti stringhe di query

Questa impostazione si applica solo quando si sceglie Forward all, cache basata su allowlist for. 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 Configurare video on demand per Microsoft Smooth Streaming.

Restrict Viewer Access (Use Signed URLs or Signed Cookies) (Limita accesso visualizzatore (usa URL o cookie firmati))

Se desideri che le richieste per oggetti corrispondenti a `PathPattern` per questo comportamento cache utilizzino URL pubblici, scegli No.

Se desideri che le richieste per oggetti corrispondenti a `PathPattern` per questo comportamento cache utilizzino URL firmati, scegli Yes (Sì). Specificate quindi gli AWS account che desiderate utilizzare per creare URL firmati; questi account sono noti come firmatari attendibili.

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

Firmatari fidati

Questa impostazione si applica solo quando scegli Sì per Limita l'accesso degli spettatori (Usa URL firmati o cookie 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 AWS Management Console 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 URL firmati, un AWS account deve avere almeno una coppia di CloudFront key pair attiva.

> **Important**
>
> Se aggiorni una distribuzione che stai già utilizzando per distribuire contenuto, aggiungi firmatari fidati solo quando sei pronto per iniziare la generazione di URL firmati per i tuoi oggetti. Dopo aver aggiunto firmatari fidati a una distribuzione, gli utenti devono utilizzare URL firmati per accedere agli oggetti che corrispondono a `PathPattern` per questo comportamento cache.

Account AWS numeri

Questa impostazione si applica solo quando scegli Specificare gli account per i firmatari attendibili.

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

- Gli account specificati devono avere almeno una coppia di CloudFront key pair attiva. Per ulteriori informazioni, consulta Crea coppie di chiavi per i tuoi 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 I tuoi Account AWS identificatori in. Riferimenti generali di Amazon Web Services

- 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.

Compress Objects Automatically (Comprimi oggetti automaticamente)

Se desideri CloudFront comprimere automaticamente determinati tipi di file quando gli utenti supportano i contenuti compressi, scegli Sì. Quando CloudFront comprime i contenuti, i download sono più veloci perché i file sono più piccoli e le pagine web vengono visualizzate più velocemente per gli utenti. Per ulteriori informazioni, consulta Servire 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 Decidi quale CloudFront evento usare per attivare una funzione Lambda @Edge.

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 Include body.

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 CloudFront servizio. 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 le API per bloccare le richieste prima che

raggiungano i tuoi server. Puoi farlo Abilita 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 (CNAME)

Facoltativo. Specificate uno o più nomi di dominio che desiderate utilizzare per gli URL degli oggetti anziché il nome di dominio assegnato al momento della creazione della distribuzione. CloudFront Il nome di dominio deve essere di tua proprietà o devi disporre dell'autorizzazione per utilizzarlo. Per verificarlo, aggiungi un certificato SSL/TLS.

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 URL personalizzati aggiungendo nomi di dominio alternativi (CName). Per ulteriori informazioni sugli CloudFront URL, consulta. Personalizza il 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.

Note

Prima di specificare un certificato SSL personalizzato, è necessario specificare un nome di dominio alternativo valido. Per ulteriori informazioni, consulta Requisiti per l'utilizzo di nomi di dominio alternativi e Usa nomi di dominio alternativi e HTTPS.

- CloudFront Certificato predefinito (*.cloudfront.net): scegli questa opzione se desideri utilizzare il nome di CloudFront dominio negli URL dei tuoi oggetti, ad esempio. `https://d111111abcdef8.cloudfront.net/image1.jpg`
- Custom SSL Certificate (Certificato SSL personalizzato) - Scegli questa opzione se desideri utilizzare il tuo nome di dominio negli URL per gli oggetti come un 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 negli URL di oggetti (https://example.com/logo.jpg). Se utilizzi il tuo nome di dominio di CloudFront distribuzione (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 CloudFront dominio non corrisponde al nome di dominio nel certificato 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 HTTPS: CloudFront

- 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 AWS CloudFormation, il campo è denominato `SslSupportMethod` (notate le diverse lettere maiuscole).
- 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 CloudFrontdei prezzi di Amazon e cerca SSL personalizzato con IP dedicato.

  Per applicare questa impostazione utilizzando l' CloudFront API, specifica `vip` nel `SSLSupportMethod` campo. In AWS 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.

Politica 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 protocollo SSL/TLS 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 **`true`** nell'API), imposta automaticamente la politica di sicurezza su TLSv1. CloudFront
- Quando SSL Certificate (Certificato SSL) è Custom SSL Certificate (example.com) (Certificato SSL personalizzato (example.com)) e Custom SSL Client Support (Supporto client SSL personalizzato) è Clients that Support Server Name Indication (SNI) - (Recommended) (Client che supportano l'indicazione del nome del server (SNI) - (scelta suggerita) (quando nell'API `CloudFrontDefaultCertificate` è `false` e `SSLSupportMethod` è `sni-only`), è possibile scegliere tra le seguenti policy di sicurezza:
  - TLSv1.2_2021
  - TLSv1.2_2019
  - TLSv1.2_2018
  - TLSv1.1_2016
  - TLSv1_2016
  - TLSv1
- Quando SSL Certificate (Certificato SSL) è Custom SSL Certificate (example.com) (Certificato SSL personalizzato (example.com) e Custom SSL Client Support (Supporto client SSL personalizzato) è Legacy Clients Support (Supporto client legacy) (quando nell'API

`CloudFrontDefaultCertificate` è `false` e `SSLSupportMethod` è `vip`), è possibile scegliere tra le seguenti policy di sicurezza:

- TLSv1
- SSLv3

In questa configurazione, le politiche di sicurezza TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 e TLSv1_2016 non sono disponibili nella console o nell'API. 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 di Custom SSL Client Support (Supporto client SSL personalizzato) della distribuzione in Clients that Support Server Name Indication (SNI) (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 CloudFront disponibile e può anche ridurre i costi.
- Se è necessario mantenere il supporto client legacy con indirizzi IP dedicati, è possibile richiedere uno degli altri criteri di protezione TLS (TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 o TLSv1_2016) creando un caso nel Centro assistenza AWS.

> **Note**
>
> Prima di contattare AWS Support per richiedere questa modifica, considera quanto segue:
>
> - Quando aggiungi una di queste politiche di sicurezza (TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 o TLSv1_2016) a una distribuzione Legacy Clients Support, la politica di sicurezza viene applicata a tutte le richieste di visualizzatori non SNI per tutte le distribuzioni Legacy Clients Support nel 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 si sceglie di aggiornare le policy di protezione di una distribuzione da TLSv1 a TLSv1.1_2016, tale distribuzione

non supporterà più la crittografia DES-CBC3-SHA. 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 versione successiva e Server Name Indication (SNI). CloudFront non offre supporto nativo per gRPC su HTTP/2.

Per i visualizzatori e CloudFront per utilizzare HTTP/3, i visualizzatori devono supportare TLSv1.3 e Server Name Indication (SNI). CloudFront supporta la migrazione della connessione HTTP/3 per consentire al visualizzatore 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 sulla crittografia TLS1.3 supportata, consulta Protocolli e cifrari supportati tra visualizzatori e CloudFront.

Default Root Object (Oggetto root di default)

Facoltativo. L'oggetto che desideri richiedere CloudFront alla tua origine (ad esempio,`index.html`) quando un visualizzatore richiede l'URL principale della tua distribuzione (`https://www.example.com/`) anziché un oggetto nella tua 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 Specificate un oggetto radice predefinito.

Registrazione

Se desideri CloudFront registrare le informazioni su ogni richiesta di un oggetto e archiviare i file di registro in un bucket Amazon S3. Puoi attivare o disattivare la registrazione in qualsiasi momento. L'attivazione della registrazione non comporta spese supplementari, ma vengono addebitati i costi abituali Amazon S3 relativi all'archiviazione e all'accesso ai file in un bucket Amazon S3. Puoi eliminare i log in qualsiasi momento. Per ulteriori informazioni sui log di CloudFront accesso, consulta. Configurazione e utilizzo di registri standard (registri di accesso)

Bucket for Logs (Bucket per log)

Se hai scelto On for Logging, il bucket Amazon S3 in cui CloudFront desideri archiviare i log di accesso, ad esempio,. *myLogs-*`DOC-EXAMPLE-BUCKET.s3.amazonaws.com`

Important

Non scegliere un bucket Amazon S3 in nessuna delle seguenti regioni, perché CloudFront non fornisce 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)

Se abiliti la registrazione, CloudFront registra le informazioni su ogni richiesta dell'utente finale per un oggetto e archivia i file nel bucket Amazon S3 specificato. Puoi attivare o disattivare la registrazione in qualsiasi momento. Per ulteriori informazioni sui CloudFront log di accesso, consulta. Configurazione e utilizzo di registri standard (registri di accesso)

> **Note**
>
> Devi disporre delle autorizzazioni necessarie per ottenere e aggiornare le liste ACL di bucket Amazon S3 e la lista ACL S3 per il bucket deve concederti l'autorizzazione `FULL_CONTROL`. Ciò consente di CloudFront autorizzare l'`awslogsdelivery`account a salvare i file di registro nel bucket. Per ulteriori informazioni, consulta Autorizzazioni richieste per configurare la registrazione standard e per accedere ai file di log.

Log Prefix (Prefisso log)

Facoltativo. Se avete scelto Attivato per la registrazione, specificate l'eventuale stringa da aggiungere come prefisso CloudFront ai 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 sui log di CloudFront accesso, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 cookie, di conseguenza, a meno che la tua distribuzione non includa anche un origine Amazon EC2 o un'altra origine personalizzata, ti consigliamo di scegliere Off per il valore di Cookie Logging (Registrazione cookie).

Per ulteriori informazioni sui cookie, consulta Contenuto della cache basato sui cookie.

Enable IPv6 (Abilita IPv6)

IPv6 è una nuova versione del protocollo IP. È l'eventuale sostituto di IPv4 e utilizza uno spazio di indirizzi più ampio. CloudFront risponde sempre alle richieste IPv4. Se desideri rispondere CloudFront alle richieste provenienti da indirizzi IP IPv4 (come 192.0.2.44) e alle richieste da indirizzi IPv6 (come 2001:0 db 8:85 a3: :8a2e: 0370:7334), seleziona Abilita IPv6.

In generale, devi abilitare IPv6 se hai utenti su reti IPv6 che desiderano accedere al tuo contenuto. Tuttavia, se utilizzi URL o cookie firmati per limitare l'accesso al tuo contenuto e una policy personalizzata che include il parametro `IpAddress` per limitare gli indirizzi IP che possono accedere al tuo contenuto, non abilitare 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 URL firmati utilizzando una policy personalizzata, consulta Crea un URL firmato utilizzando una politica personalizzata. Per informazioni sulla creazione di cookie firmati utilizzando una policy personalizzata, consulta Imposta i cookie firmati utilizzando una politica 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:

- Abiliti IPv6 per la distribuzione
- Stai utilizzando nomi di dominio alternativi negli URL 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 i log di CloudFront accesso, la `c-ip` colonna include valori in formato IPv4 e IPv6. Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso).

> **Note**
>
> Per mantenere un'elevata disponibilità dei clienti, CloudFront risponde alle richieste degli utenti utilizzando IPv4 se i nostri dati suggeriscono che IPv4 offrirà un'esperienza utente

migliore. Per scoprire quale percentuale di richieste CloudFront viene gestita tramite 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 crescere nel corso del tempo, ma rimarrà una parte minima del traffico in quanto IPv6 non è ancora supportato da tutte le reti mondiali di visualizzatori. Alcune reti di visualizzatori offrono un eccellente supporto di IPv6, mentre altre non offrono alcun supporto (una rete di visualizzatori è analoga all'operatore Internet o wireless).
Per ulteriori informazioni sul nostro supporto per IPv6, consulta le domande frequenti. CloudFront Per informazioni sull'attivazione di log di accesso, vedi i campi Registrazione, Bucket for Logs (Bucket per log) e Log Prefix (Prefisso log).

Commento

Facoltativo. 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 abilitata, CloudFront accetta e gestisce tutte le richieste degli utenti finali relative ai contenuti che utilizzano il nome di dominio associato a tale distribuzione.

  Quando si crea, si modifica o si elimina una CloudFront distribuzione, è necessario 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 richieste dell'utente finale che utilizzano 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 Crea 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 desideri restituire CloudFront a un visualizzatore quando l'origine restituisce

il codice di stato HTTP specificato per il codice di 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 Limita la distribuzione geografica dei tuoi contenuti.

Prova 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 testare la tua distribuzione, procedi come segue:

1. Attendi che la distribuzione venga distribuita.
   - Visualizza i dettagli della distribuzione nella console. Al termine della distribuzione, il campo Ultima modifica cambia da Distribuzione a data e ora.

2. Crea collegamenti ai tuoi oggetti con il nome di CloudFront dominio utilizzando la procedura seguente.
3. Prova i link. CloudFront fornisce gli oggetti alla pagina Web o all'applicazione.

Crea collegamenti ai tuoi oggetti

Utilizzate la seguente procedura per creare collegamenti di prova per gli oggetti nella vostra distribuzione CloudFront web.

Creazione di collegamenti a oggetti in una distribuzione Web

1. Copia il seguente codice HTML in un nuovo file, sostituisci *nome-dominio* con il nome di dominio della distribuzione e sostituisci *nome-oggetto* con il nome dell'oggetto.

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

   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, fornito dalla posizione periferica che ha CloudFront determinato essere appropriata per servire l'oggetto.

Aggiornamento di una distribuzione

Nella CloudFront console, puoi vedere le CloudFront distribuzioni associate al tuo AWS account, 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 .

Per aggiornare una distribuzione CloudFront

1. Accedi a AWS Management Console 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 modificare le impostazioni di una distribuzione, scegli la scheda Distribution Settings (Impostazioni distribuzione).
4. Per aggiornare le impostazioni generali, scegli Edit (Modifica). Altrimenti, scegli la scheda per le impostazioni che desideri aggiornare: Origins (Origini) o Behaviors (Comportamenti).
5. Effettua gli aggiornamenti, quindi, per salvare le modifiche scegli Yes, Edit (Sì, modifica). 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)
6. 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. Fino a quando la configurazione non viene aggiornata in una edge location, CloudFront continua a fornire i contenuti da quella posizione in base alla configurazione precedente. Dopo l'aggiornamento della configurazione in una edge location, inizia CloudFront immediatamente a distribuire i contenuti da quella posizione in base alla nuova configurazione.

Le modifiche non si propagano contemporaneamente a tutte le edge location. Durante CloudFront la propagazione delle modifiche, non siamo in grado di determinare se una determinata edge location stia servendo i tuoi contenuti sulla base della configurazione precedente o della nuova configurazione.

Per vedere quando le modifiche vengono propagate, visualizza i dettagli della distribuzione nella console. Il campo Ultima modifica cambia da Distribuzione a data e ora di completamento della distribuzione.

Etichettare una distribuzione

I tag sono parole o frasi che puoi usare per identificare e organizzare AWS le tue risorse. Puoi 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 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.
- Tieni traccia delle informazioni di fatturazione in diverse categorie. Quando applichi tag a CloudFront distribuzioni o altre AWS risorse (come istanze Amazon EC2 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

Si applicano le seguenti limitazioni di base ai tag:

- Per il numero massimo di tag per distribuzione, consultaQuote 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 .

Aggiungere, modificare ed eliminare i tag per le distribuzioni

Puoi usare la CloudFront console per gestire i tag per le tue distribuzioni.

Aggiunta, modifica o eliminazione di tag per una distribuzione

1. Accedi AWS Management Console 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. Scegli 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, scegliere Remove (Rimuovi).
6. Seleziona Salvataggio delle modifiche.

Etichettatura programmatica

Puoi anche utilizzare l' CloudFront API, AWS Command Line Interface (AWS CLI), AWS gli SDK e AWS Tools for Windows PowerShell applicare tag. Per ulteriori informazioni, consulta i seguenti argomenti:

- CloudFront Operazioni API:
  - ListTagsForResource
  - TagResource
  - UntagResource
- AWS CLI — Vedi cloudfront nel Command Reference AWS CLI
- AWS SDK: consulta la documentazione SDK applicabile nella pagina Documentazione AWS
- Strumenti per Windows PowerShell : consulta Amazon CloudFront nella guida di riferimento ai AWS Tools for 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 Elimina una distribuzione con un OAC collegato a un bucket S3 per dettagli importanti.

> **Note**
>
> Tieni presente che prima di eliminare una distribuzione dovrai disabilitarla e pertanto è necessaria l'autorizzazione per aggiornare la distribuzione.
> 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).

Per eliminare una distribuzione CloudFront

1. Accedi a AWS Management Console 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 Disabilitato, vai al passaggio 6.
   - Se lo stato mostra Abilitato ma la distribuzione mostra ancora Distribuzione nella colonna Ultima modifica, attendi che la distribuzione finisca prima di continuare con il passaggio 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 Disabilitato.
5. Attendi che il nuovo timestamp venga visualizzato nella colonna Ultima modifica.
   - Potrebbero essere necessari alcuni minuti prima che la modifica CloudFront venga propagata a tutte le posizioni periferiche.

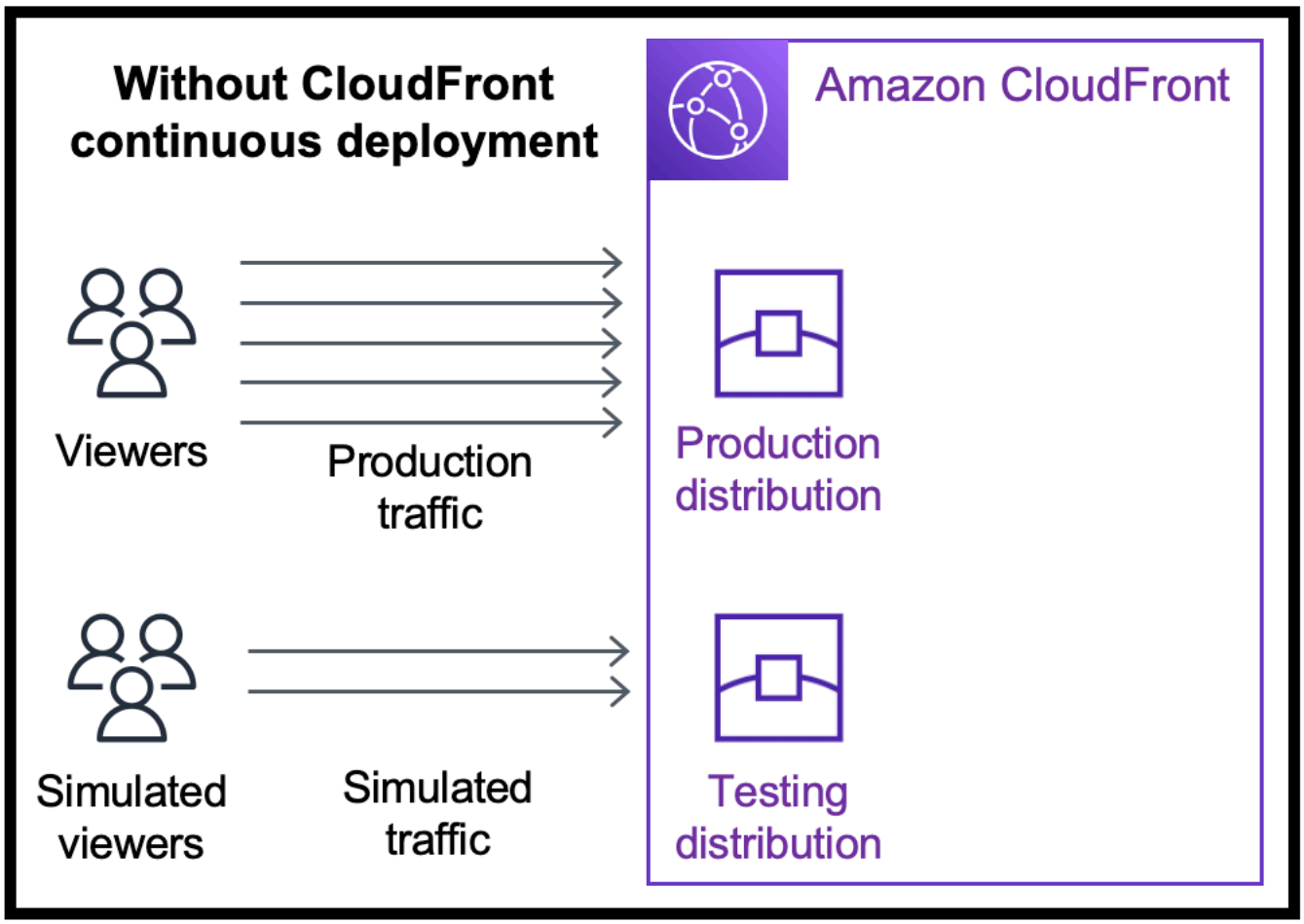
6. Selezionate la casella di controllo relativa alla distribuzione che desiderate eliminare.
7. Scegli Delete (Elimina), poi Delete (Elimina).

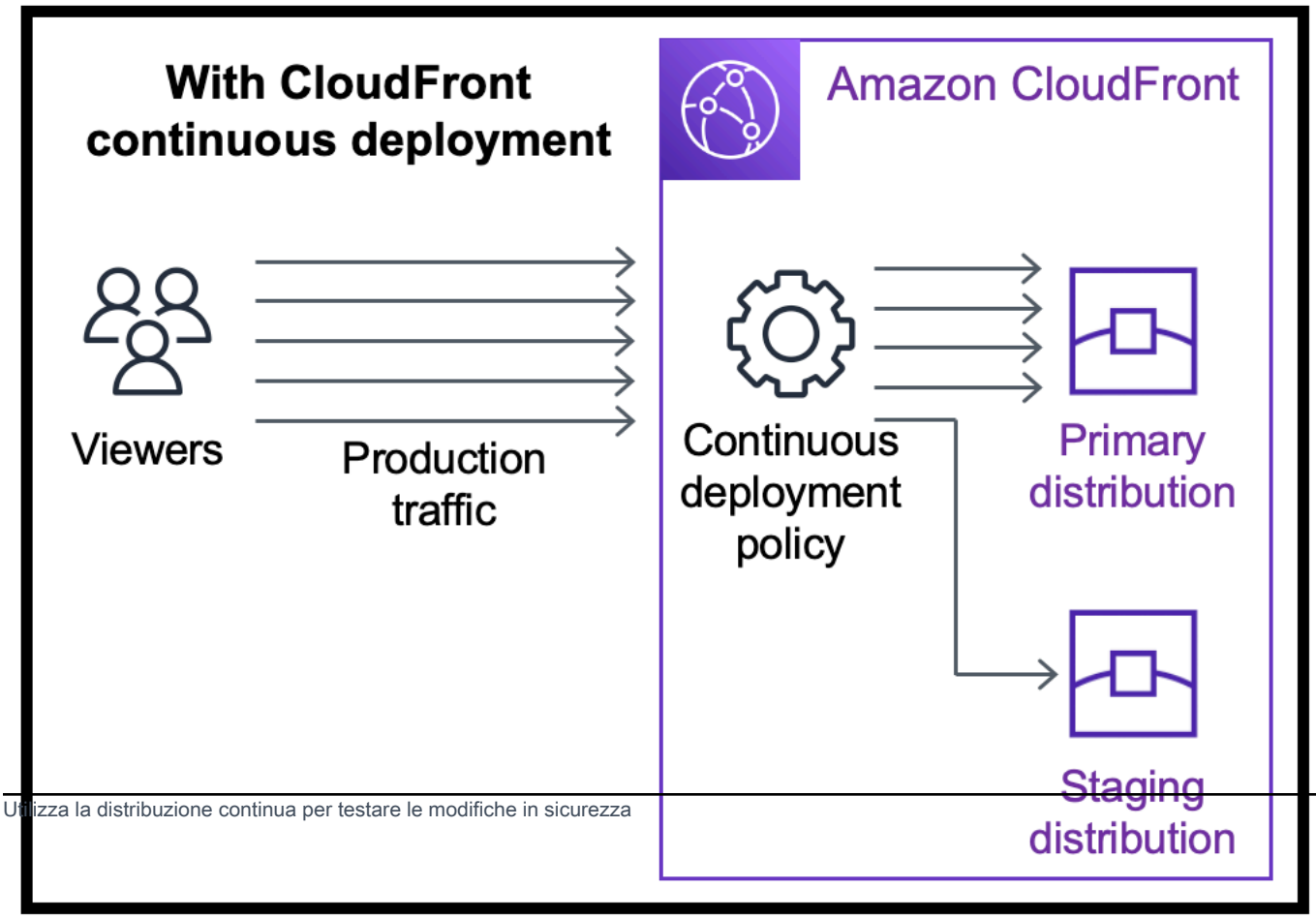
   - Se l'opzione Elimina non è disponibile, significa che la modifica CloudFront viene ancora propagata alle posizioni periferiche. Attendi che il nuovo timestamp venga visualizzato nella colonna Ultima modifica, quindi ripeti i passaggi 6-7.

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

Scopri di più sull'utilizzo della distribuzione continua nei seguenti argomenti.

Argomenti

CloudFront flusso di lavoro di distribuzione continua

Il seguente flusso di lavoro di alto livello spiega come testare e implementare in sicurezza le modifiche alla configurazione con la distribuzione CloudFront 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 “Indirizza le richieste alla distribuzione temporanea”.
4. Aggiornare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiorna le distribuzioni primarie e staging”.
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 “Monitora 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.

Utilizza una politica di distribuzione temporanea e di distribuzione 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.

Crea una distribuzione temporanea con una politica di distribuzione continua

Le seguenti procedure mostrano come creare una distribuzione temporanea con una politica di distribuzione continua.

Console

È possibile creare una distribuzione temporanea con una politica di distribuzione continua utilizzando. AWS Management Console

Creazione di una distribuzione temporanea e di una policy di implementazione continua (console)

1. Accedi a AWS Management Console e 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 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. Seleziona Successivo.

   c. Modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiorna le distribuzioni primarie e staging”.

      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 “Indirizza le 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, sostituire *`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:

   - Sostituire *`primary_distribution_ID`* con l'ID della distribuzione principale.
   - Sostituire *`primary_distribution_ETag`* con il valore `ETag` della distribuzione principale (che hai copiato nella fase precedente).
   - (Facoltativo) Sostituire *`CLI_example`* 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 “Indirizza le 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`. Sostituire *`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. Sostituire *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 distribuita 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 “Indirizza le 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.

Aggiornare una distribuzione temporanea

Le seguenti procedure mostrano come aggiornare una distribuzione temporanea con una politica di distribuzione continua.

Console

È possibile aggiornare determinate configurazioni sia per la distribuzione primaria che per quella temporanea. Per ulteriori informazioni, consulta Aggiorna le distribuzioni primarie e staging.

Aggiornamento di una distribuzione temporanea (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. 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 “Aggiorna le distribuzioni primarie e staging”.

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`. Sostituire *`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 “Aggiorna le distribuzioni primarie e staging”.
   - 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. Sostituire *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 per il traffico in entrata instradato alla distribuzione temporanea.

API

Per aggiornare la configurazione di una distribuzione temporanea, usa UpdateDistribution(sulla distribuzione temporanea) per modificare la configurazione della distribuzione temporanea. Per ulteriori informazioni sulle impostazioni che è possibile aggiornare, consulta the section called “Aggiorna le distribuzioni primarie e staging”.

Aggiorna una politica di distribuzione continua

Le seguenti procedure mostrano come aggiornare una politica di distribuzione continua.

Console

È possibile aggiornare la configurazione del traffico della distribuzione aggiornando la politica di distribuzione continua.

Aggiornamento di una policy di implementazione continua (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 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`. Sostituire *`continuous_deployment_policy_ID`* con l'ID della policy di implementazione 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, consulta the section called “Indirizza le 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. Sostituire *`continuous_deployment_policy_ID`* con l'ID della policy di implementazione 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 sulle edge location, 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

Promuovi una configurazione di distribuzione temporanea

Le seguenti procedure mostrano 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:
  - Sostituire *`primary_distribution_ID`* con l'ID della distribuzione principale.
  - Sostituire *`staging_distribution_ID`* con l'ID della distribuzione temporanea.
  - Sostituire *`primary_distribution_ETag`* e *`staging_distribution_ETag`* con i valori `ETag` delle distribuzioni principali e temporanee. 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

Monitora 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. Per 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 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 primaria 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.

Scopri come funziona la distribuzione continua

I seguenti argomenti spiegano come funziona la distribuzione CloudFront continua.

Argomenti

- Indirizza le richieste alla distribuzione temporanea
- Persistenza della sessione per configurazioni basate sul peso
- Aggiorna le distribuzioni primarie e staging
- Le distribuzioni principali e temporanee non condividono una cache

Indirizza le richieste alla distribuzione temporanea

Quando si utilizza la distribuzione CloudFront continua, non è necessario modificare nulla delle richieste degli spettatori. 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 garantire 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

Aggiorna le distribuzioni primarie e staging

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**
>
> Se utilizzi la distribuzione continua e la distribuzione primaria è impostata con OAC per l'accesso ai bucket S3, aggiorna la policy del bucket S3 per consentire l'accesso alla distribuzione temporanea. Ad esempio, le politiche relative ai bucket S3, vedi. the section called “Concedi all'origine il permesso di controllo dell'accesso per accedere al bucket S3”

AWS WAF ACL web

Se abiliti la distribuzione continua per la tua distribuzione, valgono le seguenti considerazioni: AWS WAF

- Non è possibile associare una lista di controllo degli accessi AWS WAF Web (ACL) alla distribuzione per la prima volta.
- Non è possibile dissociare un ACL AWS WAF Web dalla distribuzione.

Prima di poter eseguire le attività precedenti, è necessario eliminare la politica di distribuzione continua per la distribuzione di produzione. Ciò elimina anche la distribuzione temporanea. Per ulteriori informazioni, consulta Usa AWS WAF protezioni.

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.

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

Argomenti

Usa un 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

Usa 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 del bucket in questo formato, puoi utilizzare le seguenti funzionalità: 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 di accesso all'origine per richiedere che gli spettatori accedano ai tuoi contenuti utilizzando gli CloudFront URL, non utilizzando gli URL di Amazon S3. Per ulteriori informazioni, consulta the section called “Limita l'accesso a un'origine Amazon Simple Storage Service”.
- Aggiorna il contenuto del tuo bucket inviando e richiedendo a. `POST` `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

Usa Amazon S3 Object Lambda

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 Amazon S3 Object Lambda come origine per la tua distribuzione, devi configurare le seguenti quattro autorizzazioni.

Object Lambda Access Point

Per aggiungere le autorizzazioni per l'access point Object Lambda

1. Accedi AWS Management Console 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3-object-lambda:Get*",
            "Resource": "arn:aws:s3-object-lambda:region:AWS-account-
ID:accesspoint/Object-Lambda-Access-Point-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudfront::AWS-account-
ID:distribution/CloudFront-distribution-ID"
                }
            }
        }
    ]
}
```

7. Seleziona Salvataggio delle modifiche.

Amazon S3 Access Point

Per aggiungere autorizzazioni per l'Amazon S3 Access Point

1. Accedi AWS Management Console 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.

```
{
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-
name",
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-name/
object/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "s3-object-lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

7. Selezionare Salva.

Amazon S3 bucket

Per aggiungere autorizzazioni al bucket Amazon S3

1. Accedi AWS Management Console 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.

```
{
    "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. Seleziona Salvataggio delle modifiche.

AWS Lambda function

Per aggiungere autorizzazioni alla funzione Lambda

1. Accedi AWS Management Console 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. Selezionare Salva.

Usa il punto di accesso Amazon S3

Quando utilizzi un Access Point S3, Amazon S3 genera automaticamente un alias univoco per te. Puoi usare questo alias al posto del nome di un bucket Amazon S3 come origine per la tua distribuzione. CloudFront

Quando utilizzi un alias Amazon S3 Access Point come origine per CloudFront, ti consigliamo di utilizzare il seguente formato:

alias`.s3.`*region*`.amazonaws.com`

Per ulteriori informazioni su come trovare il bucket*alias*, consulta Using a bucket alias for your S3 bucket access point nella Amazon S3 User Guide.

> **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 Amazon S3 Object Lambda come origine per la tua distribuzione, devi configurare le due autorizzazioni seguenti.

Amazon S3 Access Point

Per aggiungere autorizzazioni per l'Amazon S3 Access Point

1. Accedi AWS Management Console 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.

```
{
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-
name",
                "arn:aws:s3:region:AWS-account-ID:accesspoint/Access-Point-name/
object/*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceArn": "arn:aws:cloudfront::AWS-
account-ID:distribution/CloudFront-distribution-ID"}
            }
        }
    ]
}
```

7. Selezionare Salva.

Amazon S3 bucket

Per aggiungere autorizzazioni al bucket Amazon S3

1. Accedi AWS Management Console 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.

```
{
    "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. Seleziona Salvataggio delle modifiche.

Usa un bucket Amazon S3 configurato come 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 gli utenti di Amazon Simple Storage Service. (fornisce CloudFront anche pagine di errore personalizzate. Per ulteriori informazioni, vederethe section called “Crea 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 “Contenuto della cache in base alle intestazioni delle richieste”.

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 (come

DOC-EXAMPLE-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, usa il nome di CloudFront dominio della tua distribuzione negli URL degli oggetti, ad esempio. `https://d111111abcdef8.cloudfront.net/images/image.jpg`

   Per ulteriori informazioni sul formato degli CloudFront URL, consulta. the section called "Personalizza gli URL dei file"

3. Se utilizzi i CNAM Amazon S3, l'applicazione usa il tuo nome di dominio (ad esempio example.com) per fare riferimento agli oggetti nel tuo bucket Amazon S3 anziché utilizzare il nome del bucket (per esempio, DOC-EXAMPLE-BUCKET1.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.

   Per consentire ai CNAME S3 di funzionare, il tuo fornitore di servizi DNS deve avere un set di record di risorse CNAME per il tuo dominio che attualmente instrada 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://DOC-EXAMPLE-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 CNames con, consulta. CloudFront the section called “Usa URL personalizzati”

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 OAI, consulta the section called “Usa

un'identità di accesso all'origine (legacy, non consigliata)". Per un elenco di quelli Regioni AWS che supportano Signature Version 2, consulta il processo di firma di Signature Version 2 nel. 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 "Pubblica video live formattati con AWS Elemental MediaPackage"

Utilizzare un Application Load Balancer

Se la tua origine è uno o più server HTTP (S) (server Web) ospitati su una o più istanze Amazon EC2, puoi utilizzare un Application Load Balancer con accesso a Internet per distribuire il traffico alle istanze. Un sistema di bilanciamento del carico connesso a Internet ha un nome DNS risolvibile pubblicamente e indirizza le richieste dai client alle destinazioni tramite Internet.

Per ulteriori informazioni sull'utilizzo di un Application Load Balancer come origine per CloudFront, incluso come assicurarsi che gli utenti possano accedere ai server Web solo tramite CloudFront e non accedendo direttamente al load balancer, consulta. the section called "Limita l'accesso agli Application Load Balancer"

Usa l'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 gli URL delle funzioni, puoi CloudFront aggiungerla 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 attacchi DDoS

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 utilizzi l'URL di una funzione Lambda come origine per una CloudFront distribuzione, l'URL della funzione deve essere accessibile pubblicamente. A tale scopo, utilizzate 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` l'autorizzazione in una policy basata sulle risorse. Per ulteriori informazioni sull'utilizzo degli URL delle funzioni Lambda per OAC, vedere. Limita l'accesso all'origine dell'URL di una AWS Lambda funzione
- Se non utilizzi OAC, puoi impostare il `AuthType` parametro dell'URL della funzione su `NONE` e consentire l'`lambda:InvokeFunctionUrl`autorizzazione in una politica basata sulle risorse.

Puoi anche aggiungere un'intestazione di origine personalizzata alle richieste CloudFront inviate all'origine e scrivere un 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 sugli URL delle funzioni Lambda, consulta i seguenti argomenti nella Guida per gli sviluppatori di AWS Lambda :

- URL funzione Lambda: una panoramica generale della funzione URL della funzione Lambda

- Richiamo di URL della funzione Lambda: include dettagli sui payload di richieste e risposte da utilizzare per la codifica dell'applicazione Web serverless
- Modello di sicurezza e autenticazione per gli URL delle funzioni Lambda: include dettagli sui tipi di autenticazione Lambda

Usa Amazon EC2 (o un'altra origine personalizzata)

Un'origine personalizzata è un server Web HTTP (S) con un nome DNS risolvibile pubblicamente che indirizza le richieste dai client alle destinazioni su Internet. Il server HTTP (S) può essere ospitato su, ad AWS esempio, un'istanza Amazon EC2, 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 “Usa un bucket Amazon S3 configurato come 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 URL firmati e cookie firmati”.

Segui queste linee guida per utilizzare le istanze Amazon EC2 e altre origini personalizzate con. CloudFront

- Ospita e servi gli stessi contenuti su tutti i server che forniscono contenuti per la stessa CloudFront origine. Per ulteriori informazioni, consulta the section called “Origin Settings (Impostazioni di origine)” nell'argomento the section called “Distribution Settings (Impostazioni distribuzione)”.
- Registra le voci di `X-Amz-Cf-Id` intestazione su tutti i server nel caso in cui sia necessario AWS Support 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 gli URL e i cookie firmati, per i log e i report. Inoltre, se monitori CloudFront l'attività utilizzando le CloudWatch metriche, tieni presente che CloudWatch utilizza 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 “Limita l'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 le origini personalizzate, ti consigliamo di eseguire quanto segue:

- Utilizza Immagine macchina Amazon che installa automaticamente il software per un server Web. Per ulteriori informazioni, consulta la documentazione di Amazon EC2.
- Utilizza un load balancer Elastic Load Balancing per gestire il traffico tra più istanze di Amazon EC2 e isolare la tua applicazione dalle modifiche alle istanze di Amazon EC2. Ad esempio, se utilizzi un sistema di bilanciamento del carico, puoi aggiungere ed eliminare istanze di Amazon EC2; senza modificare la tua applicazione. Per ulteriori informazioni, consulta la Guida per l'utente di Elastic Load Balancing.
- 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 “Aumenta la disponibilità con il failover di origine”.

Utilizza URL personalizzati aggiungendo nomi di dominio alternativi (CName)

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 informazioni su come utilizzare il proprio nome di dominio, ad esempio www.example.com, consulta i seguenti argomenti:

Argomenti

Requisiti per l'utilizzo di nomi di dominio alternativi

Quando aggiungi un nome di dominio alternativo, ad esempio www.example.com, a una CloudFront distribuzione, i requisiti sono i seguenti:

I nomi di dominio alternativi devono essere in lettere minuscole

Tutti i nomi di dominio alternativi (CNAME) devono essere minuscoli.

I nomi di dominio alternativi devono essere coperti da un certificato SSL/TLS valido

Per aggiungere un nome di dominio alternativo (CNAME) a una CloudFront distribuzione, devi allegare alla distribuzione un certificato SSL/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 un CNAME correlato CloudFront 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 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

Gli esempi seguenti illustrano come utilizzare i caratteri jolly nei nomi di dominio in un certificato per autorizzare l'utente ad aggiungere 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 Usa 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 il tuo account possiede l'altra distribuzione. 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.

Domain Fronting

CloudFront include la protezione contro il fronting dei domini che si verificano tra account diversi. AWS Il domain fronting è uno scenario in cui un client non standard crea una connessione TLS/SSL a un nome di dominio in un AWS account, ma poi effettua una richiesta HTTPS per un nome non correlato in un altro account. AWS Ad esempio, la connessione TLS potrebbe connettersi a www.example.com e quindi effettuare una richiesta HTTP per www.example.org.

Per evitare casi in cui il fronting del dominio intersechi AWS account CloudFront diversi, assicurati che l' AWS account proprietario del certificato utilizzato per una connessione specifica corrisponda sempre all' AWS account proprietario della richiesta che gestisce sulla stessa connessione.

Se i due numeri di AWS account non corrispondono, CloudFront risponde con una risposta HTTP 421 Misdirected Request per dare al client la possibilità di connettersi utilizzando il dominio corretto.

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 due vantaggi 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). Inoltre, quando utilizzi un set di record di risorse alias, non hai alcun addebito per le query Route 53.

> **Note**
>
> Se abiliti IPv6, devi creare due set di record di risorse alias: uno per instradare il traffico IPv4 (un record A) e uno per instradare il traffico IPv6 (un record AAAA). Per ulteriori informazioni, consulta Enable IPv6 (Abilita IPv6) nell'argomento Riferimento alle 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.

Aggiungi 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, consultaConfigurare le distribuzioni.

> **Note**
>
> Se desideri che i visualizzatori utilizzino HTTPS con il tuo nome di dominio alternativo, consulta Usa 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 SSL/TLS da un'autorità di certificazione autorizzata (CA) 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.

Aggiungi un nome di dominio alternativo

1. Accedi a AWS Management Console 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:

   Alternate Domain Names (CNAMEs) (Nomi di dominio alternativi (CNAME))

   Aggiungi i nomi di dominio alternativi. Separa i nomi di dominio con le virgole o digita ogni nome di dominio su una riga.

   Certificato SSL

   Scegliere l'impostazione seguente:

   - Utilizza HTTPS - Seleziona Custom SSL Certificate (Certificato SSL personalizzato), quindi scegli un certificato dall'elenco. L'elenco include i certificati forniti da AWS Certificate Manager (ACM), i certificati acquistati da un'altra CA e caricati su ACM e i certificati acquistati da un'altra CA e caricati nell'archivio certificati IAM.

Se hai caricato un certificato nello store certificati IAM ma non viene visualizzato nell'elenco, consulta la procedura Importa un certificato SSL/TLS per avere la conferma del suo corretto caricamento.

Se scegli questa impostazione, ti consigliamo di utilizzare solo un nome di dominio alternativo negli URL di oggetti (https://www.example.com/logo.jpg). Se si utilizza il nome di dominio di CloudFront distribuzione (https://d111111abcdef8.cloudfront.net.cloudfront.net/logo.jpg), un visualizzatore potrebbe comportarsi come segue, a seconda del valore scelto per Clients Supported:

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

Clients Supported (Client supportati)

Seleziona un'opzione:

- Tutti i client: CloudFront fornisce i tuoi contenuti HTTPS utilizzando indirizzi IP dedicati. Se selezioni questa opzione, ti vengono addebitati costi aggiuntivi quando associ il certificato SSL/TLS a una distribuzione abilitata. Per ulteriori informazioni, consulta Prezzi di Amazon CloudFront.
- Solo client che supportano la Server Name Indication (SNI) (scelta consigliata): browser meno recenti o altri client che non supportano la SNI devono utilizzare un altro metodo per accedere ai tuoi contenuti.

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

5. Seleziona Yes, Edit (Sì, modifica).
6. 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.
7. Configura il servizio DNS per il nome di dominio alternativo (come www.example.com) per indirizzare il traffico verso il nome di CloudFront dominio per la tua distribuzione (come 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.

> **Note**
>
> Se il record DNS punta già a una distribuzione che non è quella che stai aggiornando, puoi aggiungere il nome di dominio alternativo alla distribuzione dopo aver aggiornato il DNS. Per ulteriori informazioni, consulta Restrizioni sull'utilizzo dei nomi di dominio alternativi.

Route 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. Inoltre, puoi creare un set di record di risorse alias per il nome di dominio root (example.com), che DNS non consente per i CNAME. 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.

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 della 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

8. 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.

9. Prova il nome di dominio alternativo visitando gli URL con il tuo nome di dominio anziché il nome di CloudFront dominio della tua distribuzione.
10. Nell'applicazione, modificate gli URL dei vostri oggetti in modo da utilizzare il vostro nome di dominio alternativo anziché il nome di dominio della vostra distribuzione. CloudFront

Sposta un nome di dominio alternativo in una distribuzione diversa

Quando cerchi di aggiungere un nome di dominio alternativo a una distribuzione ma il nome di dominio alternativo è già in uso in una distribuzione diversa, viene restituito un errore `CNAMEAlreadyExists` (Uno o più CNAME forniti sono già associati a una risorsa differente). Ad esempio, questo errore viene visualizzato quando si prova ad aggiungere www.example.com a una distribuzione, ma www.example.com è già associato a un'altra distribuzione.

In tal caso, è possibile spostare il nome di dominio alternativo esistente da una distribuzione (distribuzione di origine) a un'altra (distribuzione di destinazione). I passaggi seguenti sono una panoramica del processo. Per ulteriori informazioni, consulta il link in ogni fase della panoramica.

Come spostare un nome di dominio alternativo

1. Configurare la distribuzione di destinazione. Questa distribuzione deve avere un certificato SSL/TLS che copre il nome di dominio alternativo che si sta spostando. Per ulteriori informazioni, consulta Configurazione della distribuzione di destinazione.
2. Individuare la distribuzione di origine. Puoi usare il AWS Command Line Interface (AWS CLI) per trovare la distribuzione a cui è associato il nome di dominio alternativo. Per ulteriori informazioni, consulta Individuazione della distribuzione di origine.
3. Spostare il nome di dominio alternativo. Il modo in cui eseguire questa operazione dipende dal fatto che le distribuzioni di origine e di destinazione si trovino nello stesso AWS account. Per ulteriori informazioni, consulta the section called “Spostamento del nome di dominio alternativo”.

Configurazione della distribuzione di destinazione

Prima di spostare un nome di dominio alternativo, è necessario impostare la distribuzione di destinazione (la distribuzione in cui si sta spostando il nome di dominio alternativo).

Come configurare la distribuzione di destinazione

1. Ottieni un certificato SSL/TLS che include il nome di dominio alternativo che si sta spostando. Se non ne hai uno, puoi richiederlo da AWS Certificate Manager (ACM) o ottenerlo da un'altra autorità di certificazione (CA) e importarlo in ACM. Assicurati di richiedere o importare il certificato nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).
2. Se la distribuzione di destinazione non è stata creata, creane una ora. Come parte della creazione della distribuzione di destinazione, associa il certificato (dal passaggio precedente) alla distribuzione. Per ulteriori informazioni, consulta Creazione di una distribuzione.

   Se disponi già di una distribuzione di destinazione, associa il certificato (dal passaggio precedente) alla distribuzione di destinazione. Per ulteriori informazioni, consulta Aggiornamento di una distribuzione.
3. Crea un record TXT DNS che associa il nome di dominio alternativo al nome di dominio di distribuzione della distribuzione di destinazione. Crea il tuo record TXT con un carattere di sottolineatura (_) davanti al nome di dominio alternativo. Di seguito viene illustrato un record TXT di esempio in DNS:

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

CloudFront utilizza questo record TXT per convalidare la proprietà del nome di dominio alternativo.

Individuazione della distribuzione di origine

Prima di spostare un nome di dominio alternativo da una distribuzione a un'altra, è necessario trovare la distribuzione di origine (la distribuzione in cui è attualmente in uso il nome di dominio alternativo). Se conosci l'ID account AWS delle distribuzioni di origine e di destinazione, è possibile determinare come spostare il nome di dominio alternativo.

Come trovare la distribuzione di origine per il nome di dominio alternativo

1. Utilizzate il CloudFront list-conflicting-aliasescomando in AWS Command Line Interface (AWS CLI) come illustrato nell'esempio seguente. Sostituisci *www.example.com* con il nome di dominio alternativo e *EDFDVBD6EXAMPLE* con l'ID della distribuzione di destinazione che hai impostato in precedenza. Esegui questo comando utilizzando credenziali che si trovano nello stesso AWS account della distribuzione di destinazione. Per utilizzare questo comando, è necessario disporre delle autorizzazioni `cloudfront:GetDistribution` e `cloudfront:ListConflictingAlias` nella distribuzione di destinazione.

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

   L'output del comando mostra un elenco di tutti i nomi di dominio alternativi in conflitto o si sovrappongono a quello fornito. Ad esempio:

   - Se fornisci www.example.com al comando, l'output del comando include www.example.com e il nome di dominio alternativo con caratteri jolly sovrapposti (*.example.com), se esiste.
   - Se fornisci *.example.com al comando, l'output del comando include *.example.com ed eventuali nomi di dominio alternativi coperti da quel carattere jolly (ad esempio, www.example.com, test.example.com, dev.example. com, e così via).

   Per ogni nome di dominio alternativo nell'output del comando, è possibile visualizzare l'ID della distribuzione a cui è associato e l'ID account AWS proprietario della distribuzione. Gli ID di distribuzione e account sono parzialmente nascosti, il che consente di identificare le distribuzioni

e gli account di cui si è proprietari, ma aiuta a proteggere le informazioni di quelli di cui non si è proprietari.

2. Nell'output del comando, trova la distribuzione per il nome di dominio alternativo che stai spostando e annota l'ID dell' AWS account della distribuzione di origine. Confronta l'ID dell'account della distribuzione di origine con l'ID dell'account in cui hai creato la distribuzione di destinazione e determina se queste due distribuzioni si trovano nello stesso AWS account. In questo modo è possibile determinare come spostare il nome di dominio alternativo.

   Per spostare il nome di dominio alternativo, consulta il seguente argomento.

Spostamento del nome di dominio alternativo

A seconda della situazione, scegli una delle seguenti modalità per spostare il nome di dominio alternativo:

Se le distribuzioni di origine e di destinazione si trovano nello stesso account AWS

Usa il associate-alias comando in AWS CLI per spostare il nome di dominio alternativo. Questo metodo 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). Per ulteriori informazioni, consulta the section called “Usa `associate-alias` per spostare un nome di dominio alternativo”.

Se le distribuzioni di origine e di destinazione si trovano in account AWS differenti

Se si ha accesso alla distribuzione di origine, il nome di dominio alternativo non è un dominio apex (chiamato anche dominio root, come `example.com`) e non si sta 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 all' AWS account della distribuzione di origine, puoi provare a utilizzare il associate-alias comando in AWS CLI per spostare il nome di dominio alternativo. Se la distribuzione di origine è disabilitata, è possibile spostare il nome di dominio alternativo. Per ulteriori informazioni, consulta the section called “Usa `associate-alias` per spostare un nome di dominio alternativo”. Se il file comando associate-alias non funziona, contatta AWS Support. Per ulteriori informazioni, consulta the section called “Contatta AWS Support per spostare un nome di dominio alternativo”.

Usa `associate-alias` per spostare un nome di dominio alternativo

Se la distribuzione di origine si trova nello stesso AWS account della distribuzione di destinazione o se si trova in un account diverso ma è disattivata, puoi utilizzare il CloudFront associate-aliascomando in AWS CLI per spostare il nome di dominio alternativo.

Come utilizzare un alias associato per spostare un nome di dominio alternativo

1. Utilizzate il AWS CLI per eseguire il CloudFront associate-alias comando, come illustrato nell'esempio seguente. Sostituisci *www.example.com* con il nome di dominio alternativo e *EDFDVBD6EXAMPLE* con l'ID della distribuzione di destinazione. Esegui questo comando utilizzando credenziali che si trovano nello stesso AWS account della distribuzione di destinazione. Tenere presente le seguenti limitazioni per l'utilizzo di questo comando:

   - È necessario disporre delle autorizzazioni `cloudfront:AssociateAlias` e `cloudfront:UpdateDistribution` sulla distribuzione di destinazione.
   - Se le distribuzioni di origine e di destinazione si trovano nello stesso account AWS , è necessario disporre dell'autorizzazione `cloudfront:UpdateDistribution` sulla distribuzione di origine.
   - Se le distribuzioni di origine e di destinazione sono in account AWS diversi, la distribuzione di origine deve essere disabilitata.
   - La distribuzione di destinazione deve essere configurata nel modo descritto in the section called “Configurazione della distribuzione di destinazione”.

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

   Questo comando aggiorna entrambe le distribuzioni rimuovendo il nome di dominio alternativo dalla distribuzione di origine e aggiungendolo alla distribuzione di destinazione.
2. 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.

Utilizzo di un carattere jolly per spostare un nome di dominio alternativo

Se la distribuzione di origine si trova in un AWS account diverso rispetto alla distribuzione di destinazione e la distribuzione di 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 AWS Support. Per ulteriori informazioni, consulta the section called “Contatta AWS Support 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 certificato SSL/TLS sulla distribuzione di destinazione deve includere il nome di dominio con caratteri jolly. 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 AWS Support per spostare un nome di dominio alternativo

Se le distribuzioni di origine e di destinazione si trovano in AWS account diversi e non hai accesso all' AWS account della distribuzione di origine o non puoi disabilitare la distribuzione di origine, puoi contattare AWS Support per spostare il nome di dominio alternativo.

A cui rivolgersi AWS Support 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 di destinazione.
2. Contattaci AWS Support 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.

Rimuovi 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 Sposta un nome di dominio alternativo in una distribuzione diversa. 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 che non è la tua CloudFront distribuzione, ad esempio un sistema di bilanciamento del carico Elastic Load Balancing. 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 utilizzi un altro provider di servizi DNS, utilizza il metodo fornito dal provider di servizi DNS per aggiornare o eliminare il record CNAME verso cui indirizza il traffico. 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 AWS Management Console e apri la CloudFront console all'indirizzo e aggiorna https://console.aws.amazon.com/cloudfront/v4/home 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) (Nomi di dominio alternativi (CNAME)), rimuovi il nome di dominio alternativo (o i nomi di dominio) che non desideri più utilizzare per la distribuzione.

   d. Seleziona Yes, Edit (Sì, modifica).

Usa i caratteri jolly in 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 usare qualsiasi nome di dominio che termina con example.com negli URL, ad esempio www.example.com, product-name.example.com, 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
- Product-name.example.com/images/image.jpg
- marketing.product-name.example.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 delle richieste dei visualizzatori alla tua origine. (Puoi utilizzare la politica di richiesta di origine AllViewer gestita.)
- Inoltra in particolare le intestazioni `Sec-WebSocket-Key` and `Sec-WebSocket-Version` request nella tua policy di richiesta di 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/SSL. Le opzioni scelte si Protocollo (solo origini personalizzate) applicano alle WebSocket connessioni CloudFront Viewer Protocol Policy (Policy protocollo visualizzatore) e al traffico HTTP.

WebSocketrequisiti

WebSocket le richieste devono essere conformi alla RFC 6455 nei seguenti formati standard.

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
```

Esempio di risposta di 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 legati 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`

Memorizzazione nella cache e disponibilità

È possibile utilizzare CloudFront per ridurre il numero di richieste a cui il server di origine deve rispondere direttamente. Con la CloudFront memorizzazione nella cache, più oggetti vengono serviti dalle CloudFront edge location, più vicine agli utenti. Questo riduce il carico e la latenza sul server di origine.

Maggiore è il numero di richieste che CloudFront possono essere inviate dalle cache edge, minore è il numero di richieste di visualizzazione che CloudFront devono essere inoltrate all'origine per ottenere la versione più recente o una versione unica di un oggetto. Per ottimizzare CloudFront in modo da inviare il minor numero possibile di richieste alla tua origine, prendi in considerazione l'utilizzo di CloudFront Origin Shield. Per ulteriori informazioni, consulta Utilizzo di Amazon CloudFront Origin Shield.

La proporzione di richieste che vengono servite direttamente dalla CloudFront cache rispetto a tutte le richieste è chiamata rapporto di successo della cache. Nella CloudFront console puoi visualizzare la percentuale di richieste degli utenti che risultano positive, mancate ed errori. Per ulteriori informazioni, consulta Visualizza i report sulle statistiche CloudFront della cache.

L'hit rate della cache è influenzato da diversi fattori. È possibile modificare la configurazione di CloudFront distribuzione per migliorare il rapporto di accesso alla cache seguendo le istruzioni riportate inAumentare la percentuale di richieste che vengono servite direttamente dalle CloudFront cache (rapporto di successo della cache).

Per ulteriori informazioni su come aggiungere e rimuovere il contenuto che desideri CloudFront pubblicare, consultaAggiungere, rimuovere o sostituire i contenuti CloudFront distribuiti.

Argomenti

Aumentare la percentuale di richieste che vengono servite direttamente dalle CloudFront cache (rapporto di successo della cache)

È possibile migliorare le prestazioni aumentando la percentuale di richieste dei visualizzatori che vengono servite direttamente dalla CloudFront cache anziché passare ai server di origine per la raccolta dei 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

Specificate per quanto tempo CloudFront i vostri oggetti vengono memorizzati nella cache

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 della cache, più frequentemente vengono CloudFront inviate richieste all'origine per determinare se un oggetto è cambiato 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 Gestisci la durata della permanenza dei contenuti nella cache (scadenza).

Usa Origin Shield

CloudFront Origin Shield può aiutarti a migliorare il rapporto di accesso alla cache della tua CloudFront distribuzione, poiché fornisce un ulteriore livello di caching davanti all'origine. Quando usi

Origin Shield, tutte le richieste provenienti da tutti i livelli CloudFront di memorizzazione nella cache all'origine provengono da un'unica posizione. CloudFront può recuperare ogni oggetto utilizzando una singola richiesta di origine da Origin Shield e tutti gli altri livelli della CloudFront cache (edge location e cache edge regionali) possono recuperare l'oggetto da Origin Shield.

Per ulteriori informazioni, consulta Utilizzo di Amazon CloudFront Origin Shield.

Caching Basato su parametri della stringa di query

Se configuri la cache CloudFront in base ai parametri della stringa di query, puoi migliorare la memorizzazione nella cache se esegui le seguenti operazioni:

- CloudFront Configurate per inoltrare solo i parametri della stringa di query per i quali l'origine restituirà oggetti unici.
- 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, anche se gli oggetti sono identici. Se usi just `A` ora, CloudFront inoltra meno richieste alla tua origine.
- Elenca i parametri nello stesso ordine. Per quanto riguarda le differenze tra maiuscole e minuscole, 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 all'origine e memorizza separatamente nella cache gli oggetti corrispondenti anche se sono identici. Se usi sempre lo stesso ordine per i parametri, CloudFront inoltra meno richieste all'origine.

Per ulteriori informazioni, consulta Contenuto della cache in base ai parametri della stringa di query. Se desideri esaminare le stringhe di query che CloudFront inoltrano all'origine, consulta i valori nella `cs-uri-query` colonna dei tuoi CloudFront file di registro. Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso).

Caching in base ai valori dei cookie

Se configuri la memorizzazione nella cache in base CloudFront ai valori dei cookie, puoi migliorare la memorizzazione nella cache effettuando le seguenti operazioni:

- Configura CloudFront per inoltrare solo i cookie specifici invece di inoltrare tutti i cookie. Per i cookie che configuri per l'inoltro CloudFront all'origine, CloudFront inoltra ogni combinazione di nome e valore del cookie. Quindi memorizza nella cache separatamente gli oggetti restituiti dall'origine, anche se sono tutti identici.

  Ad esempio, supponiamo che gli utenti includano due cookie in ogni richiesta, che ogni cookie abbia tre valori possibili e che tutte le combinazioni di valori dei cookie siano possibili. CloudFront inoltra fino a sei richieste diverse all'origine per ogni oggetto. Se l'origine restituisce versioni diverse di un oggetto in base a uno solo dei cookie, allora CloudFront sta inoltrando all'origine più richieste del necessario e sta inutilmente memorizzando nella cache più versioni identiche dell'oggetto.
- Crea comportamenti di cache separati per i contenuti statici e dinamici e configura l'inoltro dei cookie CloudFront all'origine solo per i contenuti dinamici.

  Ad esempio, supponiamo di avere un solo comportamento di cache per la distribuzione e di utilizzare la distribuzione sia per contenuti dinamici, come `.js` i file, sia per `.css` file che vengono modificati raramente. CloudFront memorizza nella cache versioni separate dei `.css` file in base ai valori dei cookie, in modo che ogni CloudFront edge location inoltri una richiesta all'origine per ogni nuovo valore di cookie o combinazione di valori dei cookie.

  Se create un comportamento di cache per il quale corrisponde lo schema di percorso `*.css` e per il quale CloudFront non lo memorizzate in base ai valori dei cookie, CloudFront inoltra le richieste di `.css` file all'origine solo per la prima richiesta ricevuta da una edge location per un determinato `.css` file e per la prima richiesta dopo la scadenza di un `.css` file.
- 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 Contenuto della cache basato sui cookie. Se desideri esaminare i cookie che CloudFront inoltrano alla tua origine, consulta i valori nella `cs(Cookie)` colonna dei tuoi CloudFront file di registro. Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso).

Caching in base alle intestazioni di richiesta

Se CloudFront configuri la memorizzazione nella cache in base alle intestazioni delle richieste, puoi migliorare la memorizzazione nella cache effettuando le seguenti operazioni:

- Configura CloudFront l'inoltro e la memorizzazione nella cache in base solo alle intestazioni specificate anziché all'inoltro e alla memorizzazione nella cache in base a tutte le intestazioni. Per le intestazioni specificate, CloudFront inoltra ogni combinazione di nome e valore dell'intestazione. Quindi memorizza nella cache separatamente gli oggetti restituiti dall'origine, anche se sono tutti identici.

  > **Note**
  >
  > CloudFront inoltra sempre all'origine le intestazioni specificate nei seguenti argomenti:
  >
  > - In che modo CloudFront elabora e inoltra le richieste al tuo server di origine Amazon S3 > Intestazioni di richiesta HTTP che rimuovono o aggiornano CloudFront
  > - In che modo CloudFront elabora e inoltra le richieste al tuo server di origine personalizzato > Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

  Quando configurate la memorizzazione nella cache in base CloudFront alle intestazioni delle richieste, non modificate le intestazioni da CloudFront inoltrare, ma solo se CloudFront memorizzate nella cache gli oggetti in base ai valori delle intestazioni.

- 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 desiderate pubblicare immagini di dimensioni diverse in base al dispositivo dell'utente, non configurate la cache in base CloudFront all'`User-Agent`intestazione, che ha un numero enorme di valori possibili. Configura CloudFront invece la memorizzazione nella cache in base alle intestazioni `CloudFront-Is-Desktop-Viewer` del CloudFront tipo di dispositivo,, e. `CloudFront-Is-Mobile-Viewer` `CloudFront-Is-SmartTV-Viewer` `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 Contenuto della cache in base alle intestazioni delle richieste.

Rimuovere l'intestazione **`Accept-Encoding`** quando la compressione non è necessaria

Se la compressione non è abilitata, perché l'origine non la supporta, non la supporta o il contenuto CloudFront non è comprimibile, puoi aumentare il rapporto di accesso alla cache associando un comportamento della cache nella tua distribuzione a un'origine che imposta quanto segue: Custom Origin Header

- Nome intestazione: `Accept-Encoding`
- Header value (Valore intestazione): (Lasciare vuoto)

Quando usi questa configurazione, CloudFront rimuove l'intestazione dalla chiave della cache e non include l'`Accept-Encoding`intestazione nelle richieste di origine. Questa configurazione si applica a tutto il contenuto che CloudFront serve alla distribuzione da quell'origine.

Offri 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.

Utilizzo di 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 CloudFront Origin Shield, 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. CloudFrontpuò 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 il just-in-time packaging, la trasformazione 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, consulta la pagina CloudFront Prezzi.

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 per la distribuzione di contenuti (CDN)

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
- CDN multipli

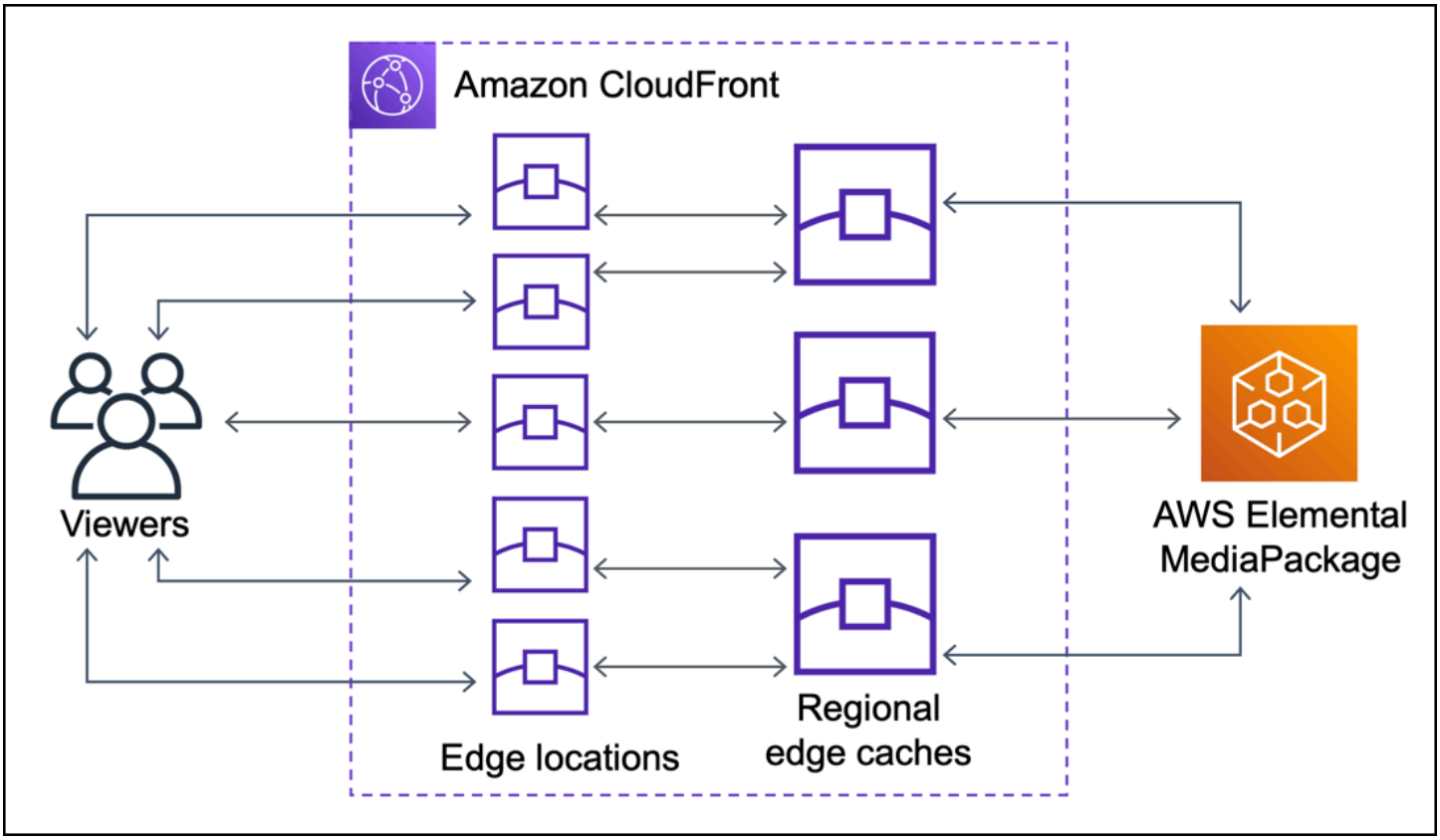
Visualizzatori in diverse regioni geografiche

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 dei visualizzatori vengono prima indirizzate a una CloudFront edge location vicina e, se l'oggetto non è memorizzato nella cache in quella 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 diagrammi seguenti, l'origine è. AWS Elemental MediaPackage

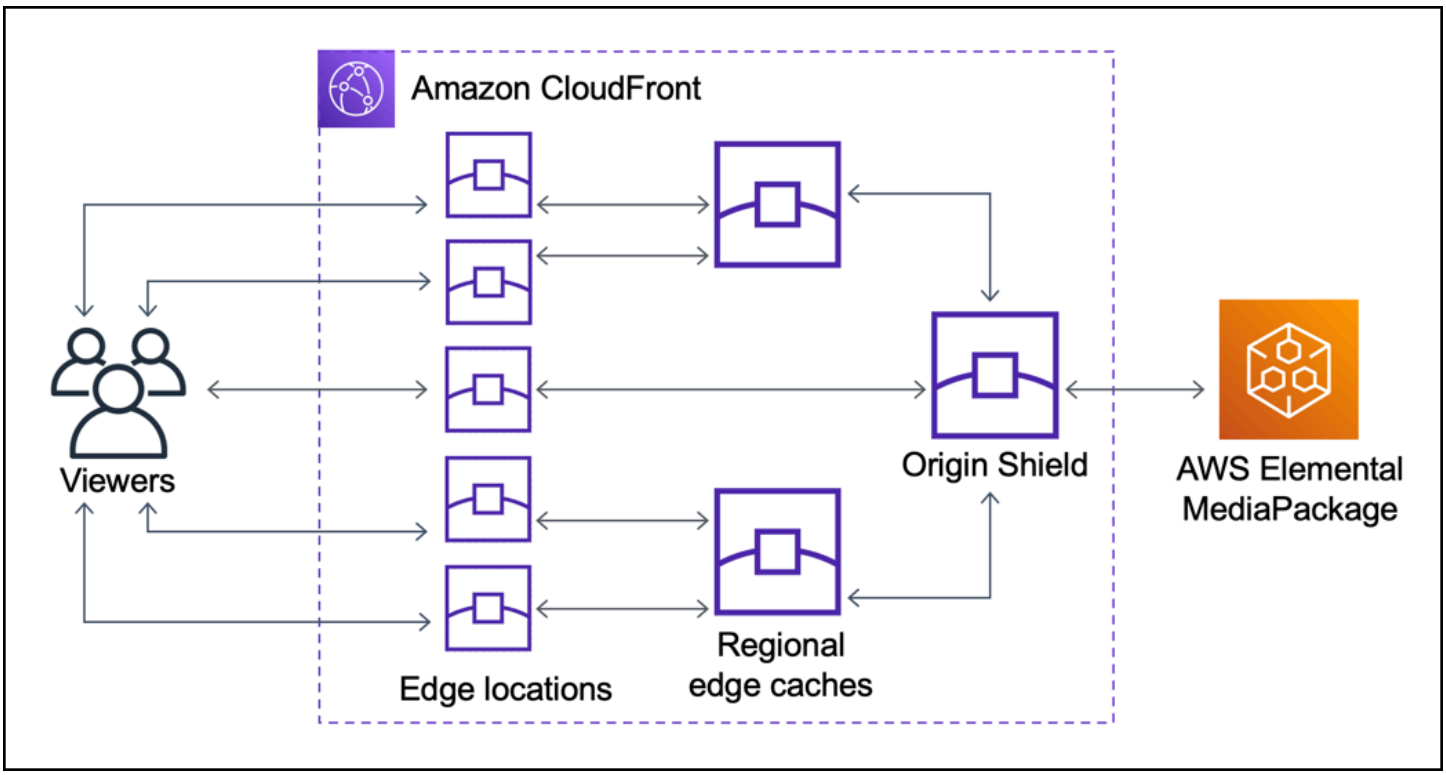
Senza scudo di origine

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.



CDN multipli

Per servire eventi video in diretta o contenuti su richiesta più diffusi, è possibile utilizzare più reti CDN (Content Delivery Network). L'utilizzo di più CDN può offrire alcuni vantaggi, ma significa anche che l'origine potrebbe ricevere molte richieste duplicate per lo stesso contenuto, ognuna proveniente da CDN diversi o posizioni diverse all'interno della stessa rete CDN. Queste richieste ridondanti potrebbero influire negativamente sulla disponibilità dell'origine o causare costi operativi aggiuntivi per processi come l' just-in-time imballaggio o il trasferimento dei dati (DTO) su Internet.

Combinando Origin Shield con l'utilizzo della CloudFront distribuzione come origine per altri CDN, puoi ottenere i seguenti vantaggi:

- Meno richieste ridondanti ricevute all'origine, riducendo così gli effetti negativi dell'utilizzo di più CDN.
- Una chiave cache comune tra i CDN e gestione centralizzata per le funzionalità di origine.
- Prestazioni di rete migliorate. Il traffico di rete proveniente da altri CDN 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

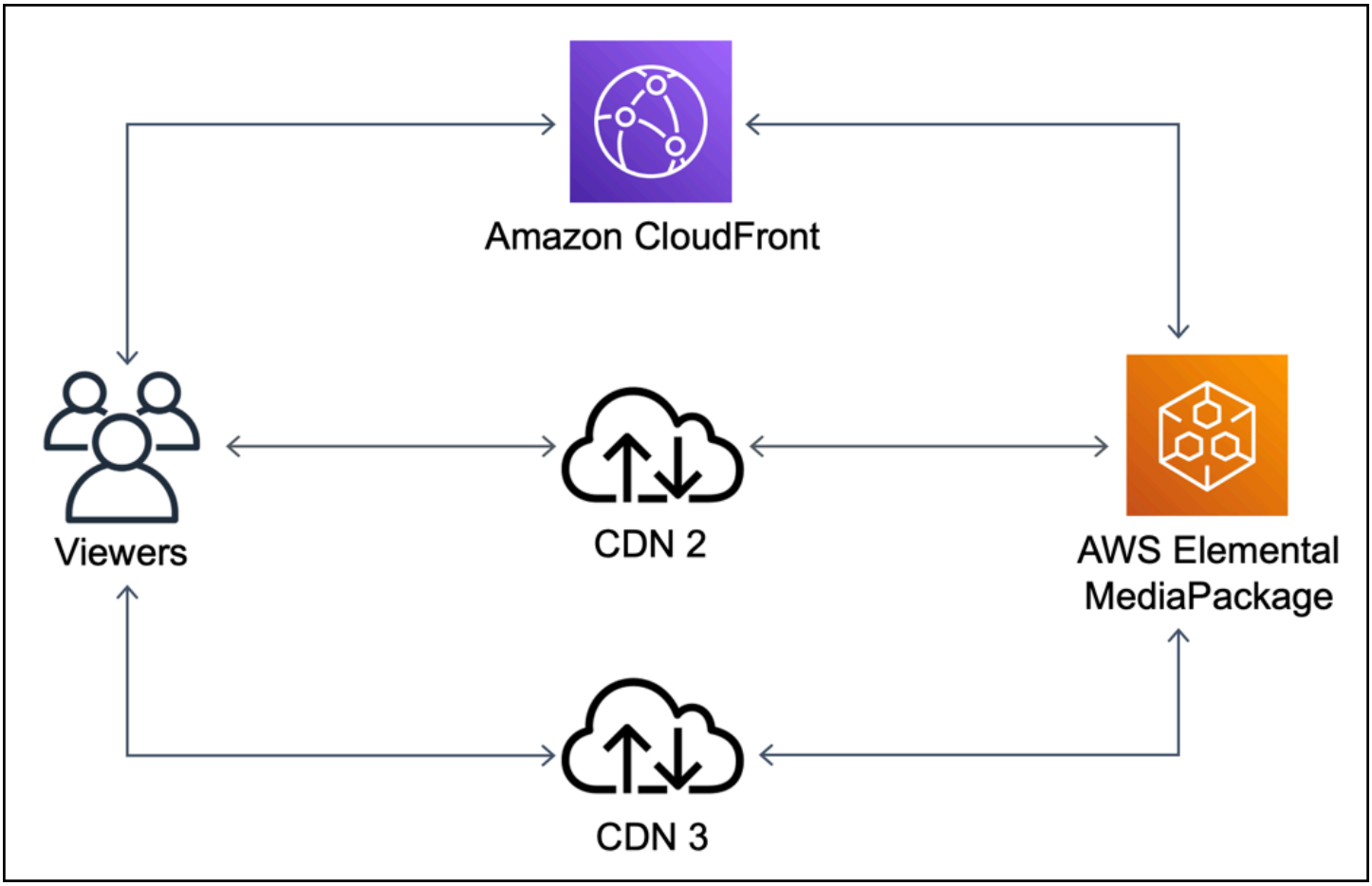
l'oggetto richiesto si trova nella cache dello scudo di origine, la richiesta all'origine viene evitata completamente.

> **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 diagrammi seguenti mostrano come questa configurazione può contribuire a ridurre al minimo il carico sull'origine quando si servono eventi video live popolari con più CDN. Nei diagrammi seguenti, l'origine è. AWS Elemental MediaPackage

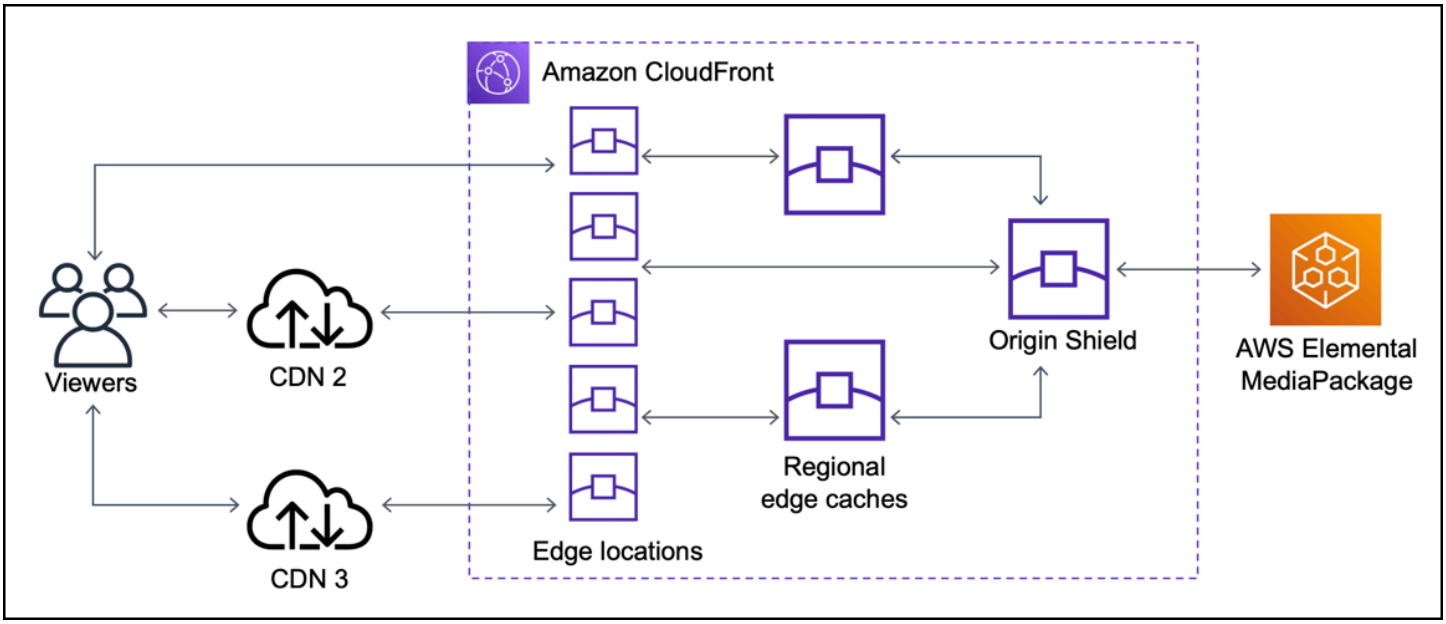
Senza scudo di origine (più CDN)

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 scudo di origine (più CDN)

L'uso di Origin Shield, con CloudFront come origine per gli altri CDN, può aiutare a ridurre il carico sull'origine, come mostrato nel diagramma seguente.



Scelta della 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 si trovano in AWS.

Per le origini in una regione AWS

Se sei originario di una AWS regione, stabilisci innanzitutto se proviene da una regione in cui è disponibile CloudFront 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`

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 istanze Amazon EC2 in alcune AWS regioni diverse geograficamente vicine alla tua origine ed eseguire alcuni test per misurare le latenze di rete tipiche tra tali regioni e la tua origine. `ping`

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 AWS CloudFormation, con o con l' CloudFrontAPI.

Console

Per abilitare Origin Shield per un'origine esistente (console)

1. Accedi AWS Management Console 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. Scegli la scheda Origins and Origin Groups (Origini e gruppi di 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, scegli la AWS regione in cui desideri abilitare Origin Shield. Per informazioni sulla scelta di una regione, vedere Scelta della AWS regione per Origin Shield.
7. Nella parte inferiore della pagina scegliere Sì, modifica.

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 AWS Management Console 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, effettuare le seguenti operazioni:

   1. Scegliere Create Distribution (Crea distribuzione).
   2. Nella sezione Web scegliere Get Started (Inizia). Nella sezione Origin Settings (Impostazioni origine) completare i passaggi seguenti, iniziando con il passaggio 3.
3. Per Enable Origin Shield (Abilita scudo di origine), scegliere Yes (Sì).
4. Per Origin Shield Region, scegli la AWS regione in cui desideri abilitare Origin Shield. Per informazioni sulla scelta di una regione, vedere Scelta della AWS regione per Origin Shield.

   Se si sta creando una nuova distribuzione, continuare a configurare la distribuzione utilizzando le altre impostazioni nella pagina. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.
5. Assicurarsi di salvare le modifiche scegliendo Create (Crea) (per una nuova origine in una distribuzione esistente) o Create Distribution (Crea distribuzione) (per una nuova origine in una nuova distribuzione).

Quando lo stato di distribuzione è Deployed (Distribuito), Origin Shield è pronto. Ci vogliono pochi minuti.

AWS CloudFormation

Per abilitare Origin Shield con AWS 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 “Scelta della 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 gli SDK o 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`.

`GET`e `HEAD` le richieste con un'impostazione TTL (time to live) inferiore a 3600 secondi sono considerate richieste dinamiche. Inoltre, anche `GET` le `HEAD` richieste che hanno disabilitato la memorizzazione nella 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, e `GET` `HEAD`,`OPTIONS`, Origin Shield è talvolta un livello incrementale. Quando attivi Origin Shield, scegli Origin Shield. Regione AWS Per le richieste che vanno naturalmente alla cache edge regionale nella stessa regione di Origin Shield, Origin Shield non è un livello incrementale. Non ti vengono addebitati costi Origin Shield per queste richieste. Per le richieste che vanno a una cache edge regionale in una regione diversa da Origin Shield e poi vanno a Origin Shield, Origin Shield è 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 Origin Shield, consulta la CloudFront pagina Prezzi.

Alta disponibilità di Origin Shield.

Origin Shield sfrutta la funzionalità di cache edge CloudFront regionali. Ciascuna di queste cache edge è integrata in una AWS regione che utilizza almeno tre zone di disponibilità con flotte di istanze Amazon EC2 con scalabilità automatica. Le connessioni dalle CloudFront postazioni a Origin Shield

utilizzano anche il tracciamento attivo degli errori per ogni richiesta per indirizzare automaticamente la richiesta a una posizione Origin Shield secondaria se la posizione Origin Shield principale non è disponibile.

In che modo Origin Shield interagisce con altre funzionalità CloudFront

Le seguenti sezioni spiegano come Origin Shield interagisce con altre CloudFront funzionalità.

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 in tempo reale. Sono previsti costi aggiuntivi per l'utilizzo dei registri in tempo reale. Consulta CloudFront i prezzi 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

Origin Shield è compatibile con i gruppi di CloudFront origine. 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 verso 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.

Ottimizza l'alta disponibilità con il failover di CloudFront origine

È possibile eseguire la configurazione CloudFront con il failover di origine per scenari che richiedono un'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, passa CloudFront 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 Crea un gruppo di origine.

Dopo aver configurato il failover di origine per il comportamento della cache, CloudFront esegue le seguenti operazioni per le richieste dei visualizzatori:

- Quando si verifica un accesso alla cache, CloudFront restituisce l'oggetto richiesto.
- In caso di perdita della cache, CloudFront indirizza la richiesta all'origine primaria del 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, invia l' CloudFront 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
  - La risposta dall'origine primaria richiede troppo tempo (time out)

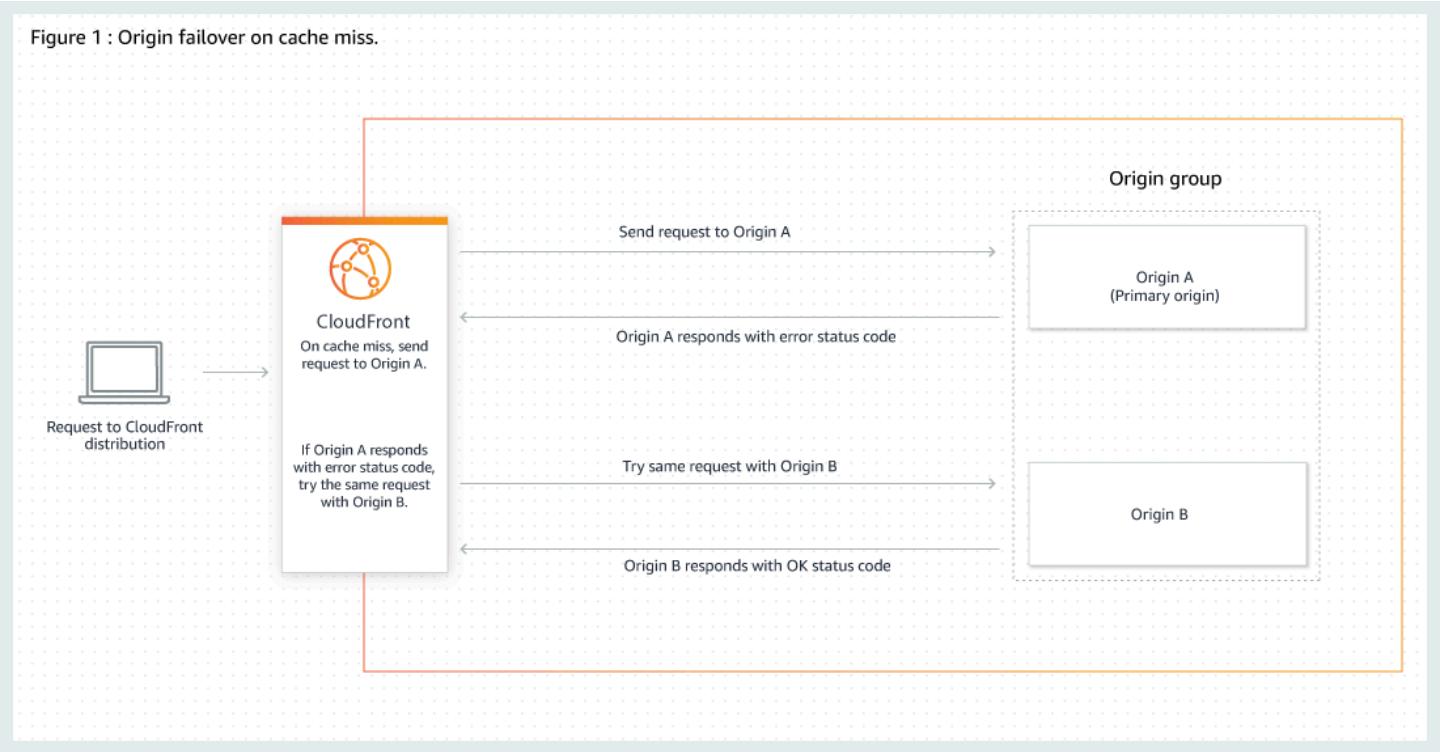
  Quindi CloudFront indirizza la richiesta all'origine secondaria nel gruppo di origine.

> **Note**
>
> In alcuni casi d'uso, come lo streaming di contenuti video, potresti CloudFront voler eseguire rapidamente il failover sull'origine secondaria. Per regolare la velocità di CloudFront failover sull'origine secondaria, consultaControlla i timeout e i tentativi di origine.

CloudFront indirizza tutte le richieste in entrata all'origine primaria, anche quando una richiesta precedente non è passata all'origine secondaria. CloudFront invia 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 `GETHEAD`, o`OPTIONS`. CloudFront non esegue il failover quando il visualizzatore invia un metodo HTTP diverso (ad esempio `POSTPUT`, e così via).

Il diagramma seguente illustrato il funzionamento del failover di origine.



Argomenti

- Crea un gruppo di origine

- Controlla i timeout e i tentativi di origine
- Utilizzo del failover di origine con le funzioni Lambda@Edge
- Utilizzo di pagine di errore personalizzate con failover di origine

Crea un gruppo di origine

Per creare un gruppo di origine

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://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, passa all'origine secondaria.

   > **Note**
   >
   > CloudFront esegue il failover sull'origine secondaria solo quando il metodo HTTP della richiesta del visualizzatore è `GETHEAD`, o`OPTIONS`. CloudFront non esegue il failover quando il visualizzatore invia un metodo HTTP diverso (ad esempio `POSTPUT`, e così via).

9. Scegliere Crea un gruppo di origine.

Assicurati di assegnare il tuo gruppo di origine come origine per il comportamento della cache della tua distribuzione. Per ulteriori informazioni, consulta Nome.

Controlla i timeout e i tentativi di origine

Per impostazione predefinita, CloudFront tenta di connettersi all'origine primaria in un gruppo di origine per un massimo di 30 secondi (3 tentativi di connessione da 10 secondi ciascuno) prima di eseguire il failover sull'origine secondaria. In alcuni casi d'uso, come lo streaming di contenuti video, potresti CloudFront voler eseguire il failover sull'origine secondaria più rapidamente. È possibile modificare le seguenti impostazioni per influire sulla velocità di CloudFront failover sull'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 velocità di CloudFront restituzione di 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 delle CloudFront attese quando si tenta di stabilire una connessione all'origine. Per impostazione predefinita, CloudFront attende 10 secondi per stabilire una connessione, ma è possibile specificare da 1 a 10 secondi (inclusi). Per ulteriori informazioni, consulta Timeout di connessione.

Tentativi di connessione all'origine

L'impostazione dei tentativi di connessione all'origine influisce sul numero di CloudFront tentativi di connessione all'origine. Per impostazione predefinita, CloudFront tenta di connettersi 3 volte, ma è possibile specificare 1—3 (incluso). 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 volte in cui si CloudFront tenta di ottenere una risposta dall'origine in caso di timeout della risposta di origine.

Timeout di risposta origine

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

L'impostazione del timeout della risposta di origine influisce sulla durata di CloudFront attesa 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 60 secondi (inclusi). Per ulteriori informazioni, consulta Timeout di risposta (solo origini personalizzate).

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.

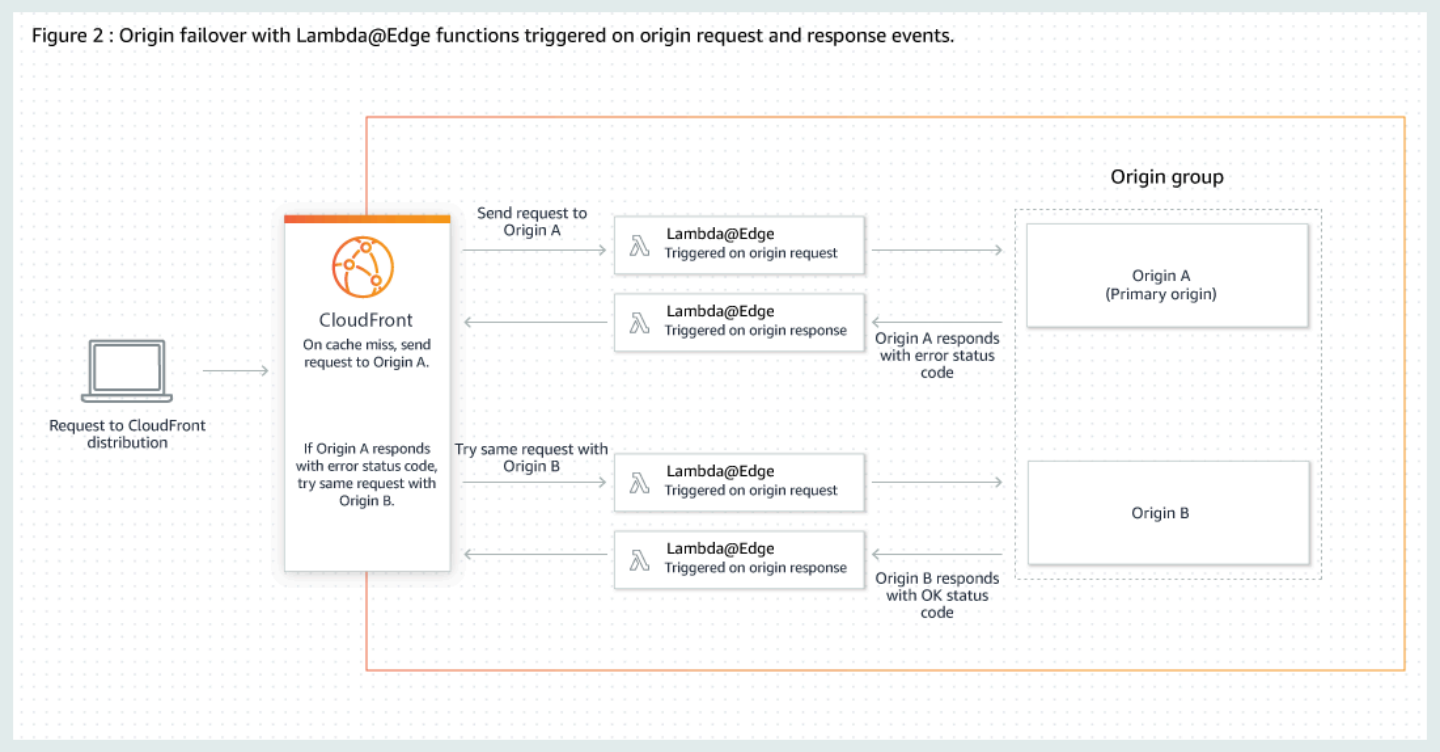
Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.

Utilizzo del failover di origine con le funzioni Lambda@Edge

Puoi usare le funzioni Lambda @Edge con le CloudFront distribuzioni che hai configurato 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 (in caso di perdita della cache).
3. L'origine primaria risponde con un codice di stato HTTP configurato per il failover.
4. La funzione Lambda viene riattivata 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 dell'origine.



Per ulteriori informazioni sull'utilizzo dei trigger Lambda@Edge, consulta the section called "Aggiungere trigger per una funzione Lambda @Edge".

Per ulteriori informazioni sulla gestione del failover DNS, consulta la sezione Configurazione del failover DNS nella Amazon Route 53 Developer Guide.

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 utilizzi il failover di origine, puoi configurare CloudFront la restituzione di una pagina di errore personalizzata per l'origine primaria o secondaria (o entrambe):

- Restituisce una pagina di errore personalizzata per l'origine principale: 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, vedereGenerazione di risposte di errore personalizzate.

Gestisci la durata della permanenza dei contenuti nella cache (scadenza)

Puoi controllare per quanto tempo i tuoi file rimangono in una CloudFront cache prima di CloudFront inoltrare 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 serve un file da una edge location fino alla scadenza della durata della cache specificata, ovvero fino alla scadenza del file. Dopo la scadenza, la volta successiva che l'edge location riceve una richiesta per il file, CloudFront inoltra la richiesta all'origine per verificare che la cache contenga la versione più recente del file. La risposta dall'origine dipende dall'eventuale modifica del file:

- Se la CloudFront cache ha già la versione più recente, l'origine restituisce un codice di stato. `304 Not Modified`
- Se la CloudFront cache non ha la versione più recente, l'origine restituisce un codice di stato `200 OK` e la versione più recente del file.

Se un file in una edge location non viene richiesto frequentemente, CloudFront potrebbe eliminarlo, ovvero rimuoverlo prima della data di scadenza, per fare spazio ai file che sono stati richiesti più di recente.

Per impostazione predefinita, ogni file scade automaticamente dopo 24 ore, ma puoi modificare il comportamento predefinito in due modi:

- Per modificare la durata della cache per tutti i file che corrispondono allo stesso modello di percorso, puoi modificare le CloudFront impostazioni di TTL minimo, TTL massimo e TTL predefinito per il comportamento della cache. Per informazioni sulle singole impostazioni, consulta TTL minimo, TTL massimo e TTL predefinito in the section called “Distribution Settings (Impostazioni distribuzione)”.
- 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 Usa le 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 “Specificate la quantità di tempo di memorizzazione degli oggetti nella cache CloudFront ”.

Puoi anche controllare per quanto tempo gli errori (ad esempio`404 Not Found`) rimangono in una CloudFront cache prima di CloudFront riprovare a recuperare l'oggetto richiesto 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

- Usa le intestazioni per controllare la durata della cache per i singoli oggetti
- Pubblica contenuti non aggiornati (scaduti)
- Specificate la quantità di tempo di memorizzazione degli oggetti nella cache CloudFront
- Aggiungi intestazioni ai tuoi oggetti utilizzando la console Amazon S3

Usa le 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 `Cache-Control max-age` direttiva consente di specificare per quanto tempo (in secondi) un oggetto deve rimanere nella cache prima di CloudFront recuperarlo dal server di origine. Il tempo di scadenza minimo CloudFront supportato è 0 secondi. Il valore massimo è 100 anni. Specifica il valore nel seguente formato:

  ```
  Cache-Control: max-age=secondi
  ```

  Ad esempio, la seguente direttiva indica CloudFront di mantenere l'oggetto associato nella cache per 3600 secondi (un'ora):

  ```
  Cache-Control: max-age=3600
  ```

Se desideri che gli oggetti rimangano nelle cache CloudFront edge per una durata diversa da quella che rimangono nelle cache del browser, puoi usare le direttive `Cache-Control max-age` and `Cache-Control s-maxage` insieme. Per ulteriori informazioni, consulta Specificate la quantità di tempo di memorizzazione degli oggetti nella cache CloudFront .

- 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
  ```

È consigliabile utilizzare la direttiva `Cache-Control max-age` invece del campo dell'intestazione `Expires` per controllare la memorizzazione nella cache dell'oggetto. Se specificate valori sia per che per `Cache-Control max-age``Expires`, CloudFront utilizza solo il valore di. `Cache-Control max-age`

Per ulteriori informazioni, consulta Specificate la quantità di tempo di memorizzazione degli oggetti nella cache CloudFront .

Non è possibile utilizzare i campi HTTP `Cache-Control` o di `Pragma` intestazione in una `GET` richiesta di un visualizzatore CloudFront per forzare il ritorno al server di origine dell'oggetto. CloudFront ignora quei 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

Pubblica contenuti non aggiornati (scaduti)

CloudFront supporta le direttive di controllo `Stale-While-Revalidate` e `Stale-If-Error` cache.

- La `stale-while-revalidate` direttiva consente di CloudFront fornire contenuti obsoleti dalla cache mentre recupera in modo asincrono una nuova versione dall'origine. Ciò migliora la latenza in quanto gli utenti ricevono le risposte immediatamente dalle CloudFront edge location senza

dover attendere il recupero in background e vengono caricati nuovi contenuti in background per le richieste future.

Nell'esempio seguente, CloudFront memorizza la risposta nella cache per un'ora (). `max-age=3600` Se viene effettuata una richiesta dopo questo periodo, CloudFront serve il contenuto non aggiornato inviando contemporaneamente una richiesta all'origine per riconvalidare e aggiornare il contenuto memorizzato nella cache. I contenuti non aggiornati vengono forniti per un massimo di 10 minuti (`stale-while-revalidate=600`) mentre i contenuti vengono riconvalidati.

```
Cache-Control: max-age=3600, stale-while-revalidate=600
```

- La `stale-if-error` direttiva consente di CloudFront 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.

  Nell'esempio seguente, CloudFront memorizza nella cache la risposta per un'ora (). `max-age=3600` Se l'origine non è attiva o restituisce un errore dopo questo periodo, CloudFront continua a fornire il contenuto non aggiornato per un massimo di 24 ore ()`stale-if-error=86400`.

  ```
  Cache-Control: max-age=3600, stale-if-error=86400
  ```

  > **Note**
  >
  > Quando sono configurate `stale-if-error` sia le risposte di errore personalizzate che quelle personalizzate, tenta CloudFront innanzitutto di fornire il contenuto non aggiornato se si verifica un errore entro la durata specificata`stale-if-error`. Se il contenuto obsoleto non è disponibile o ha una `stale-if-error` durata superiore alla scadenza, CloudFront fornisce le risposte di errore personalizzate configurate per il codice di stato dell'errore corrispondente.

Usali entrambi insieme

`stale-while-revalidate` e `stale-if-error` sono 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.

Nell'esempio seguente, CloudFront memorizza nella cache la risposta per un'ora (`max-age=3600`). Se viene effettuata una richiesta dopo questo periodo, CloudFront serve il contenuto non aggiornato per un massimo di 10 minuti (`stale-while-revalidate=600`) mentre il contenuto viene riconvalidato. Se il server di origine restituisce un errore mentre CloudFront tenta di riconvalidare il contenuto, CloudFront continua a fornire il contenuto non aggiornato per un massimo di 24 ore (). `stale-if-error=86400`

```
Cache-Control: max-age=3600, stale-while-revalidate=600, stale-if-error=86400
```

Tip

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.

Specificate la quantità di tempo di memorizzazione degli oggetti nella cache CloudFront

Per controllare il periodo di tempo che CloudFront mantiene un oggetto nella cache prima di inviare un'altra richiesta all'origine, puoi:

- Imposta i valori TTL minimo, massimo e predefinito nel comportamento della cache di una CloudFront distribuzione. 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 aiutano anche a determinare per quanto tempo un browser conserva 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	CloudFront memorizzazione nella cache CloudFront memorizza nella cache l'oggetto con il valore minore tra il valore della `Cache-Control: max-age` direttiva o il valore del CloudFront TTL massimo. Caching del browser I browser memorizzano nella cache l'oggetto per il valore della direttiva `Cache-Control: max-age` .	CloudFront memorizzazione nella cache CloudFront la memorizzazione nella cache dipende dai valori del TTL CloudFront minimo e del TTL massimo e dalla direttiva: `Cache-Control max-age` • Se TTL minimo < `max-age` < TTL massimo, memorizza nella CloudFront cache l'oggetto per il valore della direttiva. `Cache-Control: max-age` • Se `max-age` < TTL minimo, memorizza nella CloudFront cache l'oggetto per il valore del TTL minimo. CloudFront • Se `max-age` > TTL massimo, memorizza l'oggetto nella CloudFront

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
		cache 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	CloudFront memorizzazione nella cache CloudFront memorizza nella cache l'oggetto per il valore del TTL CloudFront predefinito. Caching del browser Dipende dal browser.	CloudFront memorizzazione nella cache CloudFront memorizza l'oggetto nella cache per il valore maggiore tra il TTL CloudFront minimo o il TTL predefinito. 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	CloudFront memorizzazione nella cache CloudFront memorizza nella cache l'oggetto con il valore minore tra il valore della `Cache-Control: s-maxage` direttiva o il valore del CloudFront TTL massimo. Caching del browser I browser memorizzano nella cache l'oggetto per il valore della direttiva `Cache-Control max-age` .	CloudFront memorizzazione nella cache CloudFront la memorizzazione nella cache dipende dai valori del TTL CloudFront minimo e del TTL massimo e dalla direttiva: `Cache-Control: s-maxage` • Se TTL minimo < `s-maxage` < TTL massimo, memorizza nella CloudFront cache l'oggetto per il valore della direttiva. `Cache-Control: s-maxage` • Se `s-maxage` < TTL minimo, memorizza nella CloudFront cache l'oggetto per il valore del TTL minimo. CloudFront • Se `s-maxage` > TTL massimo, memorizza l'oggetto nella CloudFront cache 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	CloudFront memorizzazione nella cache CloudFront memorizza l'oggetto nella cache fino alla data indicata nell'`Expires`intestazione o per il valore del TTL CloudFront massimo, a seconda di quale dei due eventi si verifichi per primo. Caching del browser I browser memorizzano nella cache l'oggetto fino alla data presente nell'intestazione `Expires`.	CloudFront memorizzazione nella cache CloudFront la memorizzazione nella cache dipende dai valori del TTL CloudFront minimo e del TTL massimo e dall'intestazione: `Expires` • Se TTL minimo < `Expires` < TTL massimo, memorizza l'oggetto nella CloudFront cache fino alla data e all'ora indicate nell'intestazione. `Expires` • Se `Expires` < TTL minimo, memorizza l'oggetto nella CloudFront cache per il valore del TTL minimo. CloudFront • Se `Expires` > TTL massimo, memorizza l'oggetto nella CloudFront cache per il valore del TTL massimo. CloudFront Caching del browser I browser memorizzano nella cache l'oggetto fino alla data

Intestazioni di origine	TTL minimo = 0	TTL minimo = 0
		e all'ora presenti nell'inte stazione `Expires`.
L'origine aggiunge le direttive **`Cache-Control: no-cache`**, **`no-store`** e/o **`private`** all'oggetto	CloudFront e i browser rispettano le intestazioni.	CloudFront memorizzazione nella cache CloudFront memorizza nella cache l'oggetto per il valore del TTL CloudFront minimo. 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 di cache, anche se le `private` direttive `Cache-Control: no-cacheno-store`, e/o 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 che ha 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 CloudFront venga restituito un errore in risposta alle richieste future se l'origine non è raggiungibile, anziché restituire l'oggetto ottenuto dall'origine in precedenza.

Per informazioni su come modificare le impostazioni per le distribuzioni utilizzando la CloudFront console, vedere. Aggiornamento di una distribuzione Per informazioni su come modificare le impostazioni per le distribuzioni utilizzando l' CloudFront API, consulta. UpdateDistribution

Aggiungi intestazioni ai tuoi oggetti utilizzando la console Amazon S3

Per aggiungere un campo di intestazione **`Cache-Control`** o **`Expires`** agli oggetti Amazon S3 utilizzando la console Amazon S3

1. Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Nell'elenco dei bucket, scegli il nome del bucket che contiene i file a cui stai aggiungendo le intestazioni.
3. Seleziona la casella di controllo accanto al nome del file o della cartella a cui stai aggiungendo le intestazioni. Quando aggiungi intestazioni a una cartella, ciò influisce su tutti i file all'interno di quella cartella.
4. Seleziona Actions (Operazioni), quindi Edit metadata (Modifica metadati).
5. Nel pannello Add metadata (Aggiungi metadati), effettua le seguenti operazioni:
   a. Seleziona Add metadata (Aggiungi metadati).
   b. In Type (Tipo), seleziona System defined (Definito dal sistema).
   c. Per Key (Chiave), scegli il nome dell'intestazione che stai aggiungendo (Cache-Control o Expires (Scadenze)).
   d. 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`.
6. Nella parte inferiore della pagina, scegli Edit metadata (Modifica metadati).

Contenuto della cache in base ai parametri della stringa 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, è possibile scegliere se CloudFront inoltrare le stringhe di query all'origine e se memorizzare nella cache i contenuti in base a tutti i parametri o a 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 CloudFront includono un parametro della stringa di query linguistica basato sulla lingua scelta dall'utente. È possibile CloudFront configurare l'inoltro delle stringhe di query all'origine e la memorizzazione nella cache in base al parametro della lingua. Se configurate il server Web per restituire la versione di una determinata pagina che corrisponde alla lingua selezionata, CloudFront memorizza nella cache ogni versione linguistica separatamente, in base al valore del parametro della stringa di query della lingua.

In questo esempio, se la pagina principale del sito Web è`main.html`, le seguenti cinque richieste vengono memorizzate nella cache `main.html` cinque volte, una volta per ogni valore del parametro della stringa di query della lingua: CloudFront

- `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 configurate per CloudFront inoltrare i parametri della stringa di query all'origine, vengono CloudFront comunque memorizzate nella cache in base ai valori dei parametri, anche se l'origine restituisce versioni identiche dell'oggetto CloudFront per ogni valore del parametro.
- Affinché i parametri di stringa 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 si utilizza un delimitatore diverso, è possibile ottenere risultati imprevisti, a seconda dei parametri specificati CloudFront da utilizzare come base per la memorizzazione nella cache e dell'ordine in cui i parametri vengono visualizzati nella stringa di query.

  Gli esempi seguenti mostrano cosa succede se si utilizza un delimitatore diverso e si configura la memorizzazione nella cache solo in base CloudFront al parametro: `color`

- *Nella richiesta seguente, CloudFront memorizza nella cache i contenuti in base al valore del color parametro, ma CloudFront interpreta il valore come rosso; size=large:*

  `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red;size=large`

- Nella richiesta seguente, CloudFront memorizza nella cache il contenuto ma non basa la memorizzazione nella cache sui parametri della stringa di query. Questo perché hai configurato la cache in base CloudFront al `color` parametro, ma CloudFront interpreta la seguente stringa come contenente solo un `size` parametro il cui valore è *`large`*; color=red:

  `https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large;color=red`

È possibile configurare in modo CloudFront da eseguire una delle seguenti operazioni:

- Non inoltrare le stringhe di query al server di origine. Se non inoltrate stringhe di query, CloudFront non viene memorizzata nella cache in base ai parametri delle stringhe 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 “Ottimizza la memorizzazione nella cache”.

Argomenti

Impostazioni della console e delle API per l'inoltro delle stringa di query e per la memorizzazione nella cache

Per configurare l'inoltro e la memorizzazione nella cache delle stringhe di query nella CloudFront console, consulta le seguenti impostazioni in: the section called “Distribution Settings (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' CloudFront API, consulta le seguenti impostazioni in DistributionConfige in Amazon CloudFront API DistributionConfigWithTagsReference:

- `QueryString`
- `QueryStringCacheKeys`

Ottimizza la memorizzazione nella cache

Quando configuri la cache in base CloudFront ai parametri della stringa di query, puoi eseguire le seguenti operazioni per ridurre il numero di richieste inoltrate CloudFront all'origine. Quando le CloudFront edge location servono oggetti, riduci il carico sul server di origine e riduci la latenza perché gli oggetti vengono serviti 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 a cui l'applicazione Web inoltra CloudFront, CloudFront inoltra le richieste all'origine per ogni valore di parametro e memorizza nella cache una versione separata dell'oggetto per ogni valore del 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 la cache solo in base CloudFront ai parametri della stringa di query per i quali l'origine restituisce versioni diverse e di considerare attentamente i vantaggi della memorizzazione nella cache 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, è CloudFront necessario configurarla solo in base al parametro color e non al parametro size. Ciò aumenta la probabilità che sia CloudFront possibile soddisfare una richiesta dalla cache, migliorando le prestazioni e riducendo 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. Ciò comporta CloudFront l'inoltro di due richieste separate per image.jpg all'origine e la memorizzazione nella cache di due versioni separate 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 caso dei nomi e dei valori dei parametri durante la memorizzazione nella cache 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. Ciò comporta CloudFront l'inoltro di quattro richieste separate per image.jpg all'origine e la memorizzazione nella cache di quattro versioni separate 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 utilizzi URL firmati per limitare l'accesso ai tuoi contenuti (se hai aggiunto firmatari attendibili alla tua distribuzione), CloudFront rimuove i seguenti parametri della stringa di query prima di inoltrare il resto dell'URL all'origine:

- `Expires`
- `Key-Pair-Id`
- `Policy`
- `Signature`

Se utilizzi URL firmati e desideri configurare l'inoltro delle stringhe di query CloudFront all'origine, non puoi denominare i parametri della stringa di query personalizzati,, o. `Expires` `Key-Pair-Id` `Policy` `Signature`

Parametri delle stringhe di query e log CloudFront standard (log di accesso)

Se abiliti la registrazione, CloudFront registra l'URL completo, inclusi i parametri della stringa di query. Ciò è vero indipendentemente dal fatto che tu sia stato configurato CloudFront per inoltrare le stringhe di query all'origine. Per ulteriori informazioni sulla CloudFront registrazione, vedere. the section called “Utilizzo dei registri standard (log di accesso)”

Contenuto della cache basato sui cookie

Per impostazione predefinita, CloudFront non considera i cookie durante l'elaborazione di richieste e risposte o durante la memorizzazione nella cache degli oggetti in posizioni periferiche. Se CloudFront riceve due richieste identiche ad eccezione di ciò che si trova nell'`Cookie`intestazione, per impostazione predefinita CloudFront considera le richieste identiche e restituisce lo stesso oggetto per entrambe le richieste.

Puoi configurare l'inoltro CloudFront all'origine di alcuni o tutti i cookie nelle richieste dei visualizzatori e di memorizzare nella cache versioni separate degli oggetti in base ai valori dei cookie inoltrati. In tal caso, CloudFront utilizza alcuni o tutti i cookie nelle richieste dei visualizzatori, a prescindere da quelle configurate 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 configurate CloudFront per memorizzare nella cache gli oggetti in base al valore del `country` cookie, CloudFront inoltra le richieste all'origine e include il cookie e `locations.html` il suo valore. `country` La tua origine restituisce `locations.html` e CloudFront memorizza l'oggetto nella cache una volta per le richieste in cui si trova il valore del `country` cookie `uk` e una volta per le richieste in cui è presente il valore. `fr`

> **Important**
>
> Amazon S3 e alcuni server HTTP non elaborano i cookie. Non configurate CloudFront per inoltrare i cookie a un'origine che non elabora i cookie o che non varia la risposta in base ai cookie. Ciò può causare CloudFront l'inoltro di più richieste all'origine per lo stesso oggetto, con conseguente rallentamento delle prestazioni e aumento del carico sull'origine. Se, considerando l'esempio precedente, la tua origine non elabora il `country` cookie o restituisce sempre la stessa versione di `locations.html` to CloudFront indipendentemente dal valore del `country` cookie, non configurate l'inoltro CloudFront di quel cookie.
> Al contrario, se la tua origine personalizzata dipende da un particolare cookie o invia risposte diverse in base a un cookie, assicurati di configurare CloudFront l'inoltro di quel cookie all'origine. Altrimenti, 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:

- Inoltra tutti i cookie all'origine: CloudFront include tutti i cookie inviati dal visualizzatore quando inoltra le richieste all'origine. Quando la tua origine restituisce una risposta, CloudFront memorizza la risposta nella cache utilizzando i nomi e i valori dei cookie nella richiesta del visualizzatore. Se la risposta di origine include `Set-Cookie` intestazioni, le CloudFront restituisce al visualizzatore con l'oggetto richiesto. CloudFront memorizza inoltre nella cache le `Set-Cookie` intestazioni con l'oggetto restituito dall'origine e invia tali `Set-Cookie` intestazioni ai visualizzatori su tutti gli accessi alla cache.
- Inoltra un set di cookie specificato: CloudFront rimuove tutti i cookie inviati dal visualizzatore che non sono nell'elenco consentito prima di inoltrare una richiesta all'origine. CloudFront memorizza nella cache la risposta utilizzando i nomi e i valori dei cookie elencati nella richiesta del visualizzatore. Se la risposta di origine include `Set-Cookie` intestazioni, le CloudFront restituisce al visualizzatore con l'oggetto richiesto. CloudFront memorizza inoltre nella cache le `Set-Cookie` intestazioni con l'oggetto restituito dall'origine e invia tali `Set-Cookie` intestazioni ai visualizzatori su tutti gli accessi alla 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).

- Non inoltrate i cookie all'origine: CloudFront non memorizza nella cache gli oggetti in base al cookie inviato dal visualizzatore. Inoltre, CloudFront rimuove i cookie prima di inoltrare le richieste all'origine e rimuove le `Set-Cookie` intestazioni dalle risposte prima di restituire le risposte agli utenti. Poiché questo non è il modo ottimale per utilizzare le risorse di origine, quando selezioni questo comportamento di cache, dovresti assicurarti 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 tutti gli attributi dei cookie, anche se configuri di CloudFront non inoltrare i cookie all'origine o se configuri di CloudFront inoltrare solo cookie specifici. Per ulteriori informazioni sulla CloudFront registrazione, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 di visualizzazione per lo stesso oggetto contengono cookie identici tranne che per i casi specifici, CloudFront memorizza l'oggetto due volte nella cache.

CloudFront ordina i cookie

Se CloudFront è configurato per inoltrare i cookie (tutti o un sottoinsieme), CloudFront ordina i cookie in ordine naturale in base al nome del cookie prima di inoltrare la richiesta all'origine.

`If-Modified-Since` e `If-None-Match`

`If-Modified-Sincee` le richieste `If-None-Match` condizionali 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 di cookie solo se il valore è conforme al formato standard della 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 (che si tratti di tutti i cookie o di cookie specifici), memorizza anche nella cache le intestazioni ricevute nella risposta all'`Set-Cookie`origine. CloudFront include queste `Set-Cookie` intestazioni nella risposta al visualizzatore originale e le include anche nelle risposte successive che vengono fornite dalla cache. CloudFront

Se desideri ricevere i cookie all'origine ma non vuoi CloudFront memorizzare nella cache le `Set-Cookie` intestazioni nelle risposte dell'origine, configura la tua origine per aggiungere un'`Cache-Control`intestazione con una `no-cache` direttiva che specifichi `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 CloudFront configuri l'inoltro di cookie specifici all'origine, il numero totale di byte in tutti i nomi di cookie che configuri CloudFront per l'inoltro non può superare i 512 meno il numero di cookie che stai inoltrando. Ad esempio, se configuri di CloudFront inoltrare 10 cookie all'origine, la lunghezza combinata dei nomi dei 10 cookie non può superare i 502 byte (512-10).

Se configuri CloudFront per inoltrare tutti i cookie all'origine, la lunghezza dei nomi dei cookie non ha importanza.

Per informazioni sull'utilizzo della CloudFront console per aggiornare una distribuzione in modo da CloudFront inoltrare i cookie all'origine, consultaAggiornamento di una distribuzione. Per informazioni sull'utilizzo dell' CloudFront API per aggiornare una distribuzione, UpdateDistributionconsulta Amazon CloudFront API Reference.

Contenuto della cache in base alle intestazioni delle richieste

CloudFront consente di scegliere se CloudFront inoltrare le intestazioni all'origine e memorizzare nella cache versioni separate di un oggetto specificato in base ai valori di intestazione nelle 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

Intestazioni e distribuzioni – Panoramica

Per impostazione predefinita, CloudFront non considera le intestazioni quando memorizza nella cache gli oggetti in posizioni periferiche. Se la tua origine restituisce due oggetti che differiscono solo per i valori nelle intestazioni della richiesta, CloudFront memorizza nella cache solo una versione dell'oggetto.

È possibile configurare CloudFront l'inoltro delle intestazioni all'origine, il che comporta CloudFront la memorizzazione nella cache di più versioni di un oggetto in base ai valori di una o più intestazioni di richiesta. CloudFront Per configurare la memorizzazione nella cache degli oggetti in base ai valori di intestazioni specifiche, specificate le impostazioni di comportamento della cache per la 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 CloudFront configurate la memorizzazione nella cache degli oggetti in base al valore dell'`Product`intestazione, CloudFront inoltra le richieste all'origine e include i `logo.jpg` valori dell'intestazione e

dell'`Product`intestazione. CloudFront memorizza nella cache `logo.jpg` una volta per le richieste in cui si trova il valore dell'`Product`intestazione `Acme` e una volta per le richieste in cui si trova il valore. `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 le impostazioni della cache legacy: se si configura CloudFront l'inoltro di tutte le intestazioni all'origine, CloudFront non memorizza nella cache gli oggetti associati a questo comportamento della cache. ma invia ogni richiesta all'origine.

- Inoltra un elenco di intestazioni che hai specificato. CloudFront memorizza nella cache gli oggetti in base ai valori di tutte le intestazioni specificate. CloudFront inoltra anche le intestazioni che inoltra per impostazione predefinita, ma memorizza nella cache gli oggetti solo in base alle intestazioni specificate.
- Inoltra solo le intestazioni predefinite. In questa configurazione, CloudFront non memorizza nella cache gli oggetti in base ai valori nelle intestazioni della richiesta.

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 informazioni sull'utilizzo della CloudFront console per aggiornare una distribuzione in modo da CloudFront inoltrare le intestazioni all'origine, consulta. Aggiornamento di una distribuzione Per informazioni sull'utilizzo dell' CloudFront API per aggiornare una distribuzione esistente, consulta Update Distribution in Amazon CloudFront API Reference.

Seleziona le intestazioni su cui basare la memorizzazione nella cache

Le intestazioni che puoi inoltrare all'origine e su cui si CloudFront basa la memorizzazione nella cache dipendono dal fatto che l'origine sia un bucket Amazon S3 o un'origine personalizzata.

- Amazon S3: puoi configurare CloudFront l'inoltro e la memorizzazione nella cache degli oggetti in base a una serie di intestazioni specifiche (consulta 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 CORS, è necessario inoltrare le intestazioni che consentono CloudFront di distribuire contenuti per siti Web abilitati per la condivisione di risorse tra le origini (CORS). Per ulteriori informazioni, consulta Configurare CloudFront per rispettare le impostazioni CORS.
- Per personalizzare i contenuti utilizzando le intestazioni da inoltrare all'origine Amazon S3, è necessario scrivere e aggiungere funzioni Lambda @Edge e associarle alla distribuzione in modo che vengano attivate da un CloudFront evento rivolto all'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, non è CloudFront possibile gestire tante richieste provenienti dalle cache edge quanto una percentuale di tutte le richieste.

- Origine personalizzata: puoi configurare la memorizzazione nella cache in base CloudFront al valore di qualsiasi intestazione di richiesta tranne quanto segue:
  - `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 Contenuto della cache basato sui cookie.
  - `Host (for Amazon S3 origins)`
  - `Proxy-Authorization`
  - `TE`
  - `Upgrade`

  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 numerosi valori possibili e la memorizzazione nella cache in base ai loro valori potrebbe causare CloudFront l'inoltro di un numero significativamente maggiore di richieste all'origine.

Per un elenco completo delle intestazioni delle richieste HTTP e di come le CloudFront elabora, consulta. Intestazioni e CloudFront comportamento delle richieste HTTP (origini personalizzate e Amazon S3)

Configurare 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`.
  - Configura CloudFront per inoltrare le seguenti intestazioni: `OriginAccess-Control-Request-Headers`, e. `Access-Control-Request-Method`
- Se non desideri che `OPTIONS` le risposte vengano memorizzate nella cache, configura l'inoltro dell'`Origin`intestazione, insieme CloudFront a qualsiasi altra intestazione richiesta dall'origine (ad esempio, `Access-Control-Request-HeadersAccess-Control-Request-Method`, o altre).

Server di origine personalizzati – Inoltra l'intestazione `Origin` insieme a qualsiasi altra intestazione richiesta dal server di origine.

CloudFront Per configurare la memorizzazione nella cache delle risposte basate su CORS, è necessario configurare CloudFront l'inoltro delle intestazioni utilizzando una politica di cache. Per ulteriori informazioni, consulta Controlla la 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.

Configura la memorizzazione nella cache in base al tipo di dispositivo

Se desideri CloudFront memorizzare nella cache diverse versioni dei tuoi oggetti in base al dispositivo utilizzato dall'utente per visualizzare i contenuti, configura CloudFront l'inoltro delle intestazioni applicabili 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 dell'inoltro della richiesta all'origine. Se il dispositivo ricade in più di una categoria, allora più di un valore potrebbe essere `true`. Ad esempio, per alcuni tablet, CloudFront potrebbe impostare entrambi e su. `CloudFront-Is-Mobile-Viewer` `CloudFront-Is-Tablet-Viewer` `true`

Configura la memorizzazione nella cache in base alla lingua del visualizzatore

Se desideri CloudFront memorizzare nella cache diverse versioni dei tuoi oggetti in base alla lingua specificata nella richiesta, configura CloudFront l'inoltro dell'`Accept-Language`intestazione all'origine.

Configura la memorizzazione nella cache in base alla posizione del visualizzatore

Se desideri CloudFront memorizzare nella cache diverse versioni dei tuoi oggetti in base al paese da cui proviene la richiesta, configura CloudFront l'inoltro dell'`CloudFront-Viewer-Country`intestazione all'origine. CloudFront converte automaticamente l'indirizzo IP da cui proviene la richiesta in un codice del paese di due lettere. Per un easy-to-use elenco dei codici dei paesi, ordinabili per codice e per nome del paese, consulta la voce di Wikipedia ISO 3166-1 alpha-2.

Configura la memorizzazione nella cache in base al protocollo della richiesta

Se desideri CloudFront memorizzare nella cache diverse versioni dei tuoi oggetti in base al protocollo della richiesta, HTTP o HTTPS, configura CloudFront l'inoltro dell'`CloudFront-Forwarded-Proto`intestazione all'origine.

Configura la memorizzazione nella cache 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 la cache in base CloudFront a una o più intestazioni e le intestazioni hanno più di un valore possibile, CloudFront inoltra più richieste al server di origine per lo stesso oggetto. Questo rallenta le prestazioni e aumenta il carico di lavoro del server di origine. Se il tuo server di origine restituisce lo stesso oggetto indipendentemente dal valore di una determinata intestazione, ti consigliamo di non configurare la cache in base CloudFront a quell'intestazione.

Se configuri CloudFront per inoltrare più di un'intestazione, l'ordine delle intestazioni nelle richieste dei visualizzatori non influisce sulla memorizzazione nella cache, purché i valori siano gli stessi. Ad esempio, se una richiesta contiene le intestazioni A:1, B:2 e un'altra richiesta contiene B:2, A:1, memorizza nella cache solo una copia dell'oggetto. CloudFront

In che modo il formato delle intestazioni e dei valori delle intestazioni si ripercuotono sul caching

Quando viene CloudFront memorizzata nella cache in base ai valori dell'intestazione, non considera le maiuscole e le minuscole del nome dell'intestazione, ma considera le maiuscole e minuscole del valore dell'intestazione:

- Se le richieste del visualizzatore includono entrambi `Product:Acme` e`product:Acme`, CloudFront memorizza un 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 entrambi `Product:Acme` e`Product:acme`, CloudFront memorizza un oggetto nella cache due volte, perché il valore è presente `Acme` in alcune richieste e `acme` in altre.

Intestazioni che vengono CloudFront restituite al visualizzatore

La configurazione CloudFront per l'inoltro e la memorizzazione delle intestazioni nella cache non influisce sulle intestazioni CloudFront restituite al visualizzatore. CloudFront restituisce tutte le intestazioni che ottiene dall'origine con alcune 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.

Controlla la chiave della cache con una policy

Con una politica di CloudFront cache, è possibile specificare le intestazioni HTTP, i cookie e le stringhe di query CloudFront incluse nella chiave della cache per gli oggetti che vengono memorizzati nella cache nelle edge location. CloudFront La chiave cache è l'identificatore univoco per ogni oggetto nella cache e determina se la richiesta HTTP di un visualizzatore genera un accesso alla 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. Quando si verifica un accesso alla cache, l'oggetto viene fornito al visualizzatore da una posizione CloudFront periferica, con 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. In questo modo è possibile ottenere prestazioni migliori dal sito Web o dall'applicazione, poiché il rapporto di accessi alla cache è più elevato (una percentuale maggiore di richieste degli utenti che generano un accesso alla cache). Per ulteriori informazioni, consulta Comprendi la chiave della cache.

Per controllare la chiave della cache, si utilizza una policy relativa alla CloudFront cache. Si allega una politica di cache a uno o più comportamenti della cache in una CloudFront distribuzione.

È inoltre possibile utilizzare la politica della cache per specificare le impostazioni TTL (time to live) per gli oggetti nella CloudFront cache e abilitare CloudFront la richiesta e la memorizzazione nella cache degli oggetti compressi.

Argomenti

- Comprendi le politiche relative alla cache
- Crea politiche di cache
- Usa politiche di cache gestite
- Comprendi la chiave della cache

Comprendi le politiche relative alla cache

Puoi utilizzare una policy sulla cache per migliorare il rapporto di accessi alla cache controllando i valori (stringhe di query URL, intestazioni HTTP e cookie) inclusi nella chiave della cache. CloudFrontfornisce alcune politiche di cache predefinite, note come politiche 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 Usa politiche di 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) interagiscono con le intestazioni `Cache-Control` e `Expires` HTTP (se sono presenti nella risposta di origine) per determinare per quanto tempo gli oggetti nella CloudFront cache restano validi.

Minimum TTL (TTL minimo)

Il periodo di tempo minimo, in secondi, durante il quale gli oggetti devono rimanere nella CloudFront cache prima di CloudFront eseguire controlli con l'origine per verificare se l'oggetto è stato aggiornato. Per ulteriori informazioni, consulta Gestisci la durata della permanenza dei contenuti nella cache (scadenza).

Maximum TTL (TTL massimo)

Il periodo massimo di permanenza, in secondi, degli oggetti nella CloudFront cache prima di CloudFront effettuare controlli con l'origine per verificare se l'oggetto è stato aggiornato.

CloudFront utilizza questa impostazione solo quando l'origine invia `Cache-Control` o inserisce le `Expires` intestazioni con l'oggetto. Per ulteriori informazioni, consulta Gestisci la durata della permanenza dei contenuti nella cache (scadenza).

Default TTL (TTL di default)

Il periodo di tempo predefinito, in secondi, durante il quale desiderate che gli oggetti rimangano nella CloudFront cache prima CloudFront dei controlli con l'origine per verificare se l'oggetto è stato aggiornato. CloudFront utilizza il valore di questa impostazione come TTL dell'oggetto solo quando l'origine non invia *`Cache-Control`* o non contiene `Expires` intestazioni con l'oggetto. Per ulteriori informazioni, consulta Gestisci la durata della permanenza dei contenuti nella cache (scadenza).

> **Note**
>
> Se le impostazioni TTL minimo, TTL massimo e TTL predefinito sono tutte impostate su 0, la memorizzazione nella cache viene disabilitata. CloudFront

Impostazioni chiave cache

Le impostazioni della chiave cache specificano i valori nelle richieste del visualizzatore CloudFront incluse nella chiave della cache. I valori possono includere stringhe di query URL, intestazioni HTTP e cookie. I valori che includi nella chiave della cache vengono inclusi automaticamente nelle richieste CloudFront inviate all'origine, note come richieste di origine. Per informazioni sul controllo delle richieste di origine senza influire sulla chiave della cache, consulta Controlla le 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 dei visualizzatori CloudFront incluse nella chiave della 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, incluso il relativo valore, nella chiave della cache e nelle richieste di origine.

È inoltre possibile includere alcune intestazioni generate da CloudFront nella chiave della cache. Per ulteriori informazioni, consulta the section called “Aggiungi intestazioni CloudFront di richiesta”.

Cookie

I cookie nelle richieste dei visualizzatori CloudFront incluse nella chiave della 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, incluso il suo valore, nella chiave della cache e nelle richieste di origine.

Stringhe di query

Le stringhe di query URL nelle richieste dei visualizzatori CloudFront incluse nella chiave della 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 relativo valore, nella chiave della cache e nelle richieste di origine.

Supporto della compressione

Queste impostazioni consentono CloudFront di richiedere e memorizzare nella cache gli oggetti compressi nei formati di compressione Gzip o Brotli, quando il visualizzatore li supporta. Queste impostazioni consentono CloudFront inoltre il funzionamento della compressione. 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, usa l'impostazione abilitata **`EnableAcceptEncodingGzip`** per Gzip (impostata su `true` nell' CloudFront API, negli AWS SDK o AWS CloudFormation). AWS CLI
- 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, usa l'impostazione Brotli enabled (impostata `EnableAcceptEncodingBrotli` su nell' CloudFront API, `true` negli AWS SDK o). AWS CLI AWS CloudFormation
- Il comportamento della cache a cui è associata questa politica sulla cache è configurato con la compressione. CloudFront In questo caso, è possibile abilitare la memorizzazione nella cache per Gzip o Brotli, o entrambi. Quando CloudFront la compressione è abilitata, l'attivazione della memorizzazione nella cache per entrambi i formati può aiutare a ridurre i costi per il trasferimento dei dati su Internet.

> **Note**
>
> Se abiliti la memorizzazione nella cache per uno o entrambi questi formati di compressione, non includere l'`Accept-Encoding`intestazione in una policy di richiesta

di origine associata allo stesso comportamento della cache. CloudFrontinclude sempre questa intestazione nelle richieste di origine quando la memorizzazione nella cache è abilitata per uno di questi formati, quindi 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 CloudFront compressione, 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 spiegato 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'`Accept-Encoding`intestazione, 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, ovvero se `br` i valori `gzip` and sono entrambi presenti nell'`Accept-Encoding`intestazione della richiesta del visualizzatore, effettua le seguenti operazioni: CloudFront

- 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 edge location non ha un oggetto compresso Brotli o Gzip nella cache che corrisponda alla richiesta e non sia scaduto, CloudFront include l'header () normalizzato nella richiesta di origine corrispondente. `Accept-Encoding: br,gzip` 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'`Accept-Encoding`intestazione della richiesta del visualizzatore ma non lo è, esegue le seguenti operazioni: `br` CloudFront

- 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 edge location non ha un oggetto compresso Gzip nella cache che corrisponda alla richiesta e non sia scaduto, CloudFront include l'header normalizzato () nella richiesta di origine corrispondente. `Accept-Encoding: gzip` La richiesta di origine non include altri valori presenti nell'intestazione `Accept-Encoding` inviata dal visualizzatore.

Per capire cosa succede CloudFront se il visualizzatore supporta Brotli ma non Gzip, sostituite i due formati di compressione tra loro nell'esempio precedente.

Se il visualizzatore non supporta Brotli o Gzip, ovvero l'`Accept-Encoding`intestazione nella richiesta del visualizzatore non contiene o ha valori: `br gzip` 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 cui 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 della richiesta del visualizzatore), esegue le seguenti operazioni: `Accept-Encoding` CloudFront

- 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 edge location non ha un oggetto compresso Gzip nella cache che corrisponde alla richiesta e non è scaduto, CloudFront include l'header normalizzato (`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 CloudFront succede se la memorizzazione nella cache degli oggetti compressi è abilitata per Brotli ma non per Gzip, sostituite i due formati di compressione tra loro nell'esempio precedente.

Se il visualizzatore non supporta il formato di compressione per il quale è abilitata la memorizzazione nella cache (l'`Accept-Encoding`intestazione 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 come qualsiasi altra `Accept-Encoding` 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.

Crea politiche di 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. Puoi creare una policy di cache nella CloudFront console, con AWS Command Line Interface (AWS CLI) o con l' CloudFront API.

Dopo aver creato una politica di cache, la si collega a uno o più comportamenti della cache in una CloudFront distribuzione.

Console

Per creare una policy della cache (console)

1. Accedi AWS Management Console e apri la pagina Policies nella CloudFront console 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 Comprendi le politiche relative alla 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 CloudFront console all'indirizzohttps://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. Apri la CloudFront console all'indirizzohttps://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 alle impostazioni di distribuzione.
6. Al termine, scegliere Crea distribuzione.

CLI

Per creare una politica di cache con AWS Command Line Interface (AWS CLI), usa il aws cloudfront create-cache-policy 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 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 Comprendi le politiche relative alla 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 politica della cache e ne hai bisogno per allegare la politica della cache al comportamento della cache di una CloudFront distribuzione.

Per collegare una policy della cache a una distribuzione esistente (CLI con file di input)

1. Utilizzate il comando seguente per salvare la configurazione di CloudFront distribuzione per la distribuzione che desiderate 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 alle 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 politica di cache con l' CloudFront API, usa CreateCachePolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta Comprendi le politiche relative alla cache la documentazione di riferimento sull'API per il tuo AWS SDK 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 di cache in una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a un comportamento di cache in una nuova distribuzione, usa 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 alle impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Usa politiche di cache gestite

CloudFront fornisce una serie di politiche di cache gestite che puoi collegare a qualsiasi comportamento della cache della tua 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. Puoi allegare 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 Crea politiche di cache.

Negli argomenti seguenti vengono descritte le policy della cache gestite che è possibile utilizzare.

Argomenti

Amplify

Visualizza questa politica nella console CloudFront

Questa policy è progettata per l'utilizzo con un'origine che è una Web App AWS Amplify.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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.

CachingDisabled

Visualizza questa politica nella CloudFront console

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 AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

Questa politica è progettata per ottimizzare l'efficienza della cache riducendo al minimo i valori CloudFront inclusi nella chiave della cache. CloudFront non include stringhe di query o cookie nella chiave cache e include solo l'intestazione normalizzata`Accept-Encoding`. Ciò consente di CloudFront memorizzare separatamente gli oggetti nei formati di compressione Gzip e Brotli quando l'origine li restituisce o quando è abilitata la compressione dei bordi. CloudFront

Quando si utilizza AWS CloudFormation, o l' CloudFront API AWS CLI, l'ID per 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.

CachingOptimizedForUncompressedObjects

Visualizza questa politica nella CloudFront console

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 AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Elementare- MediaPackage

Visualizza questa politica nella console CloudFront

Questo criterio è progettato per l'utilizzo con un'origine che è un endpoint AWS Elemental MediaPackage .

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

Questa policy è progettata per essere utilizzata con un'origine che restituisce intestazioni di risposta `Cache-Control` HTTP e non fornisce contenuti diversi in base ai valori presenti nella stringa di query. Se la tua origine offre contenuti diversi in base ai valori presenti nella stringa di query, valuta la possibilità di utilizzareUseOriginCacheControlHeaders-QueryStrings.

Quando utilizzi AWS CloudFormation AWS CLI, l'o l' CloudFront API, l'ID per 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 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

Visualizza questa politica nella CloudFront console

Questa politica è progettata per essere utilizzata con un'origine che restituisce intestazioni di risposta `Cache-Control` HTTP e fornisce contenuti diversi in base ai valori presenti nella stringa di query. Se la tua origine non offre contenuti diversi in base ai valori presenti nella stringa di query, valuta la possibilità di utilizzareUseOriginCacheControlHeaders.

Quando si utilizza AWS CloudFormation AWS CLI, l'o l' CloudFront API, l'ID per 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 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.

Comprendi la chiave della cache

La chiave della cache determina se una richiesta del visualizzatore a una CloudFront edge location provoca un accesso alla 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 caso di accesso alla cache, l'oggetto richiesto viene fornito al visualizzatore da una CloudFront edge location, con 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. (È anche possibile modificare la chiave della cache utilizzando una funzione Lambda @Edge.) 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 cache predefinita

Per impostazione predefinita, la chiave cache per una CloudFront distribuzione include le seguenti informazioni:

- Il nome di dominio della CloudFront distribuzione (ad esempio, d111111abcdef8.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 di visualizzazione come questo esempio arriva a una posizione CloudFront periferica, CloudFront utilizza la chiave cache per determinare se c'è un problema 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 presente nella cache (errore nella cache), CloudFront invia una richiesta all'origine per ottenere l'oggetto. Dopo aver ottenuto l'oggetto, lo CloudFront restituisce al visualizzatore e lo memorizza nella cache dell'edge location.

Quando CloudFront riceve un'altra richiesta per lo stesso oggetto, come determinato dalla chiave della cache, invia CloudFront 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.

Personalizza la 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. In tal caso, CloudFront utilizza questa intestazione per determinare gli accessi alla cache e include l'intestazione nelle richieste di origine (richieste che vengono CloudFront inviate all'origine in caso di perdita della cache).

Una potenziale conseguenza dell'inclusione di valori aggiuntivi nella chiave della cache è che CloudFront potrebbe finire per memorizzare nella cache oggetti duplicati a causa della variazione che può verificarsi nelle richieste dei visualizzatori. 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 causare CloudFront la memorizzazione nella 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.

Controlla le richieste di origine con una policy

Quando una richiesta di un CloudFront visualizzatore causa una perdita nella cache (l'oggetto richiesto non viene memorizzato nella cache dell'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 includono CloudFront automaticamente in ogni richiesta di origine, tra cui`Host`, e `User-Agent` `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 per impostazione predefinita inoltra le intestazioni all'origine.) 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, puoi ricevere informazioni aggiuntive all'origine e anche mantenere un buon rapporto di accessi alla cache (la percentuale di richieste degli utenti che generano un accesso alla 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 di cache, si collega una policy di richiesta di origine a uno o più comportamenti della cache in una CloudFront distribuzione.

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 CloudFront prima di inviare la richiesta di origine, con valori

di intestazione determinati automaticamente in base alla richiesta del visualizzatore. Per ulteriori informazioni, consulta the section called “Aggiungi intestazioni CloudFront di richiesta”.

Argomenti

Comprendi le politiche relative alle richieste di origine

CloudFront fornisce alcune politiche di richiesta di origine predefinite, note come politiche gestite, per casi d'uso 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 Usa politiche di richiesta di 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 delle richieste di origine specificano i valori nelle richieste dei visualizzatori incluse nelle richieste CloudFront inviate 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 Controlla la chiave della cache con una policy.

Headers

Le intestazioni HTTP nelle richieste dei visualizzatori CloudFront incluse 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 CloudFront intestazioni: tutte le intestazioni HTTP nelle richieste dei visualizzatori sono incluse nelle richieste di origine. Inoltre, specifichi quali CloudFront intestazioni desideri aggiungere alle richieste di origine. Per ulteriori informazioni sulle CloudFront intestazioni, consulta. the section called “Aggiungi intestazioni CloudFront di richiesta”
- 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 Configura CloudFront per aggiungere intestazioni personalizzate alle richieste di 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 utilizzano le intestazioni Tutti i visualizzatori e le seguenti intestazioni, Include le seguenti CloudFront intestazioni o Tutte le intestazioni dei visualizzatori tranne l'impostazione, si specificano le intestazioni HTTP solo in base al nome dell'intestazione. CloudFront include l'intestazione completa, incluso il relativo valore, nelle richieste di origine.

> **Note**
>
> Quando utilizzi l'impostazione All viewer **`Host`** header tranne l'impostazione per rimuovere l'intestazione del visualizzatore, CloudFront aggiunge una nuova `Host` intestazione con il nome di dominio dell'origine alla richiesta di origine.

Cookie

I cookie nelle richieste dei visualizzatori, CloudFront incluse le 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 Includi i seguenti cookie o Tutti i cookie tranne l'impostazione, si specificano i cookie solo in base al loro nome. CloudFront include il cookie completo, incluso il relativo valore, nelle richieste di origine.

Stringhe di query

Le stringhe di query URL nelle richieste dei visualizzatori, CloudFront incluse 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 Includi le seguenti stringhe di query o Tutte le stringhe di query eccetto, si specificano le stringhe di query solo in base al nome. CloudFront include la stringa di query completa, incluso il relativo valore, nelle richieste di origine.

Crea politiche di richiesta di origine

Puoi 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. Puoi creare una policy di richiesta di origine nella CloudFront console, con AWS Command Line Interface (AWS CLI) o con l' CloudFront API.

Dopo aver creato una policy di richiesta di origine, la colleghi a uno o più comportamenti della cache in una CloudFront distribuzione.

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 AWS Management Console e apri la pagina Policies nella CloudFront console all'indirizzohttps://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 Comprendi le politiche 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 CloudFront console all'indirizzohttps://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. Apri la CloudFront console all'indirizzohttps://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 alle impostazioni di distribuzione.
6. Al termine, scegliere Crea distribuzione.

CLI

Per creare una policy di richiesta di origine con AWS Command Line Interface (AWS CLI), usa il aws cloudfront create-origin-request-policy 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 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 Comprendi le politiche 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 allegare la policy di richiesta di origine al comportamento della cache di una CloudFront distribuzione.

Per allegare una policy di richiesta origine a una distribuzione esistente (CLI con file di input)

1. Usa il comando seguente per salvare la configurazione di CloudFront distribuzione per la distribuzione che desideri 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 alle 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' CloudFront API, usa CreateOriginRequestPolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta Comprendi le politiche relative alle richieste di origine la documentazione di riferimento sull'API per il tuo AWS SDK 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 di cache in una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a un comportamento di cache in una nuova distribuzione, usa 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 alle impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Usa politiche di richiesta di origine gestite

CloudFront fornisce una serie di politiche gestite per le richieste di origine che puoi collegare a qualsiasi comportamento della cache della tua 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 Crea politiche di richiesta di origine.

Negli argomenti seguenti vengono descritte le policy di richiesta di origine gestite che è possibile utilizzare.

Argomenti

AllViewer

Visualizza questa politica nella console CloudFront

Questa policy include tutti i valori (stringhe di query, intestazioni e cookie) della richiesta visualizzatore.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella console CloudFront

Questa politica include tutti i valori (intestazioni, cookie e stringhe di query) della richiesta del visualizzatore e tutte le CloudFront intestazioni rilasciate fino a giugno 2022 (le CloudFront intestazioni rilasciate dopo giugno 2022 non sono incluse).

Quando si utilizza AWS CloudFormation, o l' CloudFront API AWS CLI, l'ID per 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 CloudFront intestazioni:
  - `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

Visualizza questa politica nella console 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 politica include anche intestazioni di CloudFront richiesta 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 destinata all'uso con Amazon API Gateway e le origini degli URL delle AWS Lambda funzioni. Queste origini prevedono che l'`Host`intestazione contenga il nome di dominio di origine, non il nome di dominio della CloudFront distribuzione. L'inoltro dell'intestazione `Host` dalla richiesta visualizzatore a queste origini può impedirne il funzionamento.

> **Note**
>
> Quando utilizzi questa politica di richiesta di origine gestita per rimuovere l'`Host`intestazione del visualizzatore, CloudFront aggiunge una nuova `Host` intestazione con il nome di dominio dell'origine alla richiesta di origine.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella console 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 AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

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 AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Elementare- - MediaTailor PersonalizedManifests

Visualizza questa politica nella console CloudFront

Questa policy è stata concepita per essere utilizzata con un'origine che è un endpoint AWS Elemental MediaTailor .

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

UserAgentRefererHeaders

Visualizza questa politica nella CloudFront console

Questa policy include solo le intestazioni `User-Agent` e `Referer`. Non include stringhe di query o cookie.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Aggiungi intestazioni CloudFront di richiesta

È possibile configurare CloudFront l'aggiunta di intestazioni HTTP specifiche alle richieste CloudFront ricevute dai visualizzatori e inoltrate alla funzione origin o 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, l'indirizzo IP, la posizione geografica, il protocollo di richiesta (HTTP o HTTPS). la versione HTTP, i dettagli della connessione TLS e l'impronta JA3 del visualizzatore.

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 la tua origine restituisce risposte diverse in base alle informazioni contenute in queste intestazioni, puoi includerle nella chiave della cache in modo che CloudFront memorizzi le risposte 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 Controlla la chiave della cache con una policy e the section called “Comprendi la 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 Controlla le richieste di origine con una policy.

Argomenti

- Intestazioni per determinare il tipo di dispositivo del visualizzatore
- Intestazioni per determinare la posizione del visualizzatore
- Intestazioni per determinare la struttura dell'intestazione del visualizzatore
- Altre CloudFront intestazioni

Intestazioni per determinare il tipo di dispositivo del visualizzatore

È possibile aggiungere le seguenti intestazioni per determinare il tipo di dispositivo del visualizzatore. In base al valore dell'`User-Agent`intestazione, CloudFront imposta il valore di queste intestazioni su o. `true` `false` Se il dispositivo ricade in più di una categoria, allora più di un valore potrebbe essere `true`. Ad esempio, per alcuni tablet, CloudFront imposta entrambi `CloudFront-Is-Mobile-Viewer` e `CloudFront-Is-Tablet-Viewer` su. `true`

- `CloudFront-Is-Android-Viewer`— Impostato su `true` when CloudFront determina che il visualizzatore è un dispositivo con sistema operativo Android.
- `CloudFront-Is-Desktop-Viewer`— Impostato su `true` quando CloudFront determina che il visualizzatore è un dispositivo desktop.
- `CloudFront-Is-IOS-Viewer`— Impostato su `true` quando CloudFront determina che il visualizzatore è un dispositivo con un sistema operativo mobile Apple, come iPhone, iPod touch e alcuni dispositivi iPad.
- `CloudFront-Is-Mobile-Viewer`— Impostato su `true` quando CloudFront determina che lo spettatore è un dispositivo mobile.
- `CloudFront-Is-SmartTV-Viewer`— Impostato su `true` quando CloudFront determina che lo spettatore è una smart TV.
- `CloudFront-Is-Tablet-Viewer`— Impostato su `true` quando CloudFront determina che lo spettatore è un tablet.

Intestazioni per determinare la posizione del visualizzatore

È possibile aggiungere le seguenti intestazioni per determinare la posizione dello spettatore. CloudFront determina i valori per queste intestazioni in base all'indirizzo IP del visualizzatore. Per i caratteri non ASCII nei valori di queste intestazioni, il carattere viene CloudFront codificato in percentuale secondo la sezione 1.2 di 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, le CloudFront applica a tutte le richieste tranne quelle che provengono dalla rete: 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`).

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.

Altre CloudFront intestazioni

È possibile aggiungere le seguenti intestazioni per determinare il protocollo, la versione, l'impronta JA3 e i dettagli della connessione TLS del visualizzatore:

- `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.
- `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). Questa intestazione si basa sul pacchetto SSL/TLS `Client Hello` del visualizzatore ed è presente solo per le richieste HTTPS.

  > **Note**
  >
  > È possibile aggiungere `CloudFront-Viewer-JA3-Fingerprint` in una policy della richiesta di origine, ma non in una policy della cache.

- `CloudFront-Viewer-TLS`— Contiene la versione SSL/TLS, il codice e 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**
>
> È possibile aggiungere `CloudFront-Viewer-TLS` in una policy della richiesta di origine, ma non in una policy della cache.

Scopri come interagiscono le politiche di richiesta di origine e le politiche di cache

Puoi utilizzare una policy di richiesta di CloudFront origine per controllare le richieste CloudFront inviate all'origine, chiamate richieste di 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 Controlla le richieste di origine con una policy.

Le politiche di richiesta di origine e le politiche di cache collaborano per determinare i valori CloudFront inclusi nelle richieste di 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. La tabella seguente spiega quali valori sono CloudFront inclusi nelle richieste di origine quando si utilizzano insieme le impostazioni di una politica di richiesta di origine e una politica di 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	All (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 Controlla le 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.
All (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	Tutte le stringhe di query e i cookie della richiesta visualizzatore sono inclusi nella richiesta origine, anche quelli specifica

	Policy di richiesta origine			
	Nessuno	All (Tutti)	Elenco di indirizzi consentiti	Elenco di indirizzi bloccati
			origine, sono inclusi nella richiesta origine.	ti 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	All (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	All (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.

Aggiungi o rimuovi le intestazioni HTTP nelle CloudFront risposte con una policy

Puoi CloudFront configurare la modifica delle intestazioni HTTP nelle risposte che invia 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, puoi rimuovere intestazioni come `X-Powered-By` e `Vary` in modo da CloudFront non includerle nelle risposte che invia agli spettatori. 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'`Server-Timing`intestazione per visualizzare le informazioni relative alle prestazioni e al routing della richiesta e della risposta. CloudFront

Per specificare le intestazioni da CloudFront aggiungere o rimuovere nelle risposte HTTP, si utilizza una politica relativa alle intestazioni di risposta. Associate una policy relativa alle intestazioni di risposta a un altro comportamento della cache e CloudFront modificate le intestazioni nelle risposte che invia alle richieste che corrispondono al comportamento della cache. CloudFront modifica le intestazioni nelle risposte che fornisce dalla cache e quelle che inoltra dall'origine. Se la risposta di origine include una o più intestazioni aggiunte in una politica di intestazioni di risposta, la policy può specificare se CloudFront utilizza l'intestazione ricevuta dall'origine o sovrascrive quell'intestazione con quella nella politica delle intestazioni di risposta.

CloudFront fornisce politiche predefinite per le intestazioni di risposta, note come politiche 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 di intestazione di risposta a più comportamenti di cache in più distribuzioni del tuo. Account AWS

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

Comprendi le politiche relative alle intestazioni di risposta

Puoi utilizzare una politica sulle intestazioni di risposta per specificare le intestazioni HTTP che Amazon CloudFront rimuove o aggiunge nelle risposte che invia agli utenti. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perchè utilizzarle, consulta Aggiungi o rimuovi le intestazioni di risposta 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 aggiungere l'`Access-Control-Allow-Credentials`intestazione nelle risposte alle richieste CORS. Quando questa impostazione è impostata su`true`, CloudFront aggiunge l'`Access-Control-Allow-Credentials: true`intestazione nelle risposte alle richieste CORS. Altrimenti, CloudFront non aggiunge questa intestazione alle risposte.

Access-Control-Allow-Headers

Speciifica i nomi delle intestazioni che CloudFront vengono utilizzati come valori per l'`Access-Control-Allow-Headers`intestazione nelle risposte alle richieste di preflight 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'`Authorization`intestazione non può utilizzare un wildcard e deve essere elencata in modo esplicito.

Esempi di utilizzo valido del carattere jolly

Esempio	Corrisponderà	Non corrisponderà
`x-amz-*`	`x-amz-test` `x-amz-`	`x-amz`
`x-*-amz`	`x-test-amz`	

Esempio	Corrisponderà	Non corrisponderà
	`x--amz`	
`*`	Tutte le intestazioni tranne `Authorization`	`Authorization`

Access-Control-Allow-Methods

Speciifica i metodi HTTP che vengono CloudFront utilizzati come valori per l'`Access-Control-Allow-Methods`sintestazione nelle risposte alle richieste di preflight 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

Speciifica i valori che CloudFront possono essere utilizzati nell'intestazione della 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. Per alcuni esempi, consultare la tabella che segue.

> **Note**
>
> Il carattere jolly (`*`) è consentito come parte più a sinistra del dominio (`*.example.org`). Il carattere jolly (`*`) non è consentito nelle seguenti posizioni:
>
> - Domini di primo livello (`example.*`)
> - A destra dei domini secondari (`test.*.example.org`)
> - All'interno dei termini (`exa*mple.org`))

In questa tabella sono mostrati esempi di uso valido del carattere jolly:

Esempio	Corrisponderà	Non corrisponderà
`http://*.example.org`	`http://www.example.org`	**`https`**`://test.example.org`

Esempio	Corrisponderà	Non corrisponderà

	`http://test.example.org`
	
	`http://test.example.org:123`
		`https``://test.example.org:123`

`*.example.org`	`test.example.org`
	
	`test.test.example.org`
	
	`.example.org`
	
	`http://test.example.org`
	
	`https://test.example.org`
	
	`http://test.example.org:123`
	
	`https://test.example.org:123`	

`example.org`	`http://example.org`
	
	`https://example.org`	

`http://example.org`		**`https`**`://example.org` `http://example.org:123`

`http://example.org:*`	`http://example.org:123`
	
	`http://example.org`	

Esempio	Corrisponderà	Non corrisponderà

`http://example.org:1*3`	`http://example.org:123`
	
	`http://example.org:1893`
	
	`http://example.org:13`	

`*.example.org:1*`	`test.example.org:123`	

Access-Control-Expose-Headers

Speciifica i nomi delle intestazioni che CloudFront vengono utilizzati come valori per l'`Access-Control-Expose-Headers`intestazione 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 numero di secondi, che viene CloudFront utilizzato come valore per l'`Access-Control-Max-Age`intestazione nelle risposte alle richieste di preflight CORS.

Sostituzione dell'origine

Un'impostazione booleana che determina come CloudFront si comporta quando la risposta dall'origine contiene una delle intestazioni CORS, anch'esse incluse nella policy.

- Se è impostata su `true` e la risposta di origine contiene un'intestazione CORS che è anche nella politica, CloudFront aggiunge l'intestazione CORS nella politica alla risposta. CloudFront quindi invia la risposta allo spettatore. CloudFront ignora l'intestazione che ha ricevuto dall'origine.
- Se impostata su `false` e la risposta di origine contiene un'intestazione CORS (indipendentemente dal fatto che l'intestazione CORS sia nella politica), CloudFront include l'intestazione CORS che ha ricevuto dall'origine alla risposta. CloudFront non aggiunge alcuna intestazione CORS nella policy alla risposta che viene 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

Speciifica le direttive della politica di sicurezza dei contenuti che CloudFront vengono utilizzate 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

Speciifica la direttiva della politica 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

Speciifica le direttive e le impostazioni da CloudFront utilizzare come valore per l'intestazione della risposta. `Strict-Transport-Security` Per questa impostazione, è necessario specificare separatamente:

- Un numero di secondi, che viene CloudFront utilizzato come valore per la `max-age` direttiva di questa intestazione

- Un'impostazione booleana (`true`o`false`) per`preload`, che determina se CloudFront include la `preload` direttiva nel valore di questa intestazione
- Un'impostazione booleana (`true`o`false`) per`includeSubDomains`, che determina se CloudFront include la `includeSubDomains` direttiva 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 l'intestazione alle risposte. `X-Content-Type-Options` Quando questa impostazione è impostata`true`, CloudFront aggiunge l'`X-Content-Type-Options: nosniff`intestazione alle risposte. Altrimenti CloudFront non aggiunge questa intestazione.

Per ulteriori informazioni su questa intestazione, consulta X-Content-Type-Options nei documenti Web MDN.

X-Frame-Options

Speciifica la direttiva da CloudFront utilizzare come valore per l'intestazione della `X-Frame-Options` risposta. 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 da CloudFront utilizzare 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 `mode=block` direttiva nel valore di questa intestazione
- Un URI di segnalazione, che determina se CloudFront include la `report=`*`reporting URI`* direttiva 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

Ciascuna di queste impostazioni delle intestazioni di sicurezza contiene un'impostazione booleana (`trueofalse`) che determina come CloudFront si comporta quando la risposta dall'origine contiene quell'intestazione.

Quando questa impostazione è impostata su `true` e la risposta di origine contiene l'intestazione, CloudFront aggiunge l'intestazione nella policy alla risposta che invia al visualizzatore. ignorando l'intestazione ricevuta dall'origine.

Quando questa impostazione è impostata su `false` e la risposta di origine contiene l'intestazione, CloudFront include l'intestazione ricevuta dall'origine nella risposta che invia al visualizzatore.

Quando la risposta di origine non contiene l'intestazione, CloudFront aggiunge l'intestazione nella policy alla risposta che invia al visualizzatore. CloudFront esegue questa operazione quando questa impostazione è impostata su `otrue`. `false`

Intestazioni personalizzate

È possibile utilizzare le impostazioni delle intestazioni personalizzate per aggiungere e configurare intestazioni HTTP personalizzate in una politica di intestazioni di risposta. CloudFront aggiunge queste intestazioni a ogni risposta che restituisce agli spettatori. 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 impostata su `true` e la risposta di origine contiene l'intestazione personalizzata inclusa nella politica, CloudFront aggiunge l'intestazione personalizzata nella politica alla risposta che invia al visualizzatore. ignorando l'intestazione ricevuta dall'origine.
- Se questa impostazione è `false` attiva e la risposta di origine contiene l'intestazione personalizzata inclusa nella policy, CloudFront include l'intestazione personalizzata ricevuta dall'origine nella risposta che invia al visualizzatore.
- Quando la risposta di origine non contiene l'intestazione personalizzata inclusa nella policy, CloudFront aggiunge l'intestazione personalizzata nella policy alla risposta che invia al visualizzatore. CloudFront esegue questa operazione quando questa impostazione è impostata su `otrue`. `false`

Rimozione delle intestazioni

Puoi specificare le intestazioni che desideri CloudFront rimuovere dalle risposte che riceve dall'origine in modo che le intestazioni non vengano incluse nelle risposte inviate agli spettatori. CloudFront CloudFront rimuove le intestazioni da ogni risposta che invia ai visualizzatori, indipendentemente dal fatto che gli oggetti vengano serviti dalla cache o dall' CloudFrontorigine. Ad esempio, puoi rimuovere le intestazioni che non sono utili per i browser, come `X-Powered-By` o`Vary`, in modo da CloudFront rimuovere queste intestazioni dalle risposte che invia ai visualizzatori.

Quando specificate le intestazioni da rimuovere utilizzando una politica sulle intestazioni di risposta, CloudFront rimuove prima le intestazioni e poi aggiunge le intestazioni specificate in altre sezioni della politica delle intestazioni di risposta (intestazioni CORS, intestazioni di sicurezza, intestazioni personalizzate, ecc.). 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 agli spettatori.

> **Note**
>
> Puoi utilizzare una politica sulle intestazioni di risposta per rimuovere le `Date` intestazioni `Server` e le intestazioni CloudFront ricevute dall'origine, in modo che queste intestazioni (così come ricevute dall'origine) non vengano incluse nelle risposte inviate agli spettatori. CloudFront Tuttavia, se lo fai, CloudFront aggiunge la propria versione di queste intestazioni alle risposte che invia agli spettatori. Per l'`Server`intestazione che CloudFront aggiunge, 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

Utilizza l'impostazione dell'`Server-Timing`intestazione per abilitare l'`Server-Timing`intestazione nelle risposte HTTP inviate da. CloudFront Puoi utilizzare questa intestazione per visualizzare metriche che possono aiutarti a ottenere informazioni sul comportamento e sulle prestazioni e sulla tua origine CloudFront . 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. Le metriche nell'`Server-Timing`intestazione possono aiutarti a risolvere i problemi o a testare l'efficienza della tua configurazione o di quella di origine. CloudFront

Per ulteriori informazioni sull'utilizzo dell'`Server-Timing`intestazione con CloudFront, consulta i seguenti argomenti.

Per abilitare l'intestazione `Server-Timing`, creare (o modificare) una policy per le intestazioni di risposta.

Argomenti

- Frequenza di campionamento e intestazione richiesta Pragma
- Intestazione Server-Timing dell'origine
- Metriche dell'intestazione del server-timing
- Esempi di intestazione Sever-Timing

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 compreso tra 0 e 100 (incluso) che specifica la percentuale di risposte a cui si desidera CloudFront aggiungere l'intestazione. `Server-Timing` Quando imposti la frequenza di campionamento su 100, CloudFront aggiunge l'`Server-Timing`intestazione alla risposta HTTP per ogni richiesta che corrisponde al comportamento della cache a cui è associata la politica delle intestazioni di risposta. Quando lo imposti 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 puoi controllare a quali risposte CloudFront aggiungere l'`Server-Timing`intestazione, ma 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'`Server-Timing`intestazione alla risposta se la richiesta contiene l'intestazione. `Pragma: server-timing`

Intestazione Server-Timing dell'origine

Quando si verifica un errore nella cache e CloudFront inoltra la richiesta all'origine, l'origine potrebbe includere un'`Server-Timing`intestazione nella sua risposta a. CloudFront In questo caso, CloudFront aggiunge le sue metriche all'`Server-Timing`intestazione ricevuta dall'origine. La risposta CloudFront inviata al visualizzatore contiene un'unica `Server-Timing` intestazione che include il valore proveniente dall'origine e le metriche aggiunte. CloudFront Il valore dell'intestazione dall'origine potrebbe trovarsi alla fine o tra due set di metriche che si CloudFront aggiungono all'intestazione.

Quando si verifica un accesso alla cache, la risposta CloudFront inviata al visualizzatore contiene un'unica `Server-Timing` intestazione che include solo le CloudFront metriche nel valore dell'intestazione (il valore dell'origine non è incluso).

Metriche dell'intestazione del server-timing

Quando CloudFront aggiunge l'`Server-Timing`intestazione a una risposta HTTP, il valore dell'intestazione contiene una o più metriche che possono aiutarti a ottenere informazioni sul comportamento e sulle prestazioni e sulla tua origine. CloudFront L'elenco seguente contiene tutti i parametri e i relativi valori potenziali. Un'`Server-Timing`intestazione contiene solo alcune di queste metriche, a seconda della natura della richiesta e della risposta. 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 fare 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'intero oggetto dall'origine.

cdn-cache-miss

CloudFront non ha fornito la risposta dalla cache. In questo caso, CloudFront ha richiesto l'intero oggetto dall'origine prima di restituire la risposta.

cdn-pop

Contiene un valore che descrive quale CloudFront punto di presenza (POP) ha gestito la richiesta.

cdn-rid

Contiene un valore con l'identificatore CloudFront univoco della richiesta. È possibile utilizzare questo identificatore di richiesta (RID) per la risoluzione dei problemi con AWS Support

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 REC (Regional Edge Cache).
- 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. Il valore zero (0) indica che ha CloudFront 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. Il valore zero (0) indica che è stata CloudFront riutilizzata 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 riportati alcuni esempi di `Server-Timing` intestazione che uno spettatore potrebbe ricevere CloudFront quando l'impostazione dell'`Server-Timing`intestazione è abilitata.

Example — cache miss

L'esempio seguente mostra un'`Server-Timing`intestazione che un visualizzatore potrebbe ricevere quando l'oggetto richiesto non è presente nella cache. 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 una posizione POP (CloudFront Point of Presence) (`cdn-upstream-layer;desc="EDGE"`).
- CloudFront ha utilizzato un risultato DNS memorizzato nella cache per origin ()`cdn-upstream-dns;dur=0`.
- Sono stati necessari 114 millisecondi per CloudFront completare la connessione TCP (e TLS, se applicabile) all'origine (). `cdn-upstream-connect;dur=114`

- Ci sono voluti 177 millisecondi per CloudFront ricevere il primo byte della risposta dall'origine, dopo aver completato la richiesta (). `cdn-upstream-fbl;dur=177`
- L'oggetto richiesto non era nella cache () CloudFront. `cdn-cache-miss`
- La richiesta è stata ricevuta nella posizione edge identificata dal codice `PHX50-C2` (`cdn-pop;desc="PHX50-C2"`).
- L'ID CloudFront univoco per questa richiesta era `yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==` (`cdn-rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg=="`).
- Sono stati necessari 436 millisecondi per CloudFront inviare il primo byte della risposta al visualizzatore, dopo aver ricevuto la richiesta del visualizzatore (). `cdn-downstream-fbl;dur=436`

Example - hit della cache

L'esempio seguente mostra un'`Server-Timing`intestazione che un visualizzatore potrebbe ricevere quando l'oggetto richiesto si trova nella cache del visualizzatore. 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 CloudFront univoco 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"`).
- Sono stati necessari 137 millisecondi per CloudFront inviare il primo byte della risposta al visualizzatore, dopo aver ricevuto la richiesta del visualizzatore (). `cdn-downstream-fbl;dur=137`

Crea politiche per le intestazioni di risposta

Puoi utilizzare una politica sulle intestazioni di risposta per specificare le intestazioni HTTP che Amazon CloudFront aggiunge o rimuove nelle risposte HTTP. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perché utilizzarle, consulta Aggiungi o rimuovi le intestazioni di risposta con una policy.

Puoi creare una politica di intestazioni di risposta nella console. CloudFront Oppure puoi crearne una utilizzando AWS CloudFormation, the AWS Command Line Interface (AWS CLI) o l' CloudFront API. Dopo aver creato una policy relativa alle intestazioni di risposta, la colleghi a uno o più comportamenti della cache in una CloudFront distribuzione.

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. Accedi a AWS Management Console, quindi vai alla scheda Intestazioni di risposta nella pagina Politiche della console all' CloudFront 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 desideri che le intestazioni configurate sovrascrivano le intestazioni CloudFront ricevute dall'origine, seleziona la casella di controllo Origin override.

      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 Rimuovi le intestazioni, aggiungi i nomi di tutte le intestazioni che desideri CloudFront rimuovere dalla risposta dell'origine e non includerle nella risposta inviata agli spettatori. CloudFront

   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 per le intestazioni di risposta, potete collegarla a un comportamento di cache in una distribuzione. CloudFront

Per allegare una policy delle intestazioni di risposta a una distribuzione esistente (console)

1. Apri la pagina Distribuzioni nella CloudFront console 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. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli 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 “Distribution Settings (Impostazioni distribuzione)”.
5. Scegliere Crea una distribuzione per creare la distribuzione.

AWS CloudFormation

Per creare una politica di intestazioni di risposta con AWS CloudFormation, usa il tipo di `AWS::CloudFront::ResponseHeadersPolicy` risorsa. L'esempio seguente mostra la sintassi del AWS CloudFormation modello, in formato YAML, per la creazione di una politica di 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, vedere AWS::CloudFront::ResponseHeadersPolicy nella Guida per l'utente.AWS CloudFormation

CLI

Per creare una politica di intestazioni di risposta con AWS Command Line Interface (AWS CLI), utilizzate il aws cloudfront create-response-headers-policy 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 policy delle intestazioni di risposta (CLI con file di input)

1. Per creare un file denominato `response-headers-policy.yaml`, utilizza il comando seguente. 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 “Comprendi le politiche relative alle 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. Ne hai bisogno per allegare la policy al comportamento della cache di una CloudFront distribuzione.

Per allegare una policy delle intestazioni di risposta a una distribuzione esistente (CLI con file di input)

1. Utilizzate il comando seguente per salvare la configurazione di CloudFront distribuzione per la distribuzione che desiderate 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 `distribution.yaml`, utilizza i comandi seguenti. 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 alle 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 politica di intestazioni di risposta con l' CloudFront API, usa CreateResponseHeadersPolicy. Per ulteriori informazioni sui campi specificati in questa chiamata API, consulta the section called “Comprendi le politiche relative alle intestazioni di risposta” la documentazione di riferimento sull'API per il tuo AWS SDK 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 di cache in una distribuzione esistente, usa UpdateDistribution.
- Per collegarlo a un comportamento di cache in una nuova distribuzione, usa 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 alle impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Utilizza politiche gestite per le intestazioni di risposta

Con una politica sulle intestazioni di CloudFront risposta, puoi specificare le intestazioni HTTP che Amazon CloudFront rimuove o aggiunge nelle risposte che invia agli utenti. Per ulteriori informazioni sulle policy delle intestazioni di risposta e sul perché utilizzarle, consulta Aggiungi o rimuovi le intestazioni di risposta con una policy.

CloudFront fornisce politiche gestite di intestazioni di risposta che puoi allegare ai comportamenti della cache nelle tue 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. Puoi allegare la policy per nome (con la console) o per ID (con AWS CloudFormation AWS CLI, o gli AWS SDK). I nomi e gli ID sono elencati nella sezione seguente.

Per ulteriori informazioni, consulta the section called “Crea politiche per le intestazioni di risposta”.

Negli argomenti seguenti vengono descritte le policy delle intestazioni di risposta gestite che è possibile utilizzare.

Argomenti

- CORS e- SecurityHeadersPolicy
- CORS-With-Preflight
- CORS- - with-preflight-and SecurityHeadersPolicy
- SecurityHeadersPolicy
- SimpleCORS

CORS e- SecurityHeadersPolicy

Visualizza questa politica nella console CloudFront

Usa questa policy gestita per consentire semplici richieste CORS da qualsiasi origine. Questa politica aggiunge anche una serie di intestazioni di sicurezza a tutte le risposte CloudFront inviate agli spettatori. Questa policy combina le policy the section called “SimpleCORS” e the section called “SecurityHeadersPolicy” in uno.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

Utilizzare questa policy gestita per consentire richieste CORS da qualsiasi origine, incluse le richieste di verifica preliminare. Per le richieste di preflight (utilizzando il `OPTIONS` metodo HTTP), CloudFront aggiunge tutte e tre le seguenti intestazioni alla risposta. Per richieste CORS semplici, CloudFront aggiunge solo l'intestazione. `Access-Control-Allow-Origin`

Se la risposta CloudFront ricevuta dall'origine include una di queste intestazioni, CloudFront utilizza l'intestazione ricevuta (e il relativo valore) nella risposta al visualizzatore. CloudFrontnon utilizza l'intestazione in questa politica.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella console CloudFront

Usa questa policy gestita per consentire richieste CORS da qualsiasi origine. Sono incluse le richieste di verifica preliminare. Questa politica aggiunge anche una serie di intestazioni di sicurezza a tutte le risposte CloudFront inviate agli spettatori. Questa policy combina le policy the section called "CORS-With-Preflight" e the section called "SecurityHeadersPolicy" in uno.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

Utilizza questa politica gestita per aggiungere un set di intestazioni di sicurezza a tutte le risposte CloudFront inviate agli spettatori. Per ulteriori informazioni su queste intestazioni di sicurezza, consulta Mozilla's web security guidelines (Linee guida sulla sicurezza Web di Mozilla).

Con questa politica sulle intestazioni di risposta, si CloudFront aggiunge `X-Content-Type-Options: nosniff` a tutte le risposte. Questo è il caso in cui la risposta CloudFront ricevuta dall'origine includeva questa intestazione e quando non lo era. Per tutte le altre intestazioni di questa politica, se la risposta CloudFront ricevuta dall'origine include l'intestazione, CloudFront utilizza l'intestazione ricevuta (e il relativo valore) nella risposta al visualizzatore. Non utilizza l'intestazione in questa policy.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Visualizza questa politica nella CloudFront console

Usa questa policy gestita per consentire semplici richieste CORS da qualsiasi origine. Con questo criterio, CloudFront aggiunge l'intestazione `Access-Control-Allow-Origin: *` a tutte le risposte per semplici richieste CORS.

Se la risposta CloudFront ricevuta dall'origine include l'`Access-Control-Allow-Origin`intestazione, CloudFront utilizza quell'intestazione (e il relativo valore) nella risposta al visualizzatore. CloudFront non utilizza l'intestazione in questa politica.

Quando si utilizza AWS CloudFormation AWS CLI, o l' CloudFront API, l'ID per 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

Le seguenti sezioni spiegano come CloudFront elabora le richieste dei visualizzatori e le inoltra al tuo Amazon S3 o all'origine personalizzata e CloudFront come elabora le risposte dall'origine, incluso il CloudFront modo in cui elabora e memorizza nella cache i codici di stato HTTP 4xx e 5xx.

Argomenti

Come elabora le richieste HTTP e HTTPS CloudFront

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 quanto riguarda le origini personalizzate, quando crei la distribuzione, puoi specificare in che modo CloudFront accede alla tua origine: solo HTTP o corrispondente al protocollo utilizzato dal visualizzatore. Per ulteriori informazioni su come CloudFront gestisce le richieste HTTP e HTTPS per le origini personalizzate, consultaProtocolli.

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

Scopri come CloudFront elabora le richieste dei visualizzatori e le inoltra alla tua origine Amazon S3.

Indice

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 Gestisci la durata della 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'intestazione `X-Forwarded-For` contiene indirizzi IPv4 (ad esempio 192.0.2.44) e IPv6 (ad esempio 2001:0db8:85a3::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 Contenuto della cache in base alle intestazioni delle richieste.

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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.

> **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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.

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 CloudFront edge location deve inviare una richiesta di convalida separata. 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 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.

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 Contenuto della cache in base ai parametri della stringa 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 Controlla i timeout e i 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 l'ultimo tentativo, CloudFront non riprova finché non riceve un'altra richiesta di 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 vuoi evitare che tutte le richieste vengano compresse, puoi utilizzare la policy di cache gestita`CachingDisabled`, che impedisce anche la memorizzazione nella cache. Per ulteriori informazioni, consulta Usa politiche di cache gestite.

Se vuoi evitare che la richiesta venga compressa per oggetti specifici, puoi impostare il TTL minimo per il comportamento della cache su 0 e configurare l'origine per inviare`Cache-Control:`

`private`,`Cache-Control: no-store`, `Cache-Control: no-cache` o. `Cache-Control: max-age=0` `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 abiliti 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 Contenuto della cache basato sui 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 URL personalizzati aggiungendo nomi di dominio alternativi (CName).

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

- User-Agent Intestazione

Autenticazione

Se inoltri l'`Authorization`intestazione all'origine, puoi quindi configurare il server di origine per richiedere l'autenticazione del 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 si utilizzano 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 Configura CloudFront per inoltrare l'intestazione `Authorization`.

È possibile 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 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 Gestisci la durata della 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 da inoltrare a ELB e se l'indirizzo IP del server CloudFront edge è 192.0.2.199, la richiesta ricevuta dall'istanza EC2 contiene l'intestazione seguente:

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> L'intestazione `X-Forwarded-For` contiene indirizzi IPv4 (ad esempio 192.0.2.44) e IPv6 (ad esempio 2001:0db8:85a3::8a2e:0370:7334).
> Si noti inoltre che l'`X-Forwarded-For`intestazione può essere modificata da ogni nodo sul percorso del server corrente (). 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 non supporta l'autenticazione client con certificati SSL lato client. Se un'origine richiede un certificato lato client, elimina la richiesta. CloudFront

Compressione

Per ulteriori informazioni, consulta Servire 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 Contenuto della cache basato sui cookie.

Cookie

È possibile configurare CloudFront l'inoltro dei cookie all'origine. Per ulteriori informazioni, consulta Contenuto della cache basato sui 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 Contenuto della cache in base alle intestazioni delle richieste.

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 e TLSv1.2. Per le origini personalizzate, puoi scegliere i protocolli SSL che desideri utilizzare per comunicare con la tua origine: CloudFront

- 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, utilizza CloudFront sempre TLSv1.2.

> **Important**
>
> Le altre versioni di SSL e TLS non sono supportate.

Per ulteriori informazioni sull'utilizzo di HTTPS con, consulta. CloudFront 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 da gestire `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 Contenuto della cache in base alle intestazioni delle richieste.

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
`Accept-Charset`	CloudFront rimuove l'intestazione.	Sì
`Accept-Encoding`		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
	Se il valore contiene `gzip` `obr`, CloudFront inoltra un'`Accept-Encoding` intestazione normalizzata all'origine. Per ulteriori informazioni, consulta Supporto della compressione e Servire file compressi.	
`Accept-Language`	CloudFront rimuove l'intestazione.	Sì
`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

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
`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 Configura la memorizzazione nella cache in base al protocollo della richiesta.	Sì
`CloudFront-Is-Desktop-Viewer`	CloudFront non aggiunge l'intestazione prima di inoltrare la richiesta all'origine. Per ulteriori informazioni, consulta Configura la memorizzazione nella cache 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 Configura la memorizzazione nella cache 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 Configura la memorizzazione nella cache in base al tipo di dispositivo.	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-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
`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 Contenuto della cache basato sui 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

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
`Host`	CloudFront imposta il valore sul nome di dominio dell'origine associato all'oggetto richiesto. Non puoi 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
`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

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
`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 (range GETs).	Sì, per impostazione predefinita
`Referer`	CloudFront rimuove l'intestazione.	Sì
`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)

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
`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. Configura la memorizzazione nella cache 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
`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

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-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 dello stapling OCSP è più pronunciato quando si CloudFront ricevono 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 molte richieste HTTPS per lo stesso dominio, ogni server nell'edge location riceve subito una risposta dalla CA che può «pinzare» su un pacchetto dell'handshake SSL; quando l'utente ritiene che il certificato sia valido, CloudFront può servire l'oggetto richiesto. Se la tua 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 origine (solo origini personalizzate) in questa sezione Riferimento alle 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. Tieni presente che CloudFront memorizza nella cache l'oggetto solo una 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 Contenuto della cache in base ai parametri della stringa 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 Controlla i timeout e i 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 l'ultimo tentativo, CloudFront non riprova finché non riceve un'altra richiesta di 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.

Per ulteriori informazioni, incluso il modo in cui configurare il timeout di risposta origine, consulta Timeout di risposta (solo origini personalizzate).

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 vuoi evitare che tutte le richieste vengano compresse, puoi utilizzare la policy di cache gestita`CachingDisabled`, che impedisce anche la memorizzazione nella cache. Per ulteriori informazioni, consulta Usa politiche di cache gestite.

Se vuoi evitare che la richiesta venga compressa per oggetti specifici, puoi impostare il TTL minimo per il comportamento della cache su 0 e configurare l'origine per inviare`Cache-Control: private`,`Cache-Control: no-store`, `Cache-Control: no-cache` o. `Cache-Control: max-age=0` `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 abiliti 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 tablet, CloudFront potrebbe impostare entrambi e su. `CloudFront-Is-Mobile-Viewer` `CloudFront-Is-Tablet-Viewer` `true` Per ulteriori informazioni sulla configurazione della cache CloudFront in base alle intestazioni delle richieste, consulta. Contenuto della cache in base alle intestazioni delle richieste

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

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 Contenuto della cache basato sui 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'`Content-Length`intestazione, CloudFront non è possibile determinare se la connessione TCP è stata interrotta accidentalmente o intenzionalmente.

Si consiglia di configurare il server HTTP per aggiungere un'`Content-Length`intestazione per CloudFront impedire 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 Contenuto della cache basato sui 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 Configura la memorizzazione nella cache 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 Front 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 comporterà addebiti 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 nell'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 Ottimizza l'alta disponibilità con il failover di CloudFront origine.

Aggiungi intestazioni personalizzate alle richieste di origine

Puoi CloudFront configurare l'aggiunta di intestazioni personalizzate alle richieste inviate all'origine. Puoi utilizzare le intestazioni personalizzate per inviare e raccogliere dalla tua origine informazioni che non si ottengono con le tipiche richieste dei visualizzatori. Puoi persino personalizzare le intestazioni per ogni origine. CloudFrontsupporta intestazioni personalizzate per origini personalizzate e origini Amazon S3.

Indice

Casi d'uso

Puoi utilizzare intestazioni personalizzate, come i seguenti esempi:

Identificazione delle richieste provenienti da CloudFront

Puoi identificare le richieste da cui proviene la tua origine CloudFront. Questo può essere utile se vuoi sapere se gli utenti stanno ignorando CloudFront la situazione o se utilizzi più di un CDN e desideri 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 configuri più di una CloudFront distribuzione per utilizzare la stessa origine, puoi aggiungere diverse intestazioni personalizzate in ciascuna distribuzione. Puoi quindi utilizzare i log della tua origine per determinare quali richieste provengono da quale CloudFront distribuzione.

Abilitazione della funzionalità Cross-Origin Resource Sharing (CORS)

Se alcuni dei tuoi visualizzatori non supportano la condivisione di risorse tra origini diverse (CORS), puoi configurare in modo CloudFront da aggiungere sempre l'`Origin`intestazione 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 per rispettare le impostazioni CORSCloudFront .

Controllo dell'accesso ai contenuti

È possibile utilizzare intestazioni personalizzate per controllare l'accesso ai contenuti. Configurando la tua origine in modo che risponda alle richieste solo quando includono

un'intestazione personalizzata che viene aggiunta da CloudFront, impedisci agli utenti di ignorare CloudFront e accedere ai tuoi contenuti direttamente dall'origine. Per ulteriori informazioni, consulta Limita l'accesso ai file su origini personalizzate.

Configura CloudFront per aggiungere intestazioni personalizzate alle richieste di 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:

- CloudFront console: 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.
- CloudFront API: per ogni origine a cui desideri aggiungere intestazioni personalizzate, specifica i nomi e i valori delle intestazioni nel campo all'interno. `CustomHeaders` `Origin` Per ulteriori informazioni, consulta CreateDistributiono UpdateDistributionconsulta Amazon CloudFront API Reference.

Se i nomi e i valori delle intestazioni specificati non sono già presenti nella richiesta del visualizzatore, li CloudFront aggiunge alla richiesta di origine. Se è presente un'intestazione, 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 non CloudFront possono essere aggiunte alle richieste di origine

Non puoi CloudFront configurare l'aggiunta 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-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`

Configura CloudFront per inoltrare l'intestazione **`Authorization`**

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:

- 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 Controlla la 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. CloudFront fornisce una politica di richiesta di

origine gestita per questo caso d'uso, denominata Managed-. AllViewer Per ulteriori informazioni, consulta Usa politiche di richiesta di origine gestite.

Come CloudFront elabora le richieste parziali per un oggetto (range GETs)

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 `Range` intestazioni non soddisfano i seguenti requisiti, CloudFront restituisce il codice di stato HTTP con l'oggetto completo anziché il codice di stato `200` con gli intervalli specificati: `206`

- 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. Considerate 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.

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 Gestisci la durata della 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 sono state configurate pagine di errore personalizzate
- Se hai configurato per quanto tempo desideri CloudFront memorizzare nella cache le risposte di errore dall'origine (errore TTL minimo di memorizzazione nella cache)
- Il codice di stato

- Per i codici di stato 5xx, indica se l'oggetto richiesto è attualmente nella cache CloudFront edge
- Per alcuni codici di stato 4xx, indica se l'origine restituisce un'`Cache-Control max-age`intestazione o `Cache-Control s-maxage`

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 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 memorizzati nella cache CloudFront

Argomenti

- In che modo CloudFront elabora gli errori quando sono state configurate pagine di errore personalizzate
- In che modo CloudFront elabora gli errori quando non sono state configurate pagine di errore personalizzate
- Codici di stato HTTP 4xx e 5xx 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: I codici di stato HTTP 4xx e 5xx che vengono sempre memorizzati nella cache CloudFront .
  - Il tuo server di origine restituisce un codice di stato HTTP 4xx senza un'intestazione `Cache-Control max-age` o un'intestazione `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 nella CloudFront 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.

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. Gestisci la durata della permanenza dei contenuti nella cache (scadenza)

In che modo CloudFront elabora gli errori quando non sono state configurate pagine di errore personalizzate

Se non 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: I codici di stato HTTP 4xx e 5xx che vengono sempre memorizzati nella cache CloudFront
  - Il tuo server di origine restituisce un codice di stato HTTP 4xx senza un'intestazione `Cache-Control max-age` o un'intestazione `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 nella CloudFront 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 tempo di memorizzazione nella cache (determinato nel passaggio 1), CloudFront risponde alle successive richieste del visualizzatore 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.
- 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. 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. Gestisci la durata della permanenza dei contenuti nella cache (scadenza)

Codici di stato HTTP 4xx e 5xx 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.

I codici di stato HTTP 4xx e 5xx che vengono sempre memorizzati nella cache CloudFront

CloudFront memorizza sempre 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.

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 nella CloudFront 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

- Configura il comportamento di risposta agli errori

- Crea una pagina di errore personalizzata per codici di stato HTTP specifici
- Archivia oggetti e pagine di errore personalizzate in posizioni diverse
- Modificare i codici di risposta restituiti da CloudFront
- Controlla per quanto tempo CloudFront memorizza gli errori nella cache

Configura il 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 AWS 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 Archivia oggetti e pagine di errore personalizzate in posizioni diverse.
- 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.

Configura risposte di errore personalizzate

Per configurare risposte di errore personalizzate nella CloudFront console, è necessario disporre di una CloudFront distribuzione. 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 CloudFront distribuzione di base.

Console

Per configurare le risposte personalizzate agli errori (console)

1. Accedi AWS Management Console 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 AWS CloudFormation

Per configurare risposte di errore personalizzate con l' CloudFront API oppure AWS CloudFormation, usa il `CustomErrorResponse` tipo in una distribuzione. Per ulteriori informazioni, consulta gli argomenti seguenti:

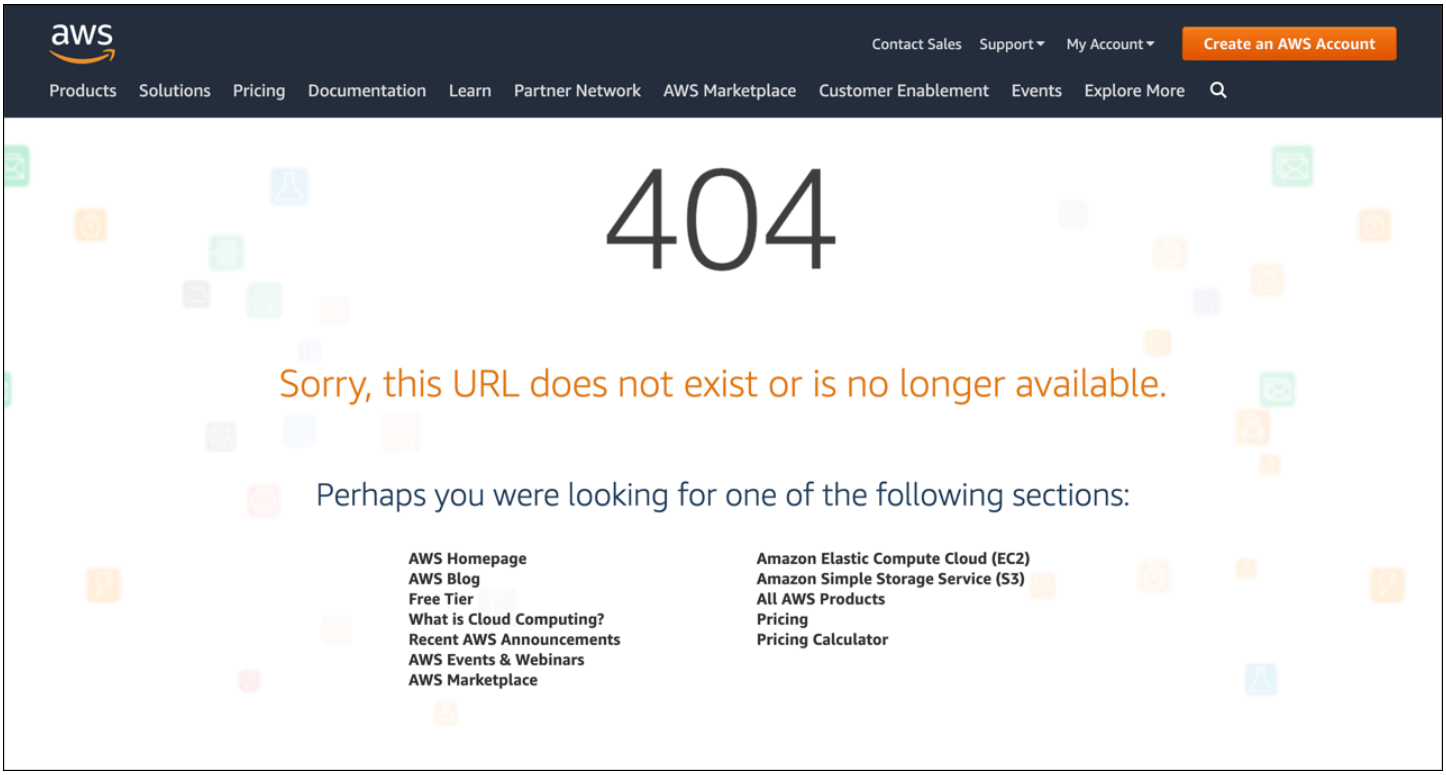
- AWS::CloudFront::Distribution CustomErrorResponse nella Guida per l'utente di AWS CloudFormation
- CustomErrorResponsenell'Amazon CloudFront API Reference

Crea 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 Configura il 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 una serie di 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

> **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

- 500, 501, 502, 503, 504

> **Note**
>
> 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.

Per una spiegazione dettagliata di come vengono CloudFront gestite le risposte di errore provenienti dall'origine, consultaIn che modo CloudFront elabora i codici di stato HTTP 4xx e 5xx dalla tua origine.

Archivia oggetti e pagine di errore personalizzate in posizioni diverse

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 vi interessa distinguere tra diversi errori del client o del server, potete 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 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**
>
> È possibile 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

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 altre **`Cache-Control`** direttive o non aggiunge alcuna intestazione, 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 Invalida i file per rimuovere il contenuto.

Aggiungere, rimuovere o sostituire i contenuti CloudFront distribuiti

Questa sezione spiega come assicurarvi di CloudFront poter accedere ai contenuti che desiderate vengano mostrati ai vostri spettatori, come specificare gli oggetti nel sito Web o nell'applicazione e come rimuovere o sostituire i contenuti.

Argomenti

Aggiungi e accedi ai contenuti che distribuiscono CloudFront

Quando si CloudFront desidera distribuire contenuti (oggetti), si aggiungono file a una delle origini specificate per la distribuzione e si espone un CloudFront collegamento ai file. Una CloudFront edge location non recupera i nuovi file da un'origine finché non riceve le richieste dei visualizzatori in merito. Per ulteriori informazioni, consulta Come distribuisce i contenuti CloudFront .

Quando aggiungi un file che desideri CloudFront distribuire, assicurati di aggiungerlo a uno dei bucket Amazon S3 specificati 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 hai altri comportamenti di cache configurati per inoltrare le richieste a quell'origine, CloudFront inoltrerà solo i file. `*.html` In questo scenario, ad esempio, non CloudFront distribuirà mai i file con estensione jpg caricati sull'origine, poiché non è stato creato un comportamento di cache che includa i file.jpg.

CloudFront i server 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.

Usa il controllo delle versioni dei file per aggiornare o rimuovere il contenuto con una distribuzione CloudFront

Per aggiornare il contenuto esistente che CloudFront è configurato per essere distribuito automaticamente, si consiglia di utilizzare un identificatore di versione nei nomi dei file o nei nomi delle cartelle. Questo ti aiuta a controllare la gestione dei contenuti che pubblichi CloudFront .

Aggiorna i file esistenti utilizzando nomi di file con versioni

Quando aggiorni i file esistenti in una CloudFront distribuzione, ti consigliamo di includere una sorta di identificatore di versione nei nomi dei file o nei nomi delle directory per avere un migliore 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. Con il controllo delle versioni, non è necessario attendere la scadenza di un oggetto prima di CloudFront iniziare a distribuirne una nuova versione e non è necessario pagare per l'invalidazione dell'oggetto.

Anche se stabilisci la versione dei file, ti consigliamo comunque di impostare una data di scadenza. Per ulteriori informazioni, consulta Gestisci la durata della 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.

Rimuovi i contenuti in modo CloudFront da non distribuirli

Puoi rimuovere dall'origine i file che non desideri più includere nella tua CloudFront distribuzione. Tuttavia, CloudFront continuerà a mostrare agli spettatori il contenuto della cache edge fino alla scadenza dei file.

Se desideri rimuovere un file immediatamente, devi eseguire una delle seguenti operazioni:

- Utilizzare la funzione Versioni multiple. Quando si utilizza il controllo delle versioni, diverse versioni di un file hanno nomi diversi che è possibile utilizzare nella CloudFront distribuzione per modificare il file che viene restituito ai visualizzatori. Per ulteriori informazioni, consulta Aggiorna i file esistenti utilizzando nomi di file con versioni.
- Invalidare il file. Per ulteriori informazioni, consulta Invalida i file per rimuovere il contenuto.

Personalizza il formato URL per i file in CloudFront

Dopo aver impostato l'origine con gli oggetti (contenuti) che desiderate mostrare CloudFront agli utenti, dovete utilizzare gli URL corretti per fare riferimento a tali oggetti nel codice del sito Web o dell'applicazione in modo che CloudFront possano essere utilizzati.

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 viene assegnato automaticamente quando si crea 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 CloudFront un percorso di directory principale per gli oggetti. Per ulteriori informazioni su come impostare il percorso di origine al momento della creazione di una distribuzione, vedi Origin Path (Percorso origine).

Per ulteriori informazioni sul formato degli URL, consulta le seguenti sezioni.

Usa il tuo nome di dominio (example.com)

Invece di usare il nome di dominio predefinito che ti viene assegnato quando CloudFront crei una distribuzione, puoi aggiungere un nome di dominio alternativo più facile da usare, ad esempio. `example.com` Configurando il tuo nome di dominio con CloudFront, puoi utilizzare un URL come questo per gli oggetti della tua distribuzione:

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

Se prevedi di utilizzare HTTPS tra i visualizzatori e CloudFront, consultaUsa nomi di dominio alternativi e HTTPS.

Usa una barra finale (/) negli URL

Quando specifichi gli URL per le directory della tua CloudFront distribuzione, scegli di utilizzare sempre una barra finale o di non usare mai una barra finale. 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 consentono di creare collegamenti a CloudFront oggetti, ma la coerenza può aiutare a prevenire problemi quando si desidera invalidare una directory in un secondo momento. CloudFront memorizza gli URL esattamente come sono definiti, comprese le barre finali. Quindi, se il formato non è coerente, dovrai invalidare gli URL delle directory con e senza la barra, per assicurarti che la directory venga rimossa. CloudFront

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. E se ciò accade, dovrai pagare per tutte le invalidazioni, anche se esiste un solo formato per ogni URL di directory. CloudFront

Crea 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 URL firmati e cookie firmati.

Specificate un oggetto radice predefinito

Puoi CloudFront configurare la restituzione di un oggetto specifico (l'oggetto root predefinito) quando un utente richiede l'URL principale per la tua distribuzione invece di richiedere un oggetto nella tua distribuzione. La specifica di un oggetto root predefinito consente di evitare l'esposizione dei contenuti della distribuzione.

Argomenti

- Come specificare un oggetto root predefinito
- Come funziona un oggetto root predefinito
- Come CloudFront funziona se non si definisce un oggetto radice

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 completando le fasi seguenti.

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 sul nome del file, vedete la descrizione dell'`DefaultRootObject`elemento in. DistributionConfig

> **Note**
>
> Se il nome di file dell'oggetto radice predefinito è troppo lungo o contiene un carattere non valido, CloudFront restituisce l'errore. `HTTP 400 Bad Request - InvalidDefaultRootObject` Inoltre, CloudFront memorizza il codice nella cache per 10 secondi (per impostazione predefinita) e scrive i risultati nei log di accesso.

2. Verificate che le autorizzazioni per l'oggetto garantiscano CloudFront almeno l'accesso. `read`

   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 tua distribuzione per fare riferimento all'oggetto root predefinito utilizzando la CloudFront console o l' CloudFront API.

   Per specificare un oggetto root predefinito utilizzando la CloudFront console:

   a. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://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 Edit Distribution (Modifica distribuzione) nel campo Default Root Object (Oggetto root predefinito), inserire il nome file dell'oggetto root predefinito.

      Inserisci solo il nome dell'oggetto, ad esempio, `index.html`. Non aggiungere una `/` prima del nome dell'oggetto.

   e. Seleziona Salvataggio delle modifiche.

   Per aggiornare la configurazione utilizzando l' CloudFront API, è necessario specificare un valore per l'`DefaultRootObject`elemento nella distribuzione. Per informazioni sull'utilizzo dell' CloudFront API per specificare un oggetto root predefinito, UpdateDistributionconsulta Amazon CloudFront API Reference.

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. Verifica che la distribuzione sia completamente distribuita visualizzando lo stato della distribuzione nella CloudFront console.
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///`) sia 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 l'oggetto root predefinito e che CloudFront riceva una richiesta dall'utente finale per la directory inclusa nella `install` distribuzione: CloudFront

`https://d111111abcdef8.cloudfront.net/install/`

CloudFront non restituisce l'oggetto root predefinito anche se nella directory è presente una copia di`index.html`. `install`

Se configurate la distribuzione per consentire tutti i metodi HTTP CloudFront supportati, l'oggetto root predefinito si applica a tutti i metodi. Ad esempio, se l'oggetto root predefinito è index.php e si scrive l'applicazione per inviare una `POST` richiesta alla radice del dominio (https://example.com), CloudFront invia la richiesta a https://example.com/index.php.

Il comportamento degli oggetti root CloudFront predefiniti è diverso dal comportamento dei documenti 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 CloudFront distribuzione. 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 CloudFront funziona se non si definisce un oggetto radice

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 seguenti condizioni, i contenuti della tua origine sono visibili a chiunque acceda alla tua CloudFront 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 della tua origine: se configuri la tua origine come distribuzione privata (solo tu e CloudFront hai accesso), i contenuti del bucket Amazon S3 associato alla tua distribuzione sono visibili a chiunque disponga delle credenziali per accedere alla tua distribuzione. 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 URL firmati e cookie firmati”.
- `Error 403 Forbidden`— CloudFront restituisce questo errore se le autorizzazioni sul bucket Amazon S3 associato alla distribuzione o le autorizzazioni sugli oggetti in quel bucket negano l'accesso a e a tutti. CloudFront

Invalida i file per rimuovere il contenuto

Se è necessario rimuovere un file dalle cache CloudFront edge prima della scadenza, è possibile effettuare una delle seguenti operazioni:

- Invalida il file dalle edge cache. La prossima volta che un utente richiede il file, CloudFront torna all'origine per recuperare l'ultima versione del file.
- Utilizza la funzione Versioni multiple dei file per distribuire un'altra versione del file con un nome diverso. Per ulteriori informazioni, consulta Aggiorna i file esistenti utilizzando nomi di file con versioni.

Argomenti

Scegli tra l'invalidazione dei file e l'utilizzo di 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.
- CloudFront i registri di accesso includono i nomi dei file, quindi il controllo delle versioni semplifica l'analisi dei risultati delle modifiche ai 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. Il trasferimento di nuove versioni dei file CloudFront su edge location è comunque a pagamento, ma non per l'invalidazione dei file.

Per ulteriori informazioni sulla funzione Versioni multiple dei file, consulta Aggiorna i file esistenti utilizzando nomi di file con versioni.

Determina quali file 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 gli utenti non accedono necessariamente a tutti i file presenti nel file di origine, puoi determinare quali file sono stati richiesti dai visualizzatori CloudFront e invalidare solo quei file. Per determinare quali file sono stati richiesti dai visualizzatori, abilitate la registrazione degli accessi. CloudFront Per ulteriori informazioni sui log degli accessi al, consultare Configurazione e utilizzo di registri standard (registri di accesso).

Cosa devi sapere per invalidare i file

Quando specificate un file da invalidare, fate riferimento alle seguenti informazioni:

Distinzione tra lettere maiuscole e minuscole

I percorsi di invalidazione distinguono tra maiuscole e minuscole. Ad esempio, `/images/image.jpg` `/images/Image.jpg` specifica due file diversi.

Modifica dell'URI utilizzando una funzione Lambda

Se la tua CloudFront distribuzione attiva una funzione Lambda sugli eventi di richiesta del visualizzatore e se la funzione modifica l'URI del file richiesto, ti consigliamo di invalidare entrambi gli URI per rimuovere il file dalle cache edge: CloudFront

- L'URI nella richiesta del visualizzatore
- L'URI dopo la modifica eseguita dalla funzione

Example Esempio

Supponiamo che la funzione Lambda cambi l'URI di un file da:

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

A un URI che include una directory linguistica:

`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 hai configurato CloudFront per inoltrare i cookie all'origine, le cache CloudFront edge potrebbero contenere diverse versioni del file. Quando invalidi un file, CloudFront invalida ogni versione del file memorizzata nella cache indipendentemente dai cookie associati. Non puoi

selettivamente invalidare alcune versioni e non altre sulla base del cookie associati. Per ulteriori informazioni, consulta Contenuto della cache basato sui cookie.

Inoltro di intestazioni

Se hai configurato CloudFront l'inoltro di un elenco di intestazioni all'origine e la memorizzazione nella cache in base ai valori delle intestazioni, le cache CloudFront edge potrebbero contenere diverse versioni del file. Quando invalidi un file, CloudFront invalida ogni versione del file memorizzata nella cache indipendentemente dai valori dell'intestazione. Non puoi selettivamente invalidare alcune versioni e non altre sulla base dei valori delle intestazioni. (Se configuri CloudFront per inoltrare tutte le intestazioni all'origine, CloudFront non memorizza nella cache i file). Per ulteriori informazioni, consulta Contenuto della cache in base alle intestazioni delle richieste.

Inoltro di stringhe di query

Se hai configurato CloudFront per inoltrare le stringhe di query all'origine, devi includere le stringhe di query quando invalidi i file, come mostrato 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 Contenuto della cache in base ai parametri della stringa di query.

Per determinare quali stringhe di query sono in uso, è possibile abilitare la registrazione. CloudFront Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso).

Massimo consentito

Per ulteriori informazioni sul numero massimo di annullamenti consentiti, vedere. Massima richiesta di invalidamento concorrente

File Microsoft Smooth Streaming

Non puoi invalidare i file multimediali nel formato Microsoft Smooth Streaming se hai abilitato Smooth Streaming per il comportamento della 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 codificate come URL nessun altro carattere nel percorso, altrimenti la vecchia versione del file CloudFront aggiornato non verrà invalidata.

Percorsi di invalidamento

Questo percorso è relativo alla distribuzione. Ad esempio, per invalidare il file in, devi specificare. `https://d111111abcdef8.cloudfront.net/images/image2.jpg` `/images/image2.jpg`

> **Note**
>
> Nella CloudFrontconsole, puoi omettere la barra iniziale nel percorso, in questo modo:. `images/image2.jpg` Quando si utilizza direttamente l' CloudFront API, i percorsi di invalidazione 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.

Se si utilizza la AWS Command Line Interface (AWS CLI) per invalidare i file e si specifica un percorso che include il carattere `*` jolly, è necessario utilizzare le virgolette () `"` attorno al percorso, ad esempio. `"/*"`

Example Esempio: percorsi di invalidazione

- Per invalidare tutti i file in una directory:

  */directory-path/**

- Per invalidare una directory, tutte le relative sottodirectory e tutti i file nella directory e nelle 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:

  `//initial-characters-in-filenome-percorso della cartella` *

- Quando configuri la cache CloudFront in base ai parametri della stringa di query e desideri invalidare ogni versione di un file:

  *`/directory-path/file-name.file-name-extension`**

- Per invalidare tutti i file di una distribuzione:

  `/*`

  La lunghezza massima di un percorso è 4.000 caratteri. Non puoi usare un carattere jolly all'interno del percorso. Può essere aggiunto solo alla fine del percorso.

  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 CloudFront console per creare ed eseguire un'invalidazione, visualizzare un elenco delle invalidazioni inviate in precedenza e visualizzare informazioni dettagliate su una singola invalidazione. 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
- Copia, modifica ed esegui nuovamente un'invalidazione esistente
- Annulla le invalidazioni
- Elenca le invalidazioni
- Visualizza informazioni su un'invalidazione

Invalidare i file

Per invalidare i file utilizzando la CloudFront console, procedi come segue.

Console

Per invalidare i file (console)

1. Accedi a AWS Management Console e apri la CloudFront console 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 devi sapere per invalidare 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 ulteriori informazioni sull'invalidazione degli oggetti e sulla visualizzazione di informazioni sulle invalidazioni, consulta i seguenti argomenti nell'Amazon API Reference: CloudFront

- CreateInvalidation
- ListInvalidations

- GetInvalidation

> **Note**
>
> Se usi la AWS Command Line Interface (AWS CLI) per invalidare i file e specifichi un percorso che include il carattere * jolly, devi utilizzare le virgolette ('') attorno al percorso, come nell'esempio seguente:
>
> ```
> aws cloudfront create-invalidation --distribution-id distribution_ID --paths
>  "/*"
> ```

Copia, modifica ed esegui nuovamente un'invalidazione esistente

Puoi copiare un invalidamento creato precedentemente, aggiornare l'elenco dei percorsi di invalidamento ed eseguire l'invalidamento aggiornato. Non è possibile copiare un'invalidazione esistente, aggiornare i percorsi di invalidazione e quindi salvare l'invalidazione aggiornata senza eseguirla.

> **Important**
>
> Se copi un'invalidazione ancora in corso, aggiorna l'elenco dei percorsi di invalidazione, quindi esegui l'invalidazione aggiornata, senza interrompere o eliminare l'invalidazione che hai copiato. CloudFront Se nell'originale e nella copia sono presenti dei percorsi di invalidazione, cercherà di invalidare i file due volte, ed entrambe le invalidazioni CloudFront verranno conteggiate nel numero massimo di invalidamenti gratuiti per il mese. Se hai già raggiunto il numero massimo di invalidazioni gratuite, ti verranno addebitati entrambi gli invalidamenti di ciascun file. Per ulteriori informazioni, consulta Massima richiesta di invalidamento concorrente.

Per copiare, modificare e rieseguire un invalidamento esistente

1. Accedi a AWS Management Console e apri la console all'indirizzo. CloudFront 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 vuoi copiare, puoi scegliere un'invalidazione e scegliere Visualizza dettagli per visualizzare informazioni dettagliate su tale invalidazione.
5. Scegli Copia su nuovo.
6. Aggiorna l'elenco dei percorsi di invalidamento, ove applicabile.
7. Scegli Crea invalidazione.

Annulla le invalidazioni

Quando invii una richiesta di invalidazione a CloudFront, CloudFront inoltra la richiesta a tutte le edge location entro pochi secondi e ciascuna edge location inizia immediatamente a elaborare l'invalidazione. Di conseguenza, non puoi annullare una richiesta di invalidamento dopo averla inviata.

Elenca le invalidazioni

Puoi visualizzare un elenco delle ultime 100 invalidazioni che hai creato ed eseguito 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, ListInvalidationsconsulta Amazon CloudFront API Reference.

Per elencare gli invalidamenti

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://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.

Visualizza informazioni su 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 a AWS Management Console e apri la CloudFront console 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 limite massimo, viene CloudFront restituito 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.

Paga 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 viene considerato un percorso unico anche se causa l'invalidazione CloudFront di migliaia di file.

Questo valore massimo di 1000 percorsi di invalidamento gratuiti al mese è valido per il numero totale di percorsi di invalidamento per tutte le distribuzioni create con un account AWS . Ad esempio, se utilizzi il per Account AWS `john@example.com` creare tre distribuzioni e invii 600 percorsi di invalidazione per ogni distribuzione in un determinato mese (per un totale di 1.800 percorsi di invalidazione), ti AWS verranno addebitati 800 percorsi di invalidazione in quel 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 ti viene addebitato un costo per percorso, anche se raggruppi più percorsi in un'unica richiesta, ogni percorso viene comunque conteggiato individualmente ai fini della fatturazione.

Per ulteriori informazioni sui prezzi di annullamento della validità, consulta la pagina Prezzi di Amazon CloudFront . Per ulteriori informazioni sui percorsi di invalidamento, consulta Invalidation paths.

Servire file compressi

È possibile utilizzarli CloudFront per comprimere automaticamente determinati tipi di oggetti (file) e servire gli oggetti compressi quando i visualizzatori (browser Web o altri client) li supportano. I visualizzatori indicano il loro supporto per questi oggetti compressi con l'intestazione `Accept-Encoding` HTTP.

CloudFront può comprimere oggetti utilizzando i formati di compressione Gzip e Brotli. Quando il visualizzatore supporta entrambi i formati ed entrambi sono presenti nel server di cache raggiunto, preferisce Brotli. CloudFront Se nel server cache è presente un solo formato di compressione, CloudFront lo restituisce.

> **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.

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. Soprattutto per JavaScript i file CSS, i download più rapidi possono comportare un rendering più rapido delle pagine Web per gli utenti. Inoltre, poiché il costo del trasferimento dei CloudFront dati si basa sulla quantità totale di dati forniti, servire oggetti compressi può essere meno costoso che servirli non compressi.

Alcune origini personalizzate possono anche comprimere gli oggetti. La tua origine potrebbe essere in grado di comprimere oggetti che CloudFront non si comprimono (vedi). Tipi di file che CloudFront comprime Se la tua origine restituisce un oggetto compresso a CloudFront, CloudFront rileva che l'oggetto è compresso in base alla presenza di un'`Content-Encoding`intestazione e non comprime nuovamente l'oggetto.

CloudFront Configura per comprimere gli oggetti

CloudFront Per configurare la compressione degli oggetti, aggiorna il comportamento della cache in base al quale desideri utilizzare gli oggetti compressi effettuando tutte le seguenti operazioni:

1. Assicurarsi che l'impostazione Compress Objects Automatically (Comprimi oggetti automaticamente) risulti come Sì. (In AWS CloudFormation o nell' CloudFront API, impostato su`Compress`.) `true`
2. Usare una policy di cache per specificare le impostazioni di memorizzazione nella cache e verificare che le impostazioni Gzip e Brotli siano entrambe abilitate. (Nella AWS CloudFormation o nell' CloudFrontAPI, imposta `EnableAcceptEncodingGzip` e `EnableAcceptEncodingBrotli` su`true`.)
3. Verificare che i valori TTL nella policy cache siano impostati su un valore superiore a zero. Quando impostate i valori TTL su zero, la memorizzazione nella cache è disabilitata e CloudFront non comprime gli oggetti.

Per aggiornare un comportamento della cache, è possibile utilizzare uno dei seguenti strumenti:

- La console CloudFront
- AWS CloudFormation
- Gli SDK AWS e gli strumenti della riga di comando

Come funziona CloudFront la compressione

Quando CloudFront configuri per comprimere gli oggetti (vedi la sezione precedente), ecco come funziona:

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 sia Gzip che Brotli, preferisce Brotli. CloudFront

> **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.

2. Nella posizione periferica, CloudFront verifica la presenza di una copia compressa dell'oggetto richiesto nella cache.
3. Se l'oggetto compresso è già presente nella cache, lo CloudFront invia al visualizzatore e salta i passaggi rimanenti.

   Se l'oggetto compresso non è 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 accadere quando CloudFront in precedenza si è saltata la compressione. Quando ciò accade, CloudFront memorizza nella cache l'oggetto non compresso e continua a utilizzarlo fino alla scadenza, all'eliminazione o all'invalidazione dell'oggetto.

4. Se l'origine restituisce un oggetto compresso, come indicato dalla presenza di un'`Content-Encoding`intestazione nella risposta HTTP, CloudFront invia l'oggetto compresso al visualizzatore, lo aggiunge alla cache e salta il passaggio rimanente. CloudFront non comprime nuovamente l'oggetto.

   Se l'origine restituisce un oggetto non compresso a CloudFront (non c'è un'`Content-Encoding`intestazione nella risposta HTTP), CloudFront determina se l'oggetto è comprimibile. Per ulteriori informazioni su come CloudFront determina se un oggetto è comprimibile, consultate la sezione seguente.
5. Se l'oggetto è comprimibile, lo CloudFront comprime, lo invia al visualizzatore e lo aggiunge alla cache. (In rari casi, CloudFront potrebbe saltare la compressione e inviare l'oggetto non compresso al visualizzatore.)

Quando comprime gli oggetti CloudFront

L'elenco seguente fornisce ulteriori informazioni su quando CloudFront comprime gli oggetti.

La richiesta utilizza HTTP 1.0

Se una richiesta CloudFront utilizza HTTP 1.0, CloudFront rimuove l'`Accept-Encoding`intestazione e non comprime l'oggetto nella risposta.

Intestazione della richiesta **`Accept-Encoding`**

Se l'`Accept-Encoding`intestazione non è presente nella richiesta del visualizzatore o se non contiene `gzip` o `br` non è un valore, CloudFront non comprime l'oggetto nella risposta. Se l'`Accept-Encoding`intestazione include valori aggiuntivi, ad esempio`deflate`, li CloudFront rimuove prima di inoltrare la richiesta all'origine.

Quando CloudFront è configurato per comprimere gli oggetti, include automaticamente l'`Accept-Encoding`intestazione nella chiave della cache e nelle richieste di origine.

Contenuti dinamici

CloudFront non sempre comprime i contenuti dinamici. Le risposte per i contenuti dinamici a volte vengono compresse mentre altre volte no.

Il contenuto viene già memorizzato nella cache quando si configura la compressione degli CloudFront oggetti

CloudFront comprime gli oggetti quando li recupera dall'origine. Quando si configura CloudFront per comprimere oggetti, CloudFront non comprime gli oggetti che sono già memorizzati nella cache nelle posizioni laterali. Inoltre, quando un oggetto memorizzato nella cache scade in una posizione CloudFront periferica e inoltra un'altra richiesta per l'oggetto all'origine, CloudFront non comprime l'oggetto quando l'origine restituisce un codice di stato HTTP 304, il che significa che l'edge location ha già la versione più recente dell'oggetto. Se desiderate CloudFront comprimere oggetti che sono già memorizzati nella cache in posizioni periferiche, dovete invalidare tali oggetti. Per ulteriori informazioni, consulta Invalida i file per rimuovere il contenuto.

L'origine è già configurata per comprimere gli oggetti

Se configurate CloudFront per comprimere oggetti e l'origine comprime anche gli oggetti, l'origine deve includere un'`Content-Encoding`intestazione, che indichi che l'oggetto è già compresso. CloudFront Quando una risposta proveniente da un'origine include l'`Content-Encoding`intestazione, CloudFront non comprime l'oggetto, indipendentemente dal valore

dell'intestazione. CloudFront invia la risposta al visualizzatore e memorizza l'oggetto nella cache nella posizione del bordo.

Tipi di file che comprimono CloudFront

Per un elenco completo dei tipi di file CloudFront compressi, vedere. Tipi di file che CloudFront comprime

Dimensioni degli oggetti che si comprimono CloudFront

CloudFront comprime oggetti di dimensioni comprese tra 1.000 e 10.000.000 di byte.

`Content-Length` Intestazione

L'origine deve includere un'`Content-Length`intestazione nella risposta, che viene CloudFront utilizzata per determinare se la dimensione dell'oggetto rientra nell'intervallo di compressione. CloudFront Se l'`Content-Length`intestazione è mancante, contiene un valore non valido o contiene un valore che non rientra nell'intervallo di dimensioni, la compressione CloudFront non comporta la CloudFront compressione dell'oggetto.

Il codice di stato HTTP per la risposta

CloudFront comprime gli oggetti solo quando il codice di stato HTTP della risposta è, o. `200` `403` `404`

La risposta non ha corpo

Quando la risposta HTTP dall'origine non ha un corpo, non c'è nulla CloudFront da comprimere.

`ETag` Intestazione

CloudFront a volte modifica l'`ETag`intestazione nella risposta HTTP quando comprime gli oggetti. Per ulteriori informazioni, consulta the section called “Conversione dell'intestazione `ETag`”.

CloudFront salta la compressione

CloudFront comprime gli oggetti nel miglior modo possibile. In rari casi, CloudFront salta la compressione. CloudFront prende questa decisione in base a una serie di fattori, inclusa la capacità dell'host. Se CloudFront salta la compressione di un oggetto, memorizza nella cache l'oggetto non compresso e continua a mostrarlo ai visualizzatori fino alla scadenza, all'eliminazione o all'invalidazione dell'oggetto.

Tipi di file che CloudFront comprime

Se configurate CloudFront per comprimere oggetti, comprime CloudFront solo gli oggetti che hanno uno dei 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

Conversione dell'intestazione **ETag**

Quando l'oggetto non compresso dall'origine include un'intestazione ETag HTTP valida e forte e CloudFront comprime l'oggetto, converte CloudFront anche il valore di ETag intestazione forte in debole e restituisce il valore debole ETag al visualizzatore. ETag 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 e all'origine di trattare le versioni compresse e non compresse di un oggetto come semanticamente equivalenti, il che riduce il trasferimento di dati non necessario. CloudFront

Un valore di intestazione `ETag` valido e consolidato inizia con un carattere di virgoletta doppia (`"`). Per convertire il `ETag` valore forte in uno debole, CloudFront aggiunge i caratteri `W/` all'inizio del valore forte. `ETag`

Quando l'oggetto di origine include un valore di `ETag` intestazione debole (un valore che inizia con i caratteri`W/`), CloudFront non modifica questo valore e lo restituisce al visualizzatore così come ricevuto dall'origine.

Quando l'oggetto di origine include un valore di `ETag` intestazione non valido (il valore non inizia con `"` o con`W/`), CloudFront rimuove l'`ETag`intestazione 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)
- Intestazione HTTP `If-None-Match`

Usa AWS WAF protezioni

È possibile utilizzarlo AWS WAFper proteggere le CloudFront distribuzioni e i server di origine. AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API bloccando le richieste prima che raggiungano i server. Per ulteriori dettagli, consulta Accelerare e proteggere i siti Web utilizzando CloudFront e AWS WAF.

Per abilitare AWS WAF le protezioni, puoi:

- Usa la protezione con un clic nella CloudFront console. La protezione con un clic crea un AWS WAF elenco di controllo degli accessi Web (Web ACL), configura le regole per proteggere i server dalle minacce Web comuni e collega l'ACL Web alla distribuzione per te. CloudFront 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 AWS WAF console o utilizzando le API. AWS WAF Per ulteriori informazioni, consulta gli elenchi di controllo degli accessi Web (ACL) nella Guida per gli AWS WAF sviluppatori e AssociateWebACL nell'API Reference AWS WAF

Puoi abilitarlo 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 AWS consigliato 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 le metriche di sicurezza nella dashboard di sicurezza. CloudFront Se non è abilitata AWS WAF, puoi utilizzare la

dashboard di sicurezza solo per abilitare AWS WAF o configurare le restrizioni CloudFront geografiche. Per ulteriori informazioni sulla dashboard, consulta Gestisci le protezioni di AWS WAF sicurezza nella dashboard CloudFront di sicurezza, più avanti in questa sezione.

Argomenti

Abilita AWS WAF per le distribuzioni

È possibile abilitare AWS WAF quando si crea una distribuzione oppure è possibile abilitare le protezioni di sicurezza per una lista di controllo degli accessi (ACL) esistente.

Se abiliti AWS WAF la CloudFront distribuzione, puoi anche abilitare il controllo dei bot e configurare la protezione di sicurezza per categoria di bot.

Argomenti

Abilita AWS WAF per una nuova distribuzione

La procedura seguente mostra come abilitare AWS WAF quando si crea una nuova CloudFront distribuzione.

AWS WAF Per abilitare una nuova distribuzione

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi scegli Crea distribuzione.

3. Se necessario, segui i passaggi indicati in Creazione di una distribuzione.
4. Nella sezione Web Application Firewall, scegli Modifica, quindi scegli Abilita protezioni di sicurezza.
5. Completare i seguenti campi:

   - Usa la modalità di monitoraggio: abiliti la modalità di monitoraggio quando desideri raccogliere dati per la prima volta 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. Controlla le impostazioni di distribuzione rimanenti, quindi scegli Crea distribuzione.

Dopo aver creato una distribuzione, CloudFront crea una dashboard di sicurezza. È possibile utilizzare questa dashboard per disabilitare o abilitare AWS WAF. Se non l'hai AWS WAF ancora abilitato, i diagrammi e i grafici 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

Per utilizzare una configurazione esistente AWS WAF

1. Apri la CloudFront console all'indirizzohttps://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 scegli la scheda Sicurezza.
3. Nella sezione Web Application Firewall (WAF), scegli Modifica, quindi Abilita 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. Controlla le impostazioni di distribuzione rimanenti, quindi scegli Crea distribuzione.

Abilita il controllo dei bot

Se AWS WAF abiliti la CloudFront distribuzione, puoi visualizzare le richieste dei bot per un determinato intervallo di tempo nella dashboard di sicurezza della CloudFront console. Puoi anche abilitare o disabilitare il controllo dei bot qui.

Quando abiliti il controllo dei bot, ti vengono addebitati dei costi. La dashboard di sicurezza fornisce una stima dei costi.

Se abiliti il controllo dei bot, la dashboard di sicurezza mostra il traffico dei bot per ogni tipo e categoria di bot. Se disabiliti il controllo dei bot, il traffico dei bot viene visualizzato in base al campionamento delle richieste.

Per abilitare il Rilevamento dei bot

1. Apri la CloudFront console all'indirizzohttps://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 Bot Control, in Configurazione, seleziona la casella di controllo Abilita il controllo dei bot per i bot comuni.
6. Seleziona Salvataggio delle modifiche.

Configura la protezione per categoria di bot

Quando abiliti il controllo 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 Monitor e assegnare una sfida a un link checker.

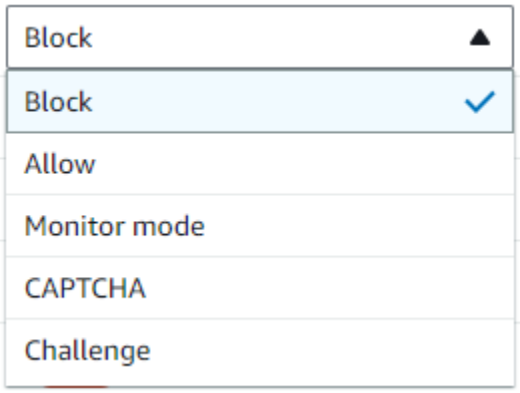
> **Note**
>
> I bot noti AWS per essere comuni e verificabili, come i crawler dei motori di ricerca noti, non sono soggetti alle azioni che hai impostato qui. Il Rilevamento dei bot conferma che i bot convalidati provengono dalla fonte dichiarata prima di contrassegnarli come verificati.

Per configurare la protezione per una categoria di bot

1. Apri la CloudFront console all'indirizzohttps://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 di modifica.

5. Apri l'elenco ottenuto e scegli uno dei seguenti modi:

   - Blocco
   - Abilita
   - Modalità monitorata
   - CAPTCHA
   - Challenge



6. Seleziona il segno di spunta accanto all'elenco per confermare la modifica.

Gestisci le protezioni di AWS WAF sicurezza nella dashboard CloudFront di sicurezza

CloudFront crea una dashboard di sicurezza per ciascuna delle tue distribuzioni. Utilizzi i dashboard della CloudFront console. Con i dashboard, puoi utilizzarli AWS WAF insieme in un'unica posizione per monitorare CloudFront e gestire le protezioni di sicurezza comuni per le tue applicazioni web. Le dashboard forniscono le seguenti attività e dati:

- Configurazione della sicurezza: puoi abilitare e disabilitare le protezioni e visualizzare tutte AWS WAF le protezioni specifiche dell'app, ad esempio le protezioni. WordPress
- Tendenze in materia di sicurezza: includono richieste consentite e bloccate, richieste di sfida 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 di bot: puoi vedere quanto traffico proviene dai bot, 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'attivazione del controllo dei bot, consulta. Abilita il controllo dei bot
- Registri delle richieste: i dati di registro 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 Abilitare AWS WAF i log.
- Gestione delle restrizioni geografiche CloudFront e AWS WAF fornitura di funzionalità di restrizione geografica. CloudFront fornisce restrizioni geografiche gratuitamente, ma le metriche relative alle restrizioni CloudFront geografiche non vengono visualizzate nella dashboard di sicurezza. Per visualizzare le metriche relative alle richieste relative ai Paesi bloccati, devi utilizzare le restrizioni AWS WAF geografiche. A tale scopo, posiziona il mouse su una barra del paese nella dashboard di sicurezza e blocca il Paese. Per ulteriori informazioni, consulta Usa le restrizioni CloudFront geografiche.

- L'opzione Blocca potrebbe non essere disponibile se in precedenza hai creato una AWS WAF regola personalizzata all'esterno della CloudFront console per bloccare i paesi.

Argomenti

Prerequisiti

È necessario AWS WAF abilitarla se si desidera visualizzare le metriche di sicurezza nella dashboard CloudFront di sicurezza. Se non lo abiliti AWS WAF, puoi utilizzare la dashboard di sicurezza solo per abilitare AWS WAF o configurare le restrizioni CloudFront geografiche.

Per ulteriori informazioni sull'attivazione AWS WAF, consultaAbilita AWS WAF per le distribuzioni.

Abilitare AWS WAF i log

AWS WAF i dati di registro 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 AWS WAF la registrazione a CloudWatch, la dashboard CloudFront di sicurezza interroga, aggrega e visualizza le informazioni ricavate dai log. CloudWatch Non addebitiamo costi per l'utilizzo della dashboard di sicurezza, ma CloudWatch i prezzi si applicano ai log interrogati tramite la dashboard. Per ulteriori informazioni, consulta la pagina CloudWatch dei prezzi di Amazon.

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 AWS WAF i registri.
3. Scegli Abilita .

CloudFront crea un gruppo di CloudWatch log e aggiorna la AWS WAF configurazione a cui iniziare la registrazione. 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 AWS WAF richieste elaborate per quella 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 monitor. Quando la modalità monitor è abilitata, CloudFront acquisisce metriche che indicano se la velocità configurata nel campo Limitazione della velocità è stata superata, con quale frequenza e di quanto.

Dopo aver salvato la distribuzione, CloudFront inizia a raccogliere dati in base al numero nel campo Rate limiting.

È possibile gestire le impostazioni di limitazione della velocità nella sezione Sicurezza - Web Application Firewall (WAF) della scheda Sicurezza di qualsiasi distribuzione. CloudFront

Per impostare la limitazione della velocità

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi scegli la distribuzione che desideri modificare.
3. Scegliere la scheda Sicurezza .
4. Nella sezione Web Application Firewall (WAF), accanto a Rate limiting, scegli il messaggio in modalità Monitor per visualizzare una finestra di dialogo con i dettagli sui dati raccolti. Facoltativamente, puoi modificare il limite di velocità. Dopo aver regolato con precisione la velocità, puoi scegliere Abilita blocco (nella finestra di dialogo) per disattivare la modalità monitor. CloudFront inizierà a bloccare le richieste che superano il limite di velocità specificato.

Disattiva le protezioni AWS WAF di sicurezza

Se la tua distribuzione non necessita AWS WAF di protezioni di sicurezza, puoi disabilitare questa funzionalità utilizzando la CloudFront console.

Se in precedenza hai abilitato AWS WAF la protezione e non hai scelto una configurazione WAF esistente (nota anche come protezione con un clic), hai creato CloudFront automaticamente un ACL web per te. Per gli ACL Web creati in questo modo, la CloudFront console dissocierà la risorsa ed eliminerà l'ACL Web.

Dissociare un ACL Web è diverso dall'eliminarlo. La dissociazione rimuove l'ACL Web dalla tua distribuzione, ma non viene eliminato dalla tua. Account AWSPer ulteriori informazioni, consulta Associare o dissociare un ACL Web con una AWS risorsa nella, and Developer Guide.AWS WAF AWS Firewall Manager AWS Shield Advanced

Consultate la seguente procedura per disabilitare AWS WAF le protezioni e dissociare l'ACL Web dalla distribuzione.

Per disabilitare le protezioni di sicurezza AWS WAF in CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Distribuzioni, quindi scegli la distribuzione che desideri modificare.
3. Scegli la scheda Sicurezza, quindi scegli Modifica.
4. Nella sezione Web Application Firewall (WAF), scegli Disabilita AWS WAF protezione.
5. Seleziona Salvataggio delle modifiche.

> **Note**
>
> - Se hai disabilitato la protezione di AWS WAF sicurezza e desideri comunque eliminare l'ACL Web dal tuo Account AWS, puoi eliminarlo manualmente. Segui la procedura per eliminare un ACL web. Nella console AWS WAF & Shield, per la pagina Web ACL, devi scegliere l'elenco Global (CloudFront) per trovare gli ACL web.
> - Quando elimini una distribuzione dalla CloudFront console, CloudFront tenterà di eliminare anche l'ACL web se hai scelto la protezione con un clic. Questo è il massimo sforzo e non è sempre garantito. Per ulteriori informazioni, consulta Eliminazione di una distribuzione .

Configura l'accesso sicuro e limita l'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 URL CloudFront firmati o cookie firmati
- Impostare la crittografia a livello di campo per campi di contenuti specifici
- Utilizzalo AWS WAF per controllare l'accesso ai tuoi contenuti

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 Qui c'è una negoziazione SSL/TLS tra il visualizzatore 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

Per informazioni su come richiedere HTTPS tra i visualizzatori e tra i destinatari e tra i destinatari CloudFront, consulta i seguenti argomenti. CloudFront

Argomenti

- Richiedi HTTPS per la comunicazione tra gli spettatori e CloudFront
- Richiedi HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata
- Richiedi HTTPS per la comunicazione tra CloudFront e la tua origine Amazon S3
- Protocolli e cifrari supportati tra visualizzatori e CloudFront
- Protocolli e cifrari supportati tra CloudFront e l'origine

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. Le fasi di configurazione variano in base al nome di dominio utilizzato negli URL degli oggetti:

- 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 CloudFront impostazioni. È inoltre necessario utilizzare un certificato SSL/TLS fornito da AWS Certificate Manager (ACM) o importare un certificato da un'autorità di certificazione di terze parti in ACM o nello store certificati IAM. Per ulteriori informazioni, consulta Usa nomi di dominio alternativi e HTTPS.

> **Note**
>
> Se vuoi assicurarti che gli oggetti da cui gli utenti ottengono 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 Aggiungere, rimuovere o sostituire i contenuti CloudFront distribuiti.

Richiedi HTTPS per gli spettatori

Per richiedere HTTPS tra i visualizzatori e CloudFront per uno o più comportamenti della cache, esegui la procedura seguente.

Per configurare la richiesta CloudFront di HTTPS tra i visualizzatori e CloudFront

1. Accedi a AWS Management Console 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 della cache che desideri aggiornare, quindi scegli Modifica.
4. Specificate uno dei seguenti valori per la politica del protocollo Viewer:

   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 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 riguarda solo la richiesta e le intestazioni che CloudFront restituiscono 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 (Proibito) e non restituisce l'oggetto.

5. Seleziona Salvataggio delle 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 certificato SSL/TLS sul tuo server di origine (non è necessario quando utilizzi un'origine Amazon S3 o altre origini). AWS

Argomenti

Richiedi HTTPS per le origini personalizzate

La procedura seguente spiega come configurare l'uso di HTTPS CloudFront per comunicare con un sistema di bilanciamento del carico Elastic Load Balancing, un'istanza Amazon EC2 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 AWS Management Console 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 l'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 protocollo SSLv3 è meno sicuro, perciò ti consigliamo di scegliere SSLv3 solo se il server di origine non supporta TLSv1 o versioni successive. L'handshake TLSv1 è compatibile sia con le versioni precedenti che successive con SSLv3, ma TLSv1.1 e versioni successive no. Quando scegli SSLv3, invia solo richieste di handshake SSLv3. CloudFront

5. Seleziona Salvataggio delle modifiche.
6. Ripeti i passaggi da 3 a 5 per ogni origine aggiuntiva per cui desideri richiedere HTTPS tra e l'origine personalizzata. 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 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 certificato SSL/TLS sulla tua origine personalizzata

Puoi utilizzare un certificato SSL/TLS dalle seguenti origini sul server di origine personalizzato:

- Se l'origine è un sistema di bilanciamento del carico (load balancer) Elastic Load Balancing, 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 Elastic Load Balancing, è necessario utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti affidabile, 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, inoltra CloudFront sempre 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.

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 utilizzi HTTPS con un bucket Amazon S3 che supporta la comunicazione HTTPS, Amazon S3 offre automaticamente il certificato SSL/TLS.

Richiedi 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 AWS Management Console 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 reindirizzaDELETE, 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 alle PUT richieste relative a tale comportamento nella cache con il codice di stato HTTP 403 (Proibito).

   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 riguarda solo la richiesta e le intestazioni che CloudFront restituiscono 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 protocollo SSL/TLS 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 Politica 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_26	TLSv1.1_016	TLSv1.2_018	TLSv1.2_019	TLSv1.2_2021
Protocolli SSL/TLS supportati							
TLSv1.3	♦	♦	♦	♦	♦	♦	♦
TLSv1.2	♦	♦	♦	♦	♦	♦	♦
TLSv1.1	♦	♦	♦	♦			
TLSv1	♦	♦	♦				
SSLv3	♦						
Cifrari TLSv1.3 supportati							
TLS_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦
TLS_CHACHA20_POLY1305_SHA256	♦	♦	♦	♦	♦	♦	♦
Crittografie ECDSA supportate							
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES128-SHA	♦	♦	♦	♦			

	Policy di sicurezza						
	SSLv3	TLSv1	TLSv1_26	TLSv1.1_016	TLSv1.2_018	TLSv1.2_019	TLSv1.2_2021
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES256-SHA	♦	♦	♦	♦			
Crittografie RSA supportate							
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES128-SHA	♦	♦	♦	♦			
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦			

	Policy di sicurezza						
	SSLv3	TLSv1	TLSv1_26	TLSv1.1_016	TLSv1.2_018	TLSv1.2_019	TLSv1.2_2021
AES128-GCM-SHA256	♦	♦	♦	♦	♦		
AES256-GCM-SHA384	♦	♦	♦	♦	♦		
AES128-SHA256	♦	♦	♦	♦	♦		
AES256-SHA	♦	♦	♦	♦			
AES128-SHA	♦	♦	♦	♦			
DES-CBC3-SHA	♦	♦					
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.

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
Cifrari TLSv1.3 supportati	
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
Crittografie ECDSA supportate	
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Crittografie RSA supportate	
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schemi di firma supportati tra spettatori e CloudFront

CloudFront supporta i seguenti schemi di firma per le connessioni tra spettatori e. CloudFront

- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA512

- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SHA384
- TLS_SIGNATURE_SCHEME_ECDSA_SHA512
- TLS_SIGNATURE_SCHEME_ECDSA_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SECP256R1_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SECP384R1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1
- TLS_SIGNATURE_SCHEME_ECDSA_SHA1

Protocolli e cifrari supportati tra CloudFront e l'origine

Se scegli di richiedere HTTPS tra CloudFront e la tua origine, puoi decidere quale protocollo SSL/TLS 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 all'origine. CloudFront

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	

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
Crittografie RSA supportate	
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Nome cifrato OpenSSL e s2n	Nome crittografia RFC
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schemi di CloudFront firma supportati tra e l'origine

CloudFront supporta i seguenti schemi di firma per le connessioni tra CloudFront e l'origine.

- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SHA384
- TLS_SIGNATURE_SCHEME_ECDSA_SHA512
- TLS_SIGNATURE_SCHEME_ECDSA_SHA224
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1
- TLS_SIGNATURE_SCHEME_ECDSA_SHA1

Usa nomi di dominio alternativi e HTTPS

Se desideri utilizzare il nome di dominio negli URL per i tuoi file (ad esempio `https://www.example.com/image.jpg`) e desideri che i visualizzatori utilizzino HTTPS, devi completare le fasi descritte nei seguenti argomenti. (Se utilizzi il nome di dominio di CloudFront distribuzione predefinito nei tuoi URL, ad esempio`https://d111111abcdef8.cloudfront.net/image.jpg`, segui invece le indicazioni 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 diventano disponibili nuove edge location, CloudFront propaga il certificato anche a tali postazioni. 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

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.

Usa SNI per soddisfare 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 per il nome di dominio è determinato durante la negoziazione handshake SSL/TLS (l'indirizzo IP non è dedicato alla tua distribuzione).

La negoziazione SSL/TLS avviene quasi immediatamente nel processo di stabilire 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 benvenuto del client TLS.
2. Quando CloudFront riceve il messaggio di saluto del 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 Utilizza un indirizzo IP dedicato per soddisfare le richieste HTTPS (funziona per tutti i client).
- Utilizza il certificato CloudFront SSL/TLS anziché un certificato personalizzato. Ciò richiede l'utilizzo del nome di CloudFront dominio per la distribuzione negli URL dei file, ad esempio. `https://d111111abcdef8.cloudfront.net/logo.png`

  Se utilizzi il CloudFront certificato predefinito, gli utenti devono supportare il protocollo SSL TLSv1 o successivo. CloudFront non supporta SSLv3 con il certificato predefinito. CloudFront

  È inoltre necessario modificare il certificato SSL/TLS utilizzato da un certificato personalizzato CloudFront a un certificato predefinito: CloudFront

  - 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 gli URL dei file 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.

Utilizza un indirizzo IP dedicato per soddisfare 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 servire le richieste HTTPS utilizzando indirizzi IP dedicati, dovrai sostenere un costo mensile aggiuntivo. L'addebito inizia quando associ il certificato SSL/TLS a una distribuzione e abiliti 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 eseguono la negoziazione SSL/TLS 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.

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, esegui la procedura seguente. CloudFront 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 certificato SSL/TLS a una CloudFront distribuzione alla volta. Questo numero indica il numero totale di certificati SSL IP dedicati che puoi utilizzare in tutte le tue distribuzioni. CloudFront

Per richiedere l'autorizzazione a utilizzare 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 dei certificati SSL/TLS con CloudFront

I requisiti per i certificati SSL/TLS 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

È consigliabile 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 CloudFront, assicurati di richiedere (o importare) il certificato nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

CloudFront supporta le stesse autorità di certificazione (CA) di Mozilla, quindi se non usi ACM, usa un certificato emesso da una CA presente nell'elenco dei certificati CA inclusi di 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 HTTPS tra CloudFront e la tua origine e utilizzi un sistema di bilanciamento del carico in Elastic Load Balancing 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 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 CloudFront e l'origine”

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.

Autorizzazioni

È necessario disporre dell'autorizzazione per utilizzare e importare il certificato SSL/TLS. 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

Tieni presente 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 con. CloudFront

Per informazioni su come stabilire le dimensioni di una chiave RSA, consulta Determina la dimensione della chiave pubblica in un certificato RSA SSL/TLS.

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.

Se usi certificati forniti da ACM, ACM gestisce i rinnovi dei certificati senza alcun intervento da parte tua. 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 certificato SSL/TLS sull'origine include un nome di dominio nel campo Nome comune e, possibilmente, altri nomi nel campo Nomi alternativi soggetto. (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 del protocollo SSL/TLS

Se utilizzi indirizzi IP dedicati, imposta la versione minima del protocollo SSL/TLS per la connessione tra i visualizzatori e scegli una politica di sicurezza. CloudFront

Per ulteriori informazioni, consulta Politica di sicurezza (versione minima SSL/TLS) nell'argomento Riferimento alle 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 dei certificati SSL/TLS con CloudFront (HTTPS solo tra i visualizzatori e solo tra i visualizzatori) CloudFront

Nota le seguenti quote sull'utilizzo dei certificati SSL/TLS con. CloudFront Queste quote si applicano solo ai certificati SSL/TLS 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 Aumenta le quote per i certificati SSL/TLS.

CloudFront Numero massimo di certificati per distribuzione

È possibile associare un massimo di un certificato SSL/TLS a ciascuna distribuzione. CloudFront

Numero massimo di certificati che puoi importare in ACM o caricare nello store certificati IAM

Se hai ricevuto i certificati SSL/TLS da un'autorità di certificazione di terza parte, è necessario archiviare i certificati in uno dei seguenti percorsi:

- 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 una quota più elevata nella AWS Management Console.

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 certificati SSL/TLS personalizzati per il tuo AWS account, vai al Support Center e crea un caso. Indica il numero di certificati per cui hai bisogno dell'autorizzazione all'utilizzo e descrivi le circostanze nella tua richiesta. Aggiorneremo il tuo account appena possibile.

Usa lo stesso certificato per le CloudFront 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

Puoi utilizzare lo stesso certificato per una o tutte le CloudFront distribuzioni che utilizzi per soddisfare le richieste HTTPS. Tieni 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 le 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.

Configura nomi di dominio alternativi e HTTPS

Per utilizzare nomi di dominio alternativi negli URL dei file e utilizzare HTTPS tra i visualizzatori CloudFront, esegui le procedure applicabili.

Argomenti

- Ottieni un certificato SSL/TLS
- Importa un certificato SSL/TLS
- Aggiorna la tua CloudFront distribuzione

Ottieni un certificato SSL/TLS

Ricevi un certificato SSL/TLS se non ne hai già uno. Per ulteriori informazioni, consulta la documentazione relativo:

- Per utilizzare un certificato fornito da AWS Certificate Manager (ACM), consulta la Guida per l'utente.AWS Certificate Manager Quindi passa a Aggiorna la tua CloudFront distribuzione.

> **Note**
>
> Ti consigliamo di utilizzare ACM per effettuare il provisioning, gestire e distribuire certificati SSL/TLS su risorse gestite AWS . 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.

Importa 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/
```

Tieni 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 AWS Management Console 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)

   Scegli 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 Importa un certificato SSL/TLS per avere la conferma del suo corretto caricamento.

   > **Important**
   >
   > Dopo aver associato il certificato SSL/TLS alla CloudFront distribuzione, non eliminare il certificato da ACM o dall'archivio certificati IAM finché non lo rimuovi da tutte le distribuzioni e tutte le distribuzioni non sono state distribuite.

5. Seleziona Salvataggio delle modifiche.

6. Configura per richiedere HTTPS tra i visualizzatori e: CloudFront 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 reindirizzate automaticamente alle richieste HTTPS. CloudFrontrestituisce il codice di stato HTTP `301 (Moved Permanently)` 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 `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 riguarda solo la richiesta e le intestazioni che CloudFront restituiscono 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 i passaggi da a c per ogni comportamento aggiuntivo nella cache per cui desideri richiedere HTTPS tra i visualizzatori eCloudFront.

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.

Determina la dimensione della chiave pubblica in un certificato RSA SSL/TLS

Quando utilizzi nomi di dominio CloudFront alternativi e HTTPS, la dimensione massima della chiave pubblica in un certificato RSA SSL/TLS 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 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)
```

Aumenta le quote per i certificati SSL/TLS

Sono previste quote sul numero di certificati SSL/TLS che puoi importare in AWS Certificate Manager (ACM) o caricare su (IAM). AWS Identity and Access Management Esiste anche una quota sul

numero di certificati SSL/TLS che è possibile utilizzare con e Account AWS quando si configura CloudFront per servire le richieste HTTPS utilizzando indirizzi IP dedicati. Tuttavia, puoi richiedere quote più elevate.

Argomenti

Aumenta la quota per i 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 superiore, crea un ticket nella console del Centro assistenza. Specifica i seguenti valori:

- Accetta il valore predefinito in Service Limit Increase (Incremento limiti servizio).
- Per Limit type (Tipo di limite), seleziona Certificate Manager.
- Per Regione, scegli la AWS regione in cui desideri importare i certificati.
- Per Limit (Limite), seleziona Number of ACM Certificates (Numero di certificati ACM)

Quindi compila il resto del modulo e invialo.

Aumenta la quota di 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 superiore, crea un ticket nella console del Centro assistenza. Specifica i seguenti valori:

- Accetta il valore predefinito in Service Limit Increase (Incremento limiti servizio).
- Per Limit type (Tipo di limite), seleziona Certificate Manager.
- Per Regione, scegli la AWS regione in cui desideri importare i certificati.
- Per Limit (Limite), seleziona Server Certificate Limit IAM (Limite certificati server IAM).

Quindi compila il resto del modulo e invialo.

Aumenta la quota di certificati utilizzati con indirizzi IP dedicati

Per la quota relativa al numero di certificati SSL che è possibile utilizzare per ciascuno di essi Account AWS quando si gestiscono richieste HTTPS utilizzando indirizzi IP dedicati, vedereQuote sui certificati SSL.

Per richiedere una quota superiore, crea un ticket nella console del Centro assistenza. Specifica i seguenti valori:

- Accetta il valore predefinito in Service Limit Increase (Incremento limiti servizio).
- Per Tipo di limite, scegli CloudFrontDistribuzioni.
- Per Limit (Limite), scegli Dedicated IP SSL Certificate Limit per Account (Limite certificati SSL con IP dedicati per account).

Quindi compila il resto del modulo e invialo.

Ruota i certificati SSL/TLS

Se utilizzi certificati forniti da AWS Certificate Manager (ACM), non è necessario ruotare i certificati SSL/TLS. ACM gestisce i rinnovi dei certificati per te. Per ulteriori informazioni, consulta Rinnovo gestito nella Guida per l'utente di AWS Certificate Manager .

> **Note**
>
> ACM non gestisce i rinnovi di certificati acquisiti da autorità di certificazione di terze parti e importati in ACM.

Se stai utilizzando un'autorità di certificazione di terza parte e hai importato i certificati in ACM (consigliato) o li hai caricati nello store certificati IAM, dovrai occasionalmente sostituire un certificato con un altro. Ad esempio, devi sostituire un certificato quando si avvicina la data di scadenza del certificato.

> **Important**
>
> Se sei configurato CloudFront per soddisfare le richieste HTTPS utilizzando indirizzi IP dedicati, potresti incorrere in un costo aggiuntivo, ripartito proporzionalmente, per l'utilizzo di

uno o più certificati aggiuntivi durante la rotazione dei certificati. Ti consigliamo di aggiornare le distribuzioni al più presto 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. Aumenta le quote per i 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 certificato SSL/TLS nella Amazon Developer Guide. CloudFront
3. Aggiorna le distribuzioni una alla volta per utilizzare il nuovo certificato. Per ulteriori informazioni, consulta Elencare, visualizzare e aggiornare CloudFront le distribuzioni nell'Amazon CloudFront Developer Guide.
4. (Facoltativo) Dopo aver aggiornato tutte le CloudFront distribuzioni, puoi eliminare il vecchio certificato da ACM o da IAM.

> **Important**
>
> Non eliminare un certificato SSL/TLS finché non lo avrai rimosso da tutte le distribuzioni e finché lo stato delle distribuzioni che hai aggiornato non è cambiato in `Deployed`.

Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront

Se hai configurato l'uso CloudFront di HTTPS tra i visualizzatori e CloudFront hai configurato CloudFront per utilizzare un certificato SSL/TLS personalizzato, puoi modificare la configurazione per utilizzare il certificato SSL/TLS predefinito. CloudFront 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 gli URL dei file 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 ripristinare un certificato SSL/TLS personalizzato al certificato predefinito. CloudFront

Per tornare al certificato predefinito CloudFront

1. Crea una nuova CloudFront distribuzione con la configurazione desiderata. Per il certificato SSL, scegli Certificato predefinito (CloudFront*.cloudfront.net).

   Per ulteriori informazioni, consulta Creazione di una distribuzione.
2. Per i file che distribuisci utilizzando CloudFront, aggiorna gli URL dell'applicazione in modo da utilizzare il nome di dominio assegnato alla nuova distribuzione. CloudFront 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**
   >
   > Fino al completamento di questo passaggio, continua ad addebitarti i costi per l'utilizzo di un certificato SSL/TLS personalizzato AWS .
4. (Facoltativo) Elimina il certificato SSL/TLS 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-certificatesla sezione AWS CLI Command Reference.

   b. Esegui il AWS CLI comando `delete-server-certificate` per eliminare il certificato. Per ulteriori informazioni, vedere delete-server-certificatenel AWS CLI Command Reference.

Passa da un certificato SSL/TLS personalizzato con indirizzi IP dedicati a SNI

Se hai configurato CloudFront l'utilizzo di un certificato SSL/TLS personalizzato con indirizzi IP dedicati, puoi passare all'utilizzo di un certificato SSL/TLS personalizzato con SNI ed eliminare i costi associati agli indirizzi IP dedicati. La procedura seguente mostra come.

> **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 tuoi contenuti dopo la modifica. Per ulteriori informazioni, consulta Scegli in che modo CloudFront vengono servite le richieste HTTPS.

Passa dal certificato personalizzato allo SNI

La procedura seguente mostra come passare da un certificato SSL/TLS personalizzato con indirizzi IP dedicati a SNI.

Per passare da un certificato SSL/TLS personalizzato con indirizzi IP dedicati a SNI

1. Accedi a AWS Management Console e apri la console all'indirizzo. CloudFront https://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. Cambia l'impostazione di Custom SSL Client Support (Supporto client SSL personalizzato) in Only Clients that Support Server Name Indication (SNI) (Solo client che supportano Server Name Indication (SNI)).
6. Seleziona Yes, Edit (Sì, modifica).

Offri contenuti privati con URL firmati e cookie 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 URL speciali CloudFront firmati o cookie firmati.
- Richiedi che i tuoi utenti accedano ai tuoi contenuti utilizzando CloudFront URL, non URL che accedono ai contenuti direttamente sul server di origine (ad esempio, Amazon S3 o un server HTTP privato). La richiesta di CloudFront URL non è necessaria, ma la consigliamo per impedire agli utenti di aggirare le restrizioni specificate negli URL firmati o nei cookie firmati.

Per ulteriori informazioni, consulta Limita l'accesso ai file.

Come offrire 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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.
   - Origine personalizzata - Consulta Limita l'accesso ai file su origini personalizzate.

   Le origini personalizzate includono Amazon EC2, bucket Amazon S3 configurati come endpoint del sito Web, Elastic Load Balancing e server Web HTTP personalizzati.
2. Specifica i gruppi di chiavi attendibili oppure i firmatari attendibili che desideri utilizzare per creare URL firmati o cookie firmati. Ti consigliamo di utilizzare gruppi di chiavi attendibili. Per ulteriori informazioni, consulta Specificate i firmatari che possono creare URL firmati e cookie firmati.
3. Scrivi l'applicazione per rispondere a richieste provenienti da utenti autorizzati con URL firmati oppure con intestazioni `Set-Cookie` che definiscono cookie firmati. Segui le fasi in uno dei seguenti argomenti:

- Utilizza URL firmati
- Usa cookie firmati

Se non si è certi del metodo da utilizzare, consultare Decidi di utilizzare URL firmati o cookie firmati.

Argomenti

Limita l'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 URL firmati o cookie firmati. In seguito, puoi sviluppare la tua applicazione per creare e distribuire URL firmati a utenti autenticati o per inviare intestazioni `Set-Cookie` che definiscono cookie firmati per gli utenti autenticati (per offrire ad alcuni utenti accesso a lungo termine a un numero ridotto di file, puoi anche creare URL firmati manualmente).

Quando crei URL o cookie 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 RSA-SHA1 per firmare URL o cookie. CloudFront non accetta altri algoritmi.

Limita l'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 gli URL di Amazon S3. Ciò impedisce a qualcuno di aggirare CloudFront e utilizzare l'URL di Amazon S3 per ottenere contenuti a cui desideri limitare l'accesso. Questa fase non è necessaria per utilizzare URL firmati, ma la consigliamo.

Per richiedere agli utenti di accedere ai tuoi contenuti tramite CloudFront URL, esegui le seguenti operazioni:

- Autorizza il 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.
- Sopprimi l'autorizzazione di leggere i file con URL di Amazon S3 per tutti gli altri utenti.

Per ulteriori informazioni, consulta the section called “Limita l'accesso a un'origine Amazon Simple Storage Service”.

Limita l'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. Questa fase non è necessaria per utilizzare URL firmati, ma la 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 Configura CloudFront per aggiungere intestazioni personalizzate alle richieste di origine.

Viewer Protocol Policy (Policy protocollo visualizzatore)

Configura la tua distribuzione per richiedere agli spettatori di utilizzare HTTPS per accedere. 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 utilizzato dai 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 URL firmati e cookie firmati

Argomenti

Per creare URL firmati o cookie firmati, hai bisogno di 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 attendibili con URL firmati e cookie firmati. Per ulteriori informazioni, consulta Scegli tra gruppi di chiavi attendibili (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 URL firmati o cookie firmati per accedere ai tuoi file.
- Quando crei URL o cookie 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, si specificano indirettamente anche i file che richiedono URL firmati o cookie firmati aggiungendo il firmatario a un comportamento della cache. Se la tua distribuzione ha un solo comportamento cache, i visualizzatori devono utilizzare gli URL o i cookie firmati per accedere a qualsiasi file associato alla distribuzione. Se crei più comportamenti cache e aggiungi firmatari attendibili ad alcuni comportamenti cache e non ad altri, puoi richiedere che i visualizzatori utilizzino URL o cookie firmati per accedere ad alcuni file e non ad altri.

Per specificare i firmatari (le chiavi private) autorizzati a creare URL firmati o cookie 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 attendibili (consigliato) e Account AWS.
2. Per il firmatario scelto nel passaggio 1, crea una coppia di chiavi pubbliche-private. Per ulteriori informazioni, consulta Crea coppie di chiavi per i tuoi firmatari.
3. Se utilizzi .NET o Java per creare URL o cookie firmati, riformatta la chiave privata. Per ulteriori informazioni, consulta Riformatta la chiave privata (solo .NET e Java).
4. Nella distribuzione per la quale stai creando URL firmati o cookie firmati, specifica il firmatario. Per ulteriori informazioni, consulta Aggiungi un firmatario a una distribuzione.

Scegli tra gruppi di chiavi attendibili (consigliato) e Account AWS

Per utilizzare URL firmati o cookie firmati, hai bisogno di 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 degli URL CloudFront firmati e dei cookie 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 usi l'utente AWS root, devi usare il per AWS Management Console gestire le coppie di CloudFront chiavi, quindi non puoi 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.

Crea coppie di chiavi per i tuoi firmatari

Ogni firmatario utilizzato per creare URL CloudFront firmati o cookie 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.
- Deve essere in formato PEM codificato in base64.
- Deve essere una coppia di chiavi a 2048 bit.

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**
>
> I passaggi seguenti utilizzano OpenSSL come esempio di un modo per creare una coppia di chiavi. Esistono molti altri modi per creare una coppia di chiavi RSA.

1. 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
   ```

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 AWS Management Console 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, procedi come segue:

   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. Verrà usato in seguito quando si creano URL firmati o cookie firmati, come valore del campo `Key-Pair-Id`.

Per aggiungere la chiave pubblica a un gruppo di chiavi

1. Apri la console all'indirizzo. CloudFront https://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. Circa il modo consigliato per creare chiavi pubbliche per gli URL firmati

e i cookie firmati, consulta Crea 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 AWS Management Console 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 AWS Management Console. 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 AWS Management Console

1. Accedi AWS Management Console 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 chiave privata, può generare URL e cookie firmati validi e scaricare il tuo contenuto. 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 AWS Management Console, questo è chiamato Access Key ID.) Lo utilizzerai nella creazione di URL o cookie firmati.

Riformatta la chiave privata (solo .NET e Java)

Se utilizzi .NET o Java per creare URL o cookie firmati, non puoi utilizzare la chiave privata della coppia di chiavi nel formato PEM di default 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 garantire un corretto funzionamento del codificatore, aggiungi il file JAR per le API di crittografia Bouncy Castle Java al tuo progetto e quindi aggiungi il provider Bouncy Castle.

Aggiungi un firmatario a una distribuzione

Un firmatario è il gruppo di chiavi affidabile (consigliato) o la coppia di CloudFront chiavi che può creare URL firmati e cookie firmati per una distribuzione. Per utilizzare URL firmati o cookie firmati con una CloudFront distribuzione, devi specificare un firmatario.

I firmatari sono associati ai comportamenti cache. Ciò ti consente di richiedere URL o cookie firmati solo per alcuni dei file in una distribuzione. Una distribuzione richiede URL o cookie firmati solo per i file associati ai comportamenti cache corrispondenti.

Analogamente, un firmatario può firmare solo URL o cookie per i file associati ai comportamenti cache corrispondenti. Ad esempio, se disponi di un firmatario per un comportamento cache e di un altro firmatario per un altro comportamento cache, nessuno dei due firmatari attendibili può creare URL o cookie firmati per file associati all'altro comportamento 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 cache, contrariamente al secondo, non richiede URL o cookie firmati. Gli utenti saranno in grado di accedere ai file senza utilizzare URL firmati o cookie firmati, poiché 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 per iniziare a generare URL firmati e cookie 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 URL firmati o cookie 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 cache il cui modello di percorso corrisponde ai file che desideri proteggere con URL firmati o cookie firmati, quindi scegli Edit (Modifica).
6. Nella pagina Edit Behavior (Modifica comportamento) effettua le operazioni seguenti:

   a. Per Restrict Viewer Access (Use Signed URLs or Signed Cookies) (Limita accesso visualizzatore (usa URL o cookie firmati)), seleziona Yes (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 periodicamente (modificare) le coppie di chiavi per gli URL e i cookie firmati. Per ruotare le coppie di chiavi che utilizzi per creare URL o cookie firmati senza invalidare URL o cookie non ancora scaduti, procedi come segue:

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 gli URL firmati o i cookie firmati con le nuove chiavi private funzionino.
4. Attendi che la data di scadenza sia trascorsa negli URL o cookie che sono 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 URL firmati o cookie firmati

CloudFront gli URL firmati e i cookie 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 URL firmati o cookie firmati, prendi in considerazione quanto segue.

Utilizza URL firmati 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 intendi modificare i tuoi URL correnti.

Se non stai attualmente utilizzando URL firmati e i tuoi URL (senza firma) contengono uno qualsiasi dei seguenti parametri di stringa di query, non puoi utilizzare URL o cookie firmati:

- `Expires`
- `Policy`
- `Signature`
- `Key-Pair-Id`

CloudFront presuppone che gli URL che contengono uno di questi parametri della stringa di query siano URL firmati e pertanto non considererà i cookie firmati.

Utilizza sia gli URL firmati che i cookie firmati

Gli URL firmati hanno la precedenza sui cookie firmati. Se utilizzi sia URL firmati che cookie 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.

Utilizza URL firmati

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**
>
> Puoi creare alcuni URL firmati utilizzando policy predefinite e creare alcuni URL firmati utilizzando policy personalizzati per la stessa distribuzione.

Argomenti

Decidi di utilizzare politiche predefinite o personalizzate per gli URL firmati

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 ulteriori informazioni, consulta Valori da specificare in una dichiarazione di policy per un URL firmato che utilizza 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)

Descrizione	Policy predefinita	Policy personalizzata
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 URL firmati utilizzando una policy predefinita, consulta Crea un URL firmato utilizzando una politica predefinita.

Per informazioni sulla creazione di URL firmati utilizzando una policy personalizzata, consulta Crea un URL firmato utilizzando una politica personalizzata.

Funzionamento di URL firmati

Ecco una panoramica di come CloudFront configuri Amazon S3 per gli URL firmati 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 utilizzare per verificare la firma dell'URL. CloudFront Puoi utilizzare le chiavi private corrispondenti per firmare gli URL.

   Per ulteriori informazioni, consulta Specificate i firmatari che possono creare URL firmati e cookie firmati.
2. Sviluppa la tua applicazione per determinare se un utente deve avere accesso al tuo contenuto e per creare URL firmati per i file o parti della tua applicazione a cui intendi limitare l'accesso. Per ulteriori informazioni, consultare i seguenti argomenti:

   - Crea un URL firmato utilizzando una politica predefinita
   - Crea un URL firmato utilizzando una politica personalizzata
3. Un utente richiede un file per il quale sono necessari URL firmati.

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 gli URL firmati sono validi

Puoi distribuire contenuto privato utilizzando un URL firmato valido soltanto per un breve periodo di tempo, anche di pochi minuti. Gli URL firmati 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 gli URL firmati saranno validi per soltanto un breve periodo di tempo, vorrai probabilmente generarli automaticamente utilizzando un'applicazione che

sviluppi. Quando l'utente inizia a scaricare un file o inizia a riprodurre un file multimediale, CloudFront confronta la data 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. Gli URL firmati validi per un periodo di tempo più lungo sono utili per la distribuzione di contenuto privato a utenti noti, ad esempio la distribuzione di un piano aziendale a investitori o distribuzione di materiali per la formazione a dipendenti. Puoi sviluppare un'applicazione per generare questi URL firmati a lungo termine per te.

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 GET per ottenere un file in parti più piccole, qualsiasi richiesta GET che si verifica dopo la scadenza non riuscirà. Per ulteriori informazioni sulle richieste Range GET, consulta Come CloudFront elabora le richieste parziali per un oggetto (range GETs).

Codice di esempio e strumenti di terza parte.

Per il codice di esempio che crea la parte con hash e firma di URL firmati, 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

Crea un URL firmato utilizzando una politica 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 utilizzi .NET o Java per creare URL firmati e non hai riformattato la chiave privata per la coppia di chiavi dal formato .pem di default in un formato compatibile con .NET o Java, fallo adesso. Per ulteriori informazioni, consulta Riformatta la chiave privata (solo .NET e Java).

2. Concatena i seguenti valori nell'ordine elencato, replicando il formato mostrato in questo esempio di URL firmato:

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Expires=1357034400&Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5Ew
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

Rimuovi tutti gli spazi vuoti (inclusi tabulazioni e caratteri di nuova riga). È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione. Tutti i valori hanno un tipo di. `String`

1. ***URL di base per il file***

   L'URL di base è l' CloudFront URL che utilizzeresti per accedere al file se non utilizzassi URL firmati, inclusi gli eventuali parametri della stringa di query. Nell'esempio precedente, l'URL di base è. `https://d111111abcdef8.cloudfront.net/image.jpg` Per ulteriori informazioni sul formato di URL per le distribuzioni, consulta Personalizza il formato URL per i file in CloudFront.

   - L' CloudFront URL seguente è per 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`

   - I seguenti CloudFront URL si riferiscono ai 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. **?**

   ?indica che i parametri della stringa di query seguono l'URL di base. Includi ? anche se non disponi di parametri della stringa di query personalizzati.

3. ***I parametri della stringa di query, se presenti*** **&**

   Questo valore è facoltativo. Se desideri aggiungere i tuoi parametri di stringa di query, ad esempio:

   `color=red&size=medium`

   quindi aggiungi i parametri dopo ? e prima del `Expires` parametro. In alcuni rari casi, è possibile che sia necessario inserire i tuoi parametri di stringa di query dopo `Key-Pair-Id`.

   > **Important**
   >
   > I tuoi parametri non possono essere denominati `Expires`, `Signature` o `Key-Pair-Id`.

   Se aggiungete i vostri parametri, aggiungete un & dopo ognuno di essi, incluso l'ultimo.

4. **Expires=*data e ora in formato orario Unix (in secondi) e 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, le 10:00 UTC del 1° gennaio 2013 vengono convertite `1357034400` nel formato orario Unix, come illustrato nell'esempio all'inizio di questo argomento. Per utilizzare l'ora epoch, utilizzate un numero intero a 32 bit per una data non successiva a `2147483647` (19 gennaio 2038 alle 03:14:07 UTC). Per informazioni sull'UTC, consulta RFC 3339, Date and Time on the Internet: Timestamps.

5. **&Signature=*versione hash e firmata della dichiarazione politica***

   Una versione con hash, firma e codifica base64 della dichiarazione di policy JSON. Per ulteriori informazioni, consulta Crea una firma per un URL firmato che utilizza una politica predefinita.

6. **&Key-Pair-Id=*ID della chiave pubblica per la chiave CloudFront pubblica di cui stai utilizzando la chiave privata corrispondente per generare la firma***

   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 URL firmati e cookie firmati.

Crea una firma per un URL firmato che utilizza una politica predefinita

Per creare la firma per un URL firmato che utilizza una politica predefinita, completare le seguenti procedure.

Argomenti

- Create una dichiarazione politica per un URL firmato che utilizza una politica predefinita
- Crea una firma per un URL firmato che utilizza una politica predefinita

Create una dichiarazione politica per un URL firmato che utilizza una politica 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 gli URL firmati che utilizzano una policy predefinita, non includi la dichiarazione di policy nell'URL come avviene per gli URL firmati che utilizzano una policy 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 tabulazioni e caratteri di nuova riga) dall'informativa. 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`, e `Key-Pair-Id` i parametri`Signature`, ad esempio:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

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 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, la data 1 gennaio 2013 10:00 UTC viene convertita in 1357034400 nel formato 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 utilizzi l'esempio di dichiarazione di policy seguente in un URL firmato, un utente può accedere al file `https://d111111abcdef8.cloudfront.net/horizon.jpg` fino al 1° gennaio 2013 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1357034400
                }
            }
        }
    ]
}
```

Crea una firma per un URL firmato che utilizza una politica 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 Create una dichiarazione politica per un URL firmato che utilizza una politica 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 codifica e la crittografia 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 RSA per sottoporre a hashing e firmare la dichiarazione di policy che hai creato nella procedura Per creare la dichiarazione di policy per un URL firmato che utilizza una policy predefinita. Utilizza la versione dell'informativa 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 tabulazioni e caratteri di nuova riga) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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.

Crea un URL firmato utilizzando una politica personalizzata

Per creare un URL firmato utilizzando una politica personalizzata, completare la procedura seguente.

Per creare un URL firmato utilizzando una policy personalizzata

1. Se utilizzi .NET o Java per creare URL firmati e non hai riformattato la chiave privata per la coppia di chiavi dal formato .pem di default in un formato compatibile con .NET o Java, fallo adesso. Per ulteriori informazioni, consulta Riformatta la chiave privata (solo .NET e Java).
2. Concatena i seguenti valori nell'ordine elencato, replicando il formato mostrato in questo esempio di URL firmato:

```
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 (inclusi tabulazioni e caratteri di nuova riga). È possibile che tu debba includere caratteri di escape nella stringa del codice dell'applicazione. Tutti i valori hanno un tipo di. `String`

1. ***URL di base per il file***

   L'URL di base è l' CloudFront URL che utilizzeresti per accedere al file se non utilizzassi URL firmati, inclusi gli eventuali parametri della stringa di query. Nell'esempio precedente, l'URL di base è. `https://d111111abcdef8.cloudfront.net/image.jpg` Per ulteriori informazioni sul formato di URL per le distribuzioni, consulta Personalizza il formato URL per i file in CloudFront.

   I seguenti esempi mostrano i valori che specifichi per le distribuzioni.

   - L' CloudFront URL seguente è per 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
```

- I seguenti CloudFront URL si riferiscono ai 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. **?**

   ?indica che i parametri della stringa di query seguono l'URL di base. Includi ? anche se non disponi di parametri della stringa di query personalizzati.

3. ***I parametri della stringa di query, se presenti*** **&**

   Questo valore è facoltativo. Se desideri aggiungere i tuoi parametri di stringa di query, ad esempio:

   ```
   color=red&size=medium
   ```

   quindi aggiungili dopo ? e prima del `Policy` parametro. In alcuni rari casi, è possibile che sia necessario inserire i tuoi parametri di stringa di query dopo `Key-Pair-Id`.

   > **Important**
   >
   > I tuoi parametri non possono essere denominati `Policy`, `Signature` o `Key-Pair-Id`.

   Se aggiungete parametri personalizzati, aggiungete un valore & dopo ognuno di essi, compreso l'ultimo.

4. **`Policy=`*`versione codificata base64 della dichiarazione politica`***

   La tua dichiarazione politica in formato JSON, con gli spazi vuoti rimossi, quindi codificata in base64. Per ulteriori informazioni, consulta Crea una dichiarazione politica per un URL firmato che utilizza un criterio personalizzato.

   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=`*`versione hash e firmata della dichiarazione politica`***

   Una versione con hash, firma e codifica base64 della dichiarazione di policy JSON. Per ulteriori informazioni, consulta Crea una firma per un URL firmato che utilizza una politica personalizzata.

6. **`&Key-Pair-Id=`*`ID della chiave pubblica per la chiave CloudFront pubblica di cui stai utilizzando la chiave privata corrispondente per generare la firma`***

   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 URL firmati e cookie firmati.

Crea una dichiarazione politica per un URL firmato che utilizza un criterio personalizzato

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>"
                }
            }
        }
    ]
}
```

   Tieni 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 tabulazioni e caratteri di nuova riga) dall'informativa. 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, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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 “Crea una firma per un URL firmato che utilizza una politica 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 CloudFront `PolicySignature`, e. `Key-Pair-Id` Per 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.

Tieni presente quanto segue:

- Protocollo: il valore deve iniziare con `http://` `https://` o `*://`.
- Parametri della stringa di query: se l'URL dispone di parametri della stringa di query, utilizza una barra rovesciata (\) per eseguire l'escape del carattere punto interrogativo (?) che inizia la stringa di query. Per 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 suddiviso 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, il carattere jolly asterisco (*) si applica solo all'interno della sezione del percorso, in modo che corrisponda agli URL `https://www.example.com/helloworld` e `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 URL:

- `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 sezione. `Condition` 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 entro la data e l'ora specificate. Non racchiudere il valore tra virgolette.

IpAddress (Facoltativo)

L'indirizzo IP del client che esegue la richiesta HTTP. 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. 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:

  `"`*`Indirizzo IP IPv`*`/32"`
- Devi specificare gli intervalli di indirizzi IP in 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 nel formato IPv6, ad esempio 2001:0db8:85a3::8a2e:0370:7334, non sono supportati.

  Se utilizzi una policy personalizzata che include `IpAddress`, non attivare IPv6 per la distribuzione. Se intendi limitare l'accesso a una parte del contenuto per indirizzo IP e supportare le richieste IPv6 per altro contenuto, puoi creare due distribuzioni. Per ulteriori informazioni, consulta the section called “Enable IPv6 (Abilita IPv6)” nell'argomento the section called “Distribution Settings (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 copiate e incollate uno di questi esempi, rimuovete gli spazi vuoti (inclusi tabulazioni e caratteri di nuova riga), sostituite i valori con i vostri valori e includete un carattere di nuova riga dopo la parentesi quadra 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 politica: accedere 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 politica: accedere a tutti i file di una directory da un intervallo di indirizzi IP

L'esempio di policy personalizzata seguente consente di creare URL firmati per qualsiasi file nella directory `training`, 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 politica: accedere 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 creare URL firmati 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 si utilizza 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.

Crea una firma per un URL firmato che utilizza una politica 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 codifica e la crittografia 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 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. Utilizzate la versione dell'informativa che non include più spazi vuoti ma che non è ancora stata codificata in base 64.

   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 tabulazioni e caratteri di nuova riga) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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.

Usa cookie firmati

CloudFront i cookie firmati consentono di controllare chi può accedere ai contenuti quando non si desidera modificare gli URL correnti 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

- Decidi di utilizzare politiche predefinite o personalizzate per i cookie firmati

- Funzionamento di cookie firmati
- Impedisci l'uso improprio dei cookie firmati
- When CloudFront controlla la data e l'ora di scadenza in un cookie firmato
- Codice di esempio e strumenti di terza parte.
- Imposta i cookie firmati utilizzando una politica predefinita
- Imposta i cookie firmati utilizzando una politica personalizzata

Decidi di utilizzare politiche predefinite o personalizzate per i 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 Imposta i cookie firmati utilizzando una politica predefinita.

Per informazioni sulla creazione di cookie firmati utilizzando una policy personalizzata, consulta Imposta i cookie firmati utilizzando una politica 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. Puoi utilizzare le chiavi private corrispondenti per firmare gli URL.

   Per ulteriori informazioni, consulta Specificate i firmatari che possono creare URL firmati e cookie firmati.
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 di 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.

Impedisci l'uso improprio dei 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 GET per ottenere un file in parti più piccole, qualsiasi richiesta GET che si verifica dopo la scadenza non riuscirà. Per ulteriori informazioni sulle richieste Range GET, consulta Come CloudFront elabora le richieste parziali per un oggetto (range GETs).

Codice di esempio e strumenti di terza parte.

Il codice di esempio per contenuto privato mostra solo come creare la firma per URL firmati. 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, 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

Imposta i cookie firmati utilizzando una politica predefinita

Per definire un cookie firmato utilizzando una policy predefinita, completa la procedura descritta di seguito. Per creare la firma, consulta Crea una firma per un cookie firmato che utilizza una politica 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 Riformatta la 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 CloudFront firmato 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 Impedisci l'uso improprio dei 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 intendi utilizzare un nome di dominio alternativo come example.com negli URL, devi aggiungere il nome di dominio alternativo alla distribuzione indipendentemente se si specifica l'attributo `Domain`. Per ulteriori informazioni, consulta Nomi di dominio alternativi (CNAME) nell'argomento Riferimento alle 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'intestazione tramite una connessione HTTPS per garantire che gli attributi del cookie siano protetti dagli attacchi. `Set-Cookie` man-in-the-middle

`HttpOnly`

Definisce come il browser (se supportato) interagisce con il valore del cookie. Con`HttpOnly`, i valori del cookie sono inaccessibili a. JavaScript Questa precauzione può aiutare a mitigare gli attacchi XSS (Cross-Site Scripting). Per ulteriori informazioni, consulta Utilizzo dei cookie HTTP.

`CloudFront-Expires`

Specifica la data e l'ora di scadenza in formato Unix (in secondi) e UTC. Ad esempio, la data 1 gennaio 2013 10:00 UTC viene convertita in 1357034400 nel formato Unix. Per usare il tempo epoca (Unix epoch), utilizza un numero intero a 32 bit per una data non successiva

a 2147483647 (19 gennaio 2038 alle 03:14:07 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 Crea una firma per un cookie firmato che utilizza una politica predefinita.

`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. 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 URL firmati e cookie firmati.

Il seguente esempio mostra intestazioni `Set-Cookie` per un cookie firmato quando utilizzi il nome di dominio associato alla distribuzione negli URL per i tuoi file:

```
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
```

Il seguente esempio mostra intestazioni `Set-Cookie` per un cookie firmato quando utilizzi il nome di dominio alternativo example.org negli URL per i tuoi file:

```
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 intendi utilizzare un nome di dominio alternativo come example.com negli URL, devi aggiungere il nome di dominio alternativo alla distribuzione indipendentemente se si specifica l'attributo `Domain`. Per ulteriori informazioni, consulta Nomi di dominio alternativi (CNAME) nell'argomento Riferimento alle impostazioni di distribuzione.

Crea una firma per un cookie firmato che utilizza una politica predefinita

Per creare la firma per un cookie firmato che utilizza una policy predefinita, completa le seguenti procedure.

Argomenti

- Crea una dichiarazione politica per un cookie firmato che utilizza una politica predefinita
- Firma la dichiarazione sulla politica per creare una firma per un cookie firmato che utilizza una politica predefinita

Crea una dichiarazione politica per un cookie firmato che utilizza una politica 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 tabulazioni e caratteri di nuova riga) dalla dichiarazione politica. 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 la dichiarazione sulla politica per creare una firma per un cookie firmato che utilizza una politica 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 codifica e la crittografia 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 dell'informativa 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 tabulazioni e caratteri di nuova riga) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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`.

Imposta i cookie firmati utilizzando una politica 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 utilizzi .NET o Java per creare URL firmati e non hai riformattato la chiave privata per la coppia di chiavi dal formato .pem di default in un formato compatibile con .NET o Java, fallo adesso. Per ulteriori informazioni, consulta Riformatta la 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 CloudFront firmato richiede tre coppie nome-valore. 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 Impedisci l'uso improprio dei 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 intendi utilizzare un nome di dominio alternativo come example.com negli URL, devi aggiungere il nome di dominio alternativo alla distribuzione indipendentemente se si specifica l'attributo `Domain`. Per ulteriori informazioni, consulta Nomi di dominio alternativi (CNAME) nell'argomento Riferimento alle 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'intestazione tramite una connessione HTTPS per garantire che gli attributi del cookie siano protetti dagli attacchi. `Set-Cookie` man-in-the-middle

`HttpOnly`

Richiede al visualizzatore di inviare il cookie solo nelle richieste HTTP o HTTPS.

`CloudFront-Policy`

La tua dichiarazione politica in formato JSON, con gli spazi vuoti rimossi, quindi codificata in base64. Per ulteriori informazioni, consulta Crea una firma per un cookie firmato che utilizza una politica 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 Crea una firma per un cookie firmato che utilizza una politica 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 URL firmati e cookie firmati.

`Set-Cookie`Intestazioni di esempio per politiche personalizzate

Vedi i seguenti esempi di coppie di `Set-Cookie` intestazioni.

Se desideri utilizzare un nome di dominio alternativo come example.org negli URL, 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 (CNAME) nell'argomento Riferimento alle 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 negli URL dei tuoi file.

```
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 di un cookie firmato quando utilizzi un nome di dominio alternativo (example.org) negli URL dei tuoi file.

```
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 negli URL dei tuoi file.

```
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 negli URL dei tuoi file.

```
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
```

Crea una dichiarazione politica per un cookie firmato che utilizza una politica 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 tabulazioni e caratteri di nuova riga) dall'informativa. 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, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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 Crea una firma per un cookie firmato che utilizza una politica 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 entro la data e l'ora specificate. Non racchiudere il valore tra virgolette.

IpAddress (Facoltativo)

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:

  `"`*`Indirizzo IP IPv`*`/32"`
- Devi specificare gli intervalli di indirizzi IP in 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 nel formato IPv6, ad esempio 2001:0db8:85a3::8a2e:0370:7334, non sono supportati.

Se utilizzi una policy personalizzata che include `IpAddress`, non attivare IPv6 per la distribuzione. Se intendi limitare l'accesso a una parte del contenuto per indirizzo IP e supportare le richieste IPv6 per altro contenuto, puoi creare due distribuzioni. Per ulteriori informazioni, consulta Enable IPv6 (Abilita IPv6) nell'argomento Riferimento alle 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 copiate e incollate uno di questi esempi, rimuovete gli spazi vuoti (inclusi tabulazioni e caratteri di nuova riga), sostituite i valori con i vostri valori e includete un carattere di nuova riga dopo la parentesi 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 politica: accedere a un file da un intervallo di indirizzi IP
- Esempio di dichiarazione politica: accedere a tutti i file di una directory da un intervallo di indirizzi IP
- Esempio di dichiarazione politica: accedere a tutti i file associati a un ID di coppia di chiavi da un indirizzo IP

Esempio di dichiarazione politica: accedere 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": 1357034400
                }
            }
        }
    ]
}
```

Esempio di dichiarazione politica: accedere a tutti i file di 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": 1357034400
                }
            }
        }
    ]
}
```

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 politica: accedere 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": 1357034400
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1357120800
                }
            }
        }
    ]
}
```

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.

Crea una firma per un cookie firmato che utilizza una politica 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 codifica e la crittografia 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 dell'informativa che non include più spazi vuoti ma che non è ancora stata codificata in base 64.

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 tabulazioni e caratteri di nuova riga) dalla stringa con hash e firmata.
3. Codifica la stringa utilizzando la codifica base64 MIME. Per ulteriori informazioni, consulta Section 6.8, Base64 Content-Transfer-Encoding in RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
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`.

Comandi Linux e OpenSSL per la codifica e la crittografia 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 vuoti e il carattere di nuova riga aggiunti da `cat`
- OpenSSL esegue l'hash del file utilizzando SHA-1 e lo firma utilizzando RSA e il file con chiave privata `private_key.pem`
- OpenSSL base64 codifica la dichiarazione politica con hash e firmata
- `tr`sostituisce i caratteri che non sono validi nei parametri della stringa di query URL con caratteri validi

Per altri esempi di codice che dimostrano la creazione di una firma, consultaCodice 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 illustrano come creare firme per URL firmati. Vengono forniti esempi in Perl, PHP, C# e Java. Puoi utilizzare uno qualsiasi degli esempi per creare URL firmati. 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 URL CloudFront firmati Amazon in Node.js sul blog degli AWS 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
- 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 una firma per URL utilizzando Perl

Questa sezione include uno script Perl per le piattaforme Linux/Mac che puoi utilizzare per creare la firma per i 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 URL firmati.

> **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, consultaUtilizza URL firmati.

Argomenti

- Origine dello script Perl per la creazione di un URL firmato

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 È possibile scaricare l'esempio completo all'indirizzo https://docs.aws.amazon.com/ AmazonCloudFront DeveloperGuide /latest/ /samples/demo-php.zip.

Puoi anche creare URL firmati utilizzando la classe `UrlSigner` in AWS SDK for PHP. Per ulteriori informazioni, consulta Class UrlSigner in the AWS SDK for PHP API Reference.

> **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 Utilizza URL firmati.

Argomenti

Esempio: firma RSA SHA-1

Nell'esempio di codice seguente, la funzione `rsa_sha1_sign` sottopone a 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);
}
```

Esempio: creazione di una policy predefinita

Il codice di esempio seguente crea una dichiarazione di policy predefinita per la firma. Per ulteriori informazioni sulle policy predefinite, consulta Crea un URL firmato utilizzando una politica predefinita.

> **Note**
>
> La variabile `$expires` è un timestamp/data che deve essere un 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 . '}}}]}';

    // sign the canned policy
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a url
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // url-encode the query string characters to work around a flash player bug
    return encode_query_params($stream_name);
}
```

Esempio: creare una politica personalizzata

Il codice di esempio seguente crea una dichiarazione di policy personalizzata per la firma. Per ulteriori informazioni sulle policy personalizzate, consulta Crea un URL firmato utilizzando una politica personalizzata.

```
function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // sign the policy
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a url
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // url-encode the query string characters to work around a flash player bug
    return encode_query_params($stream_name);
}
```

Esempio di codice completo

Il codice di esempio seguente fornisce una dimostrazione completa della creazione di URL CloudFront firmati con PHP. È possibile scaricare questo esempio completo all'indirizzo https://docs.aws.amazon.com/ AmazonCloudFront /latest/ /samples/demo-php.zip. DeveloperGuide

Nell'esempio seguente, è possibile modificare l'`$policyCondition`elemento per consentire intervalli di indirizzi IPv4 e IPv6. Per un esempio, consulta Using IPv6 address in IAM policy 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 .= $path . $separator . "Expires=" . $expires . "&Signature=" .
 $signature . "&Key-Pair-Id=" . $key_pair_id;
    }
    // not using a canned policy, include the policy itself in the stream name
    else {
        $result .= $path . $separator . "Policy=" . $policy . "&Signature=" .
 $signature . "&Key-Pair-Id=" . $key_pair_id;
    }

    // new lines would break us, so remove them
    return str_replace('\n', '', $result);
}

function encode_query_params($stream_name) {
    // Adobe Flash Player has trouble with query parameters being passed into it,
    // so replace the bad characters with their URL-encoded forms
    return str_replace(
        array('?', '=', '&'),
        array('%3F', '%3D', '%26'),
```

```
        $stream_name);
}

function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters to support Flash Player
    return encode_query_params($stream_name);
}

function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters to support Flash Player
    return encode_query_params($stream_name);
}


// Path to your private key.  Be very careful that this file is not accessible
// from the web!
```

```
$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';

$video_path = 'example.mp4';

$expires = time() + 300; // 5 min from now
$canned_policy_stream_name = get_canned_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $expires);

$client_ip = $_SERVER['REMOTE_ADDR'];
$policy =
'{'.
    '"Statement":['.
        '{'.
            '"Resource":"'. $video_path . '",'.
            '"Condition":{'.
                '"IpAddress":{"AWS:SourceIp":"' . $client_ip . '/32"},'.
                '"DateLessThan":{"AWS:EpochTime":' . $expires . '}'.
            '}'.
        '}'.
    ']' .
    '}';
$custom_policy_stream_name = get_custom_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $policy);

?>

<html>

<head>
    <title>CloudFront</title>
<script type='text/javascript' src='https://example.cloudfront.net/player/
swfobject.js'></script>
</head>

<body>
    <h1>Amazon CloudFront</h1>
    <h2>Canned Policy</h2>
    <h3>Expires at <?= gmdate('Y-m-d H:i:s T', $expires) ?></h3>
    <br />

    <div id='canned'>The canned policy video will be here</div>
```

```
    <h2>Custom Policy</h2>
    <h3>Expires at <?= gmdate('Y-m-d H:i:s T', $expires) ?> only viewable by IP <?=
 $client_ip ?></h3>
    <div id='custom'>The custom policy video will be here</div>

    <!-- ************** Have to update the player.swf path to a real JWPlayer instance.
    The fake one means that external people cannot watch the video right now -->
    <script type='text/javascript'>
  var so_canned = new SWFObject('https://files.example.com/
player.swf','mpl','640','360','9');
  so_canned.addParam('allowfullscreen','true');
  so_canned.addParam('allowscriptaccess','always');
  so_canned.addParam('wmode','opaque');
  so_canned.addVariable('file','<?= $canned_policy_stream_name ?>');
  so_canned.addVariable('streamer','rtmp://example.cloudfront.net/cfx/st');
        so_canned.write('canned');

  var so_custom = new SWFObject('https://files.example.com/
player.swf','mpl','640','360','9');
  so_custom.addParam('allowfullscreen','true');
  so_custom.addParam('allowscriptaccess','always');
  so_custom.addParam('wmode','opaque');
  so_custom.addVariable('file','<?= $custom_policy_stream_name ?>');
  so_custom.addVariable('streamer','rtmp://example.cloudfront.net/cfx/st');
  so_custom.write('custom');
    </script>
</body>

</html>
```

Consulta anche:

- 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

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 for .NET che può rivelarsi utile nelle applicazioni .NET.

Puoi anche creare URL e cookie firmati utilizzando AWS SDK for .NET. Nella Documentazione di riferimento delle API di AWS SDK for .NET , consulta i seguenti argomenti:

- URL firmati: AmazonCloudFrontUrlSigner
- Cookie firmati — AmazonCloudFrontCookieSigner

Per scaricare il codice, consulta Signature Code in C#.

> **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 Utilizza URL firmati. Per ulteriori informazioni sull'utilizzo dei cookie firmati, vedereUsa cookie firmati.

Utilizzare 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 XML.NET Framework

```
<RSAKeyValue>
  <Modulus>
    wO5IvYCP5UcoCKDo1dcspoMehWBZcyfs9QEzGi6Oe5y+ewGr1oW+vB2GPB
    ANBiVPcUHTFWhwaIBd3oglmF0lGQljP/jOfmXHUK2kUUnLnJp+oOBL2NiuFtqcW6h/L5lIpD8Yq+NRHg
    Ty4zDsyr2880MvXv88yEFURCkqEXAMPLE=
  </Modulus>
  <Exponent>AQAB</Exponent>
  <P>
    5bmKDaTz
    npENGVqz4Cea8XPH+sxt+2VaAwYnsarVUoSBeVt8WLloVuZGG9IZYmH5KteXEu7fZveYd9UEXAMPLE==
  </P>
  <Q>
```

```
    1v9l/WN1a1N3rOK4VGoCokx7kR2SyTMSbZgF9IWJNOugR/WZw7HTnjipO3c9dy1Ms9pUKwUF4
    6d7049EXAMPLE==
  </Q>
  <DP>
    RgrSKuLWXMyBH+/l1Dx/I4tXuAJIrlPyo+VmiOc7b5NzHptkSHEPfR9s1
    OK0VqjknclqCJ3Ig86OMEtEXAMPLE==
  </DP>
  <DQ>
    pjPjvSFw+RoaTu0pgCA/jwW/FGyfN6iim1RFbkT4
    z49DZb2IM885f3vf35eLTaEYRYUHQgZtChNEV0TEXAMPLE==
  </DQ>
  <InverseQ>
    nkvOJTg5QtGNgWb9i
    cVtzrL/1pFEOHbJXwEJdU99N+7sMK+1066DL/HSBUCD63qD4USpnf0myc24in0EXAMPLE==</InverseQ>
  <D>
      Bc7mp7XYHynuPZxChjWNJZIq+A73gm0ASDv6At7F8Vi9r0xUlQe/v0AQS3ycN8QlyR4XMbzMLYk
      3yjxFDXo4ZKQtOGzLGteCU2srANiLv26/imXA8FVidZftTAtLviWQZBVPTeYIA69ATUYPEq0a5u5wjGy
      UOij9OWyuEXAMPLE=
   </D>
</RSAKeyValue>
```

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'hashing della dichiarazione di policy 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, vedi

6

&Key-Pair-Id.

Example : metodo predefinito di firma delle policy 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'hashing della dichiarazione di policy utilizzando SHA1 e crittografa il risultato utilizzando RSA e la chiave privata la cui chiave pubblica corrispondente si trova in un gruppo di chiavi attendibili.
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, vedi
>
> 6
>
> &Key-Pair-Id.

Example : metodo di firma delle 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 la 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 in AWS SDK for Java (versione 1) per creare URL CloudFront firmati.

Per altri esempi, consulta Creare URL e cookie firmati 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 Utilizza URL firmati.

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

Limita l'accesso a un' AWS origine

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 nell' AWS origine solo tramite la CloudFront distribuzione specificata, impedendo loro di accedere ai contenuti direttamente dal bucket o tramite una distribuzione involontaria CloudFront

A tale scopo, configura l'invio CloudFront di richieste autenticate all'origine e configura l' AWS origine per consentire l' AWS accesso solo alle richieste autenticate da. CloudFront Per ulteriori informazioni, consulta gli argomenti seguenti per i tipi di AWS origini compatibili.

Argomenti

- Limitazione dell'accesso a un'origine AWS Elemental MediaPackage v2
- Limita l'accesso a un' AWS Elemental MediaStore origine
- Limita l'accesso all'origine dell'URL di una AWS Lambda funzione
- Limita l'accesso a un'origine Amazon Simple Storage Service

Limitazione dell'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
- Concedere all'OAC l'autorizzazione ad 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 .

Concedere all'OAC l'autorizzazione ad accedere all'origine v2 MediaPackage

Prima di creare un OAC o configurarlo in una CloudFront distribuzione, assicurati che l'OAC disponga dell'autorizzazione per accedere all'origine v2. MediaPackage Esegui questa operazione dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all'origine MediaPackage v2 nella configurazione di distribuzione.

Per concedere all'OAC l'autorizzazione ad accedere all'origine MediaPackage v2, 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' MediaPackage origine v2.

Example : policy IAM che consente l'accesso in sola lettura a una distribuzione CloudFront

La seguente politica consente alla CloudFront distribuzione (*`E1PDK09ESKHJWT`*) l'accesso all'origine MediaPackage v2. L'origine è l'ARN specificato per l'`Resource`elemento.

```
{
    "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 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 allegare l'autorizzazione copiata all'endpoint. Per ulteriori informazioni, consulta i campi delle policy sugli endpoint nella Guida per l'AWS Elemental MediaPackage utente.

Creazione dell'OAC

Per creare un OAC, puoi utilizzare l' AWS Management Console, AWS CloudFormation AWS CLI, o l' CloudFront API.

Console

Per creare un OAC

1. Accedi a AWS Management Console 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 segue:
    a. Immettete un nome e (facoltativamente) una descrizione per l'OAC.

b. Per quanto riguarda il comportamento di firma, ti consigliamo di lasciare l'impostazione predefinita (Richieste di firma (consigliata)). 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 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. Dal menu a discesa Origin Access Control, scegli il nome OAC che desideri utilizzare.
6. Seleziona Salvataggio delle 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 AWS CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del AWS 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, fornisci l'ID OAC nel `OriginAccessControlId` campo, all'interno di un'origine. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, Riferimento alle impostazioni di distribuzione 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). AWS 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 AWS 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 AWS CloudFormation. Usa questa impostazione per disattivare l'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, una per una. 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 AWS 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.

Limita l'accesso a un' AWS Elemental MediaStore origine

CloudFront fornisce il controllo dell'accesso all'origine (OAC) per limitare l'accesso a un'origine. AWS Elemental MediaStore

Argomenti

- Crea un nuovo controllo di accesso all'origine
- Impostazioni avanzate per il controllo dell'accesso all'origine

Crea un nuovo controllo di accesso all'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 il controllo di accesso all'origine, è necessario disporre di una CloudFront distribuzione con un' MediaStore origine.

Concedere all'origine il permesso di controllo dell'accesso all' MediaStore origine

Prima di creare un controllo di accesso all'origine o di configurarlo in una CloudFront distribuzione, assicurati che l'OAC disponga dell'autorizzazione per accedere all' MediaStore origine. Esegui questa operazione dopo aver creato una CloudFront distribuzione, ma prima di aggiungere l'OAC all' MediaStoreorigine nella configurazione di distribuzione.

Per concedere all'OAC l'autorizzazione ad accedere all' MediaStore origine, utilizza una policy 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.

Di seguito sono riportati alcuni esempi di politiche relative ai MediaStore container che consentono a un CloudFront OAC di accedere a un' MediaStore origine.

Example MediaStore policy relativa ai contenitori che consente l'accesso in sola lettura a un OAC CloudFront

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

```
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject"
                ],
                "Resource":
 "arn:aws:mediastore:<region>:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

Example MediaStore politica del contenitore che consente l'accesso in lettura e scrittura a un OAC CloudFront

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadWrite",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject",
                  "mediastore:PutObject"
                ],
                "Resource":
 "arn:aws:mediastore:<region>:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
```

```
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

> **Note**
>
> Per consentire l'accesso in scrittura, è necessario configurare i metodi HTTP consentiti da includere PUT nelle impostazioni di comportamento della CloudFront distribuzione.

Crea il controllo di accesso all'origine

Per creare un OAC, puoi utilizzare l' AWS Management Console, AWS CloudFormation AWS CLI, o l' CloudFront API.

Console

Per creare un controllo di accesso all'origine

1. Accedi AWS Management Console 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 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. Seleziona Salvataggio delle 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 AWS CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del AWS 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' MediaStore origine.

```
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' MediaStoreorigine.

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 alle 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 AWS 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 AWS 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 AWS 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' MediaStore origine.

> **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 AWS 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.

Limita l'accesso all'origine dell'URL di una AWS Lambda funzione

CloudFront fornisce il controllo dell'accesso all'origine (OAC) per limitare l'accesso all'origine dell'URL di una funzione Lambda.

Argomenti

- Crea un nuovo OAC
- Impostazioni avanzate per il controllo dell'accesso all'origine

Crea un nuovo OAC

Completa i passaggi descritti nei seguenti argomenti per configurare un nuovo OAC in. CloudFront

> **Note**
>
> Se utilizzi `PUT` o `POST` metodi con l'URL della funzione Lambda, gli utenti devono includere il valore hash del payload nell'`x-amz-content-sha256`intestazione quando inviano la richiesta a. CloudFront Lambda non supporta payload non firmati.

Argomenti

Prerequisiti

Prima di creare e configurare OAC, è necessario disporre di una CloudFront distribuzione con un URL della funzione Lambda come origine. Per ulteriori informazioni, consulta Usa l'URL di una funzione Lambda.

Concedi all'OAC l'autorizzazione ad accedere all'URL della funzione Lambda

Prima di creare un OAC o configurarlo in una CloudFront distribuzione, assicurati che l'OAC 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 il AWS Command Line Interface ()AWS CLI. La modifica della policy IAM nella console Lambda non è supportata al momento.

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.

Example : AWS CLI comando per aggiornare una policy per consentire l'accesso in sola lettura a un OAC CloudFront

Il AWS CLI comando seguente consente alla CloudFront distribution (*`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
```

> **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 Concessione dell'accesso alla funzione Servizi AWS nella Guida per gli sviluppatori.

Crea l'OAC

Per creare un OAC, puoi utilizzare l' AWS Management Console, AWS CloudFormation AWS CLI, o l' CloudFront API.

Console

Per creare un OAC

1. Accedi a AWS Management Console 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 segue:
   a. Immettete un nome e (facoltativamente) una descrizione per l'OAC.
   b. Per quanto riguarda il comportamento di firma, ti consigliamo di lasciare l'impostazione predefinita (Richieste di firma (consigliata)). Per ulteriori informazioni, consulta the section called “Impostazioni avanzate per il controllo dell'accesso all'origine”.
5. Per il tipo di origine, scegli Lambda.
6. Scegli Crea.

> **Tip**
>
> Dopo aver creato l'OAC, prendi nota del nome. In questa procedura, eseguire le seguenti operazioni:

Per aggiungere un controllo di accesso all'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 l'URL di una funzione Lambda a cui desideri aggiungere l'OAC, quindi scegli la scheda Origins.
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. Dal menu a discesa Origin Access Control, scegli il nome OAC che desideri utilizzare.
6. Seleziona Salvataggio delle 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 inviate all'URL della funzione Lambda.

CloudFormation

Per creare un OAC con AWS CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del AWS 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.

Per 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 un URL della funzione Lambda come origine.

```
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'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, fornisci l'ID OAC nel `OriginAccessControlId` campo, 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). AWS 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 AWS 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 AWS CloudFormation. Usa questa impostazione per disattivare l'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, una per una. 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 Modello di sicurezza e autenticazione per gli URL delle funzioni Lambda nella AWS Lambda Guida per 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 AWS CloudFormation. Utilizzate questa impostazione quando desiderate firmare CloudFront le richieste 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 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 gli URL della funzione Lambda associati a questo controllo di accesso di origine.

Limita l'accesso a un'origine Amazon Simple Storage Service

CloudFront offre due modi per inviare richieste autenticate a un'origine Amazon S3: Origin Access Control (OAC) e Origin Access Identity (OAI). OAC ti aiuta a proteggere le tue origini, ad esempio per Amazon S3. Si consiglia di utilizzare OAC perché supporta:

- 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

L'identità di accesso origine (OAI) non funziona per gli scenari dell'elenco precedente o richiede soluzioni alternative aggiuntive in tali scenari. I seguenti argomenti descrivono come utilizzare OAC con origine Amazon S3. Per informazioni su come migrare dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC), vedere 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 hai bisogno di ACL, 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 del sito Web, devi configurarlo CloudFront come origine personalizzata. Ciò significa che non è possibile utilizzare OAC (o OAI). OAC non supporta il reindirizzamento all'origine tramite Lambda @Edge.

Argomenti

Crea un nuovo controllo di accesso all'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 “Inizia con una distribuzione di base”

> **Note**
>
> Quando usi OAC per proteggere l'origine del tuo bucket S3, la comunicazione tra e Amazon CloudFront S3 avviene sempre tramite HTTPS, indipendentemente dalle tue impostazioni specifiche.

Concedi all'origine il permesso di controllo dell'accesso per accedere al bucket S3

Prima di creare un controllo di accesso all'origine (OAC) o configurarlo in una CloudFront distribuzione, assicurati che l'OAC 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.

Per concedere all'OAC l'autorizzazione ad accedere al bucket S3, utilizza una policy del bucket S3 per consentire al CloudFront service principal () di accedere al bucket. `cloudfront.amazonaws.com` Utilizza un `Condition` elemento della policy per consentire l'accesso CloudFront al bucket solo quando la richiesta è per conto della distribuzione che contiene l' CloudFront origine S3.

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 a un CloudFront OAC di accedere a un'origine S3.

Example Policy dei bucket S3 che consente l'accesso in sola lettura a un OAC CloudFront

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

```
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudfront.amazonaws.com"
        },
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::<S3 bucket name>/*",
        "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
    }
}
```

Example Policy S3 bucket che consente l'accesso in lettura e scrittura a un OAC CloudFront

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowCloudFrontServicePrincipalReadWrite",
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudfront.amazonaws.com"
        },
        "Action": [
            "s3:GetObject",
            "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::<S3 bucket name>/*",
        "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
    }
}
```

SSE-KMS

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 l'OAC disponga dell'autorizzazione

per utilizzare la chiave. AWS KMS Per concedere all'OAC l'autorizzazione per utilizzare la chiave KMS, aggiungi una dichiarazione alla Policy 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 .

L'esempio seguente mostra una dichiarazione di policy della chiave KMS che consente all'OAC di utilizzare la chiave KMS.

Example Dichiarazione politica chiave KMS che consente a un OAC di accedere a una chiave KMS per SSE-KMS CloudFront

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

Crea il controllo di accesso all'origine

Per creare un controllo di accesso all'origine (OAC), puoi utilizzare l' AWS Management Console AWS CloudFormation, AWS CLI, o l' CloudFront API.

Console

Per creare un controllo di accesso all'origine

1. Accedi AWS Management Console 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 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 Origin Access, scegli le impostazioni di controllo degli accessi di Origin (consigliato).
5. Nel menu a discesa Controllo degli accessi origine, scegliere l'OAC che desideri utilizzare.
6. Seleziona Salvataggio delle 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 AWS CloudFormation, usa il tipo di `AWS::CloudFront::OriginAccessControl` risorsa. L'esempio seguente mostra la sintassi del AWS 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 alle impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Elimina una distribuzione con un OAC collegato a un bucket S3

Se devi eliminare una distribuzione con un OAC collegato a un bucket S3, devi 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 public 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 all'origine (OAI) legacy a un controllo dell'accesso all'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 a OAC di accedere a un bucket S3, aggiorna la Policy del bucket per includere due dichiarazioni, una per ogni tipo di principale.

Il seguente esempio di policy del bucket S3 consente sia a un OAI che a un OAC di accedere a un'origine S3.

Example Policy del bucket S3 che consente l'accesso in sola lettura a un OAI e a un OAC

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipalReadOnly",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                }
            }
        },
        {
            "Sid": "AllowLegacyOAIReadOnly",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

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 “Crea un nuovo controllo di accesso all'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 all'origine il permesso di controllo dell'accesso 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 AWS 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 AWS 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 AWS 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 AWS 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.

Usa un'identità di accesso all'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. Questo è il motivo per cui consigliamo di utilizzare invece OAC. 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 dicembre 2022

Per ulteriori informazioni sulla migrazione da OAI a OAC, consultare the section called “Migrazione dell'identità di accesso origine (OAI) al controllo degli accessi origine (OAC)”.

Concedi l'autorizzazione all'identità di accesso all'origine 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 gli URL di Amazon S3 per accedere ai tuoi file dall'esterno. 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.

Usa le policy dei 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. Per 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.

```
{
    "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

```
{
    "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 gli ACL degli oggetti Amazon S3 (non consigliato)

> **Important**
>
> Consigliamo l'utilizzo delle policy di bucket Amazon S3 per consentire a un OAI l'accesso a un bucket S3. È possibile utilizzare le liste di controllo degli accessi (ACL) come descritto in questa sezione, ma non è consigliato.
> Amazon S3 consiglia di impostare S3 Object Ownership a proprietario del bucket applicato, il che significa che gli ACL 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).
> Questa sezione seguente è solo per i casi d'uso legacy che richiedono ACL.

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.

Usa un'identità di accesso all'origine nelle regioni Amazon S3 che supportano solo l'autenticazione con firma versione 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.

Limita l'accesso agli Application Load Balancer

Per un'applicazione Web o altro contenuto fornito da un Application Load Balancer con accesso a Internet in Elastic Load Balancing CloudFront , puoi memorizzare nella cache gli oggetti e servirli direttamente agli utenti (visualizzatori), riducendo il carico sull'Application Load Balancer. Un sistema di bilanciamento del carico connesso a Internet ha un nome DNS risolvibile pubblicamente e indirizza le richieste dai client alle destinazioni su Internet.

CloudFrontpuò anche contribuire a ridurre la latenza e persino ad assorbire alcuni attacchi DDoS (Distributed Denial of Service).

Tuttavia, se gli utenti possono bypassare CloudFront e accedere direttamente all'Application Load Balancer, non si ottengono questi vantaggi. Ma puoi configurare Amazon CloudFront e il tuo

Application Load Balancer per impedire 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 impedire agli utenti di accedere direttamente a un Application Load Balancer e consentire l'accesso solo tramite CloudFront, completa questi passaggi di alto livello:

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. (Facoltativo) Richiedi HTTPS per migliorare la sicurezza di questa soluzione.

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

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 AWS 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, 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.

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, consulta Aggiornamento di una distribuzione e Creazione di una distribuzione.

Come aggiungere un'intestazione HTTP personalizzata (AWS CloudFormation)

In un AWS 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, consultate Origin and OriginCustomHeaderproperties 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 non CloudFront possono essere aggiunte alle richieste di origine.

Configurare 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.

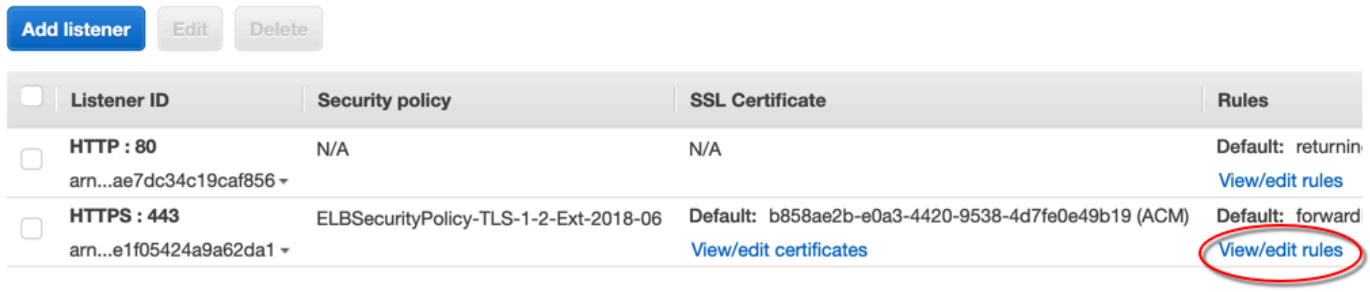
Prerequisiti

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.

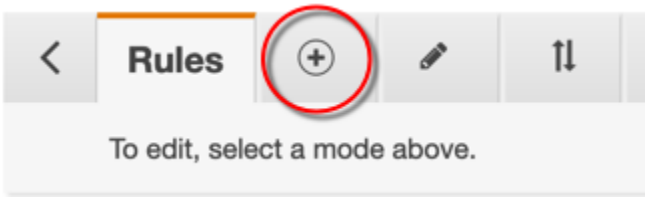
Le procedure seguenti modificano un listener HTTPS. È possibile utilizzare lo stesso processo per modificare un listener HTTP.

Per aggiornare le regole in un listener di Application Load Balancer

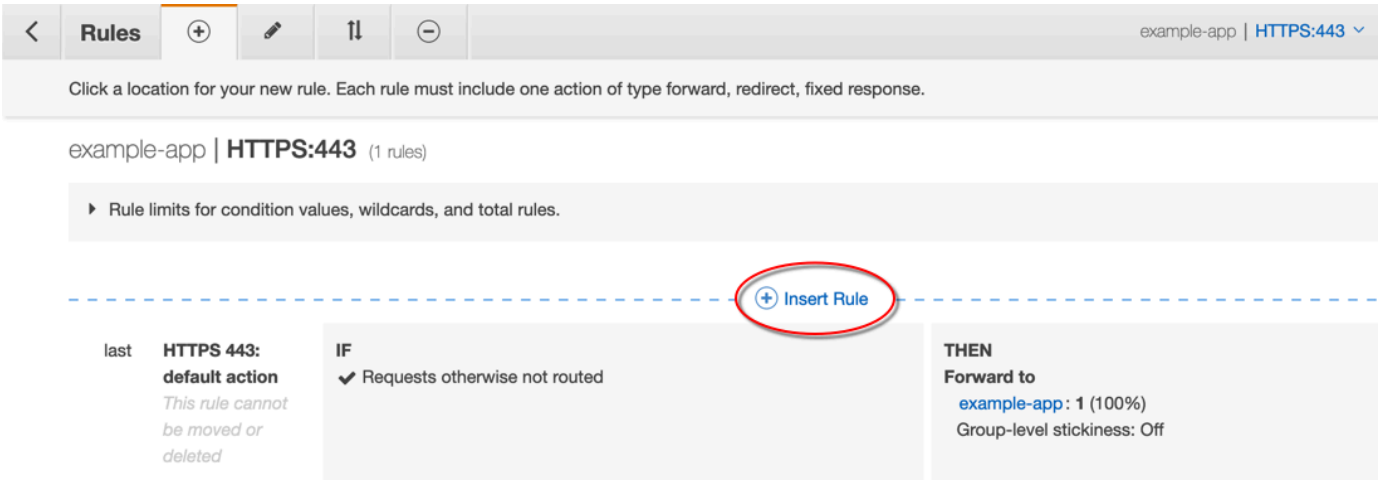
1. Apri la paginaLoad Balancers nella console Amazon EC2.
2. Scegli il load balancer che è l'origine della tua CloudFront distribuzione, quindi scegli la scheda Listeners.
3. Per il listener che si sta modificando, scegli Visualizza/Modifica regole.



4. Scegli l'icona per aggiungere regole.



5. Scegliere Insert rule (Inserisci regola).

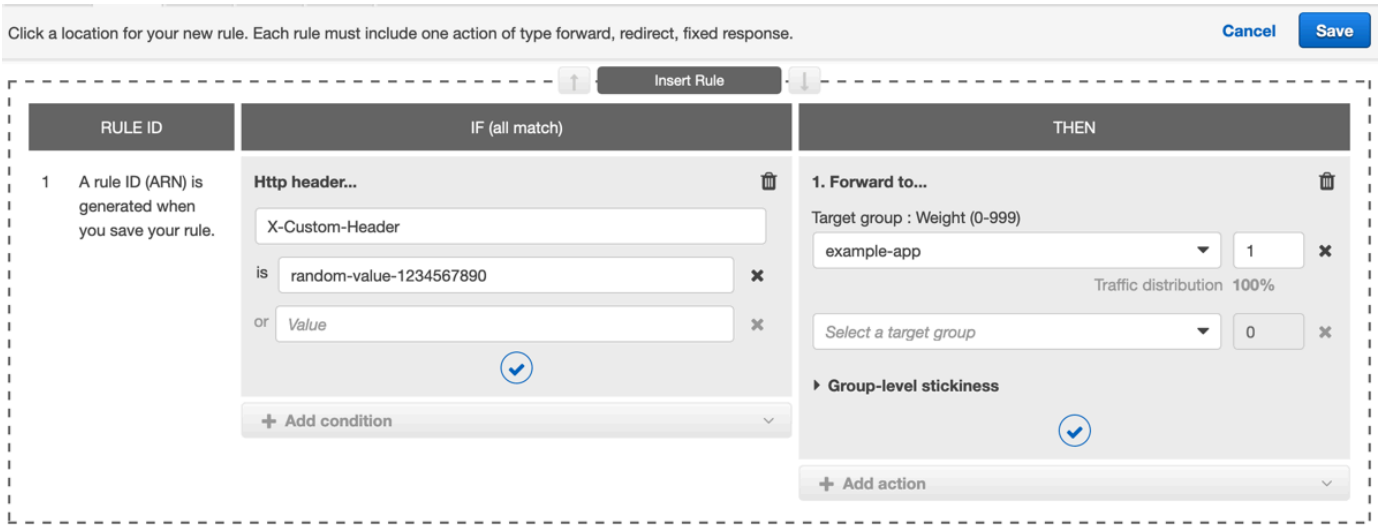


6. Per la nuova regola, effettuare le seguenti operazioni:

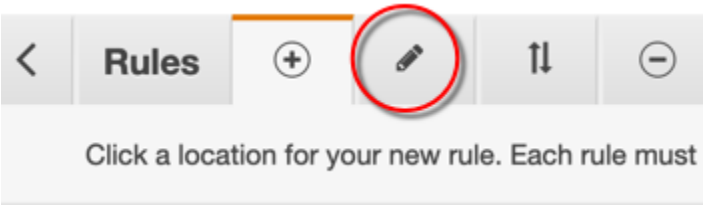
   a. Scegliere Aggiungi condizione e quindi selezionare Header Http. Specificate il nome e il valore dell'intestazione HTTP che avete aggiunto come intestazione personalizzata di origine. CloudFront

   b. Scegliere Aggiungi azione, quindi Inoltra a. Scegliere il gruppo target in cui si desidera inoltrare le richieste.

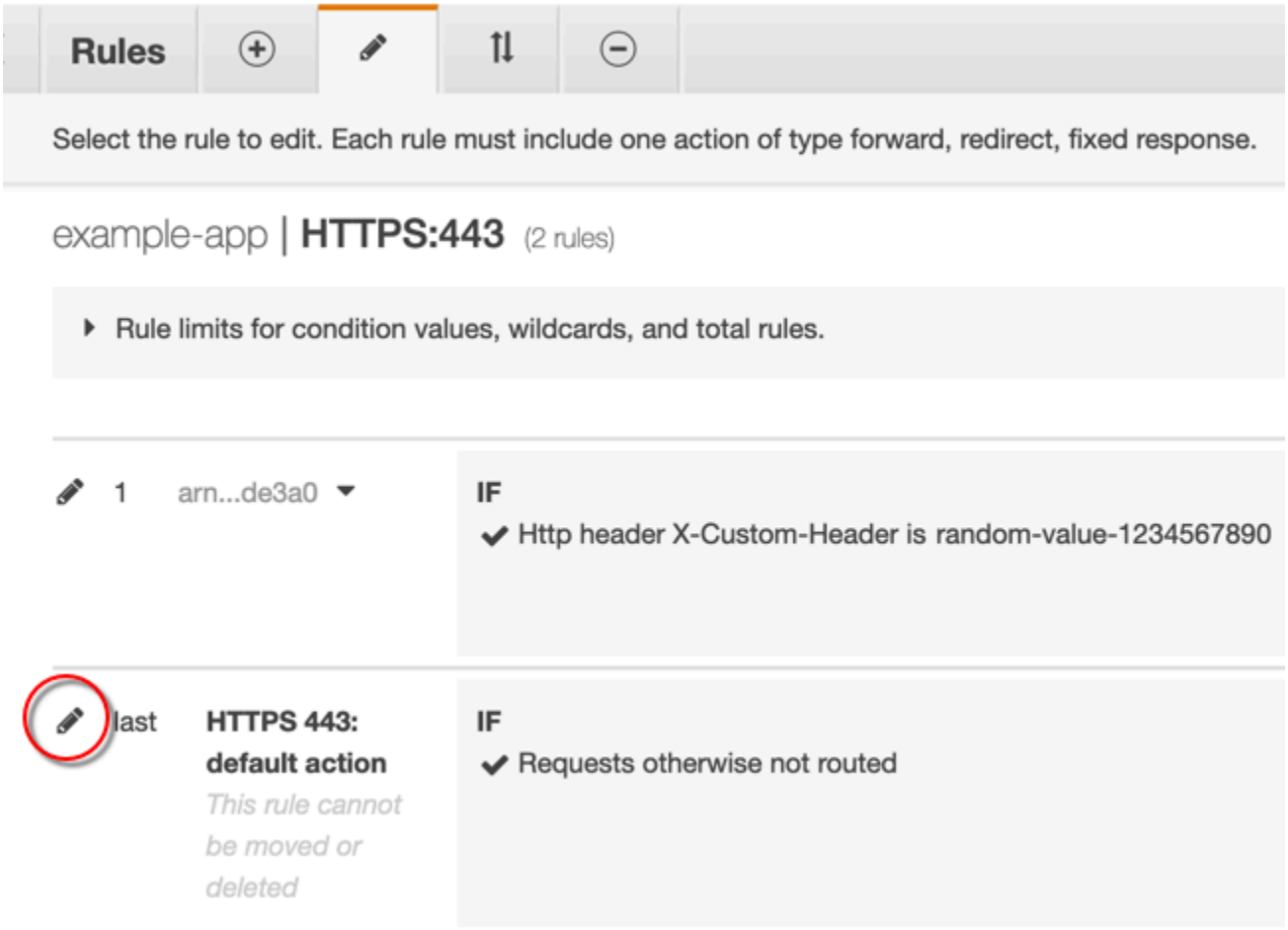
   c. Scegliere Save (Salva) per creare la nuova regola.



7. Scegliere l'icona per modificare le regole.



8. Scegliere l'icona di modifica per la regola predefinita.



9. Per la regola predefinita, effettuare le seguenti operazioni:

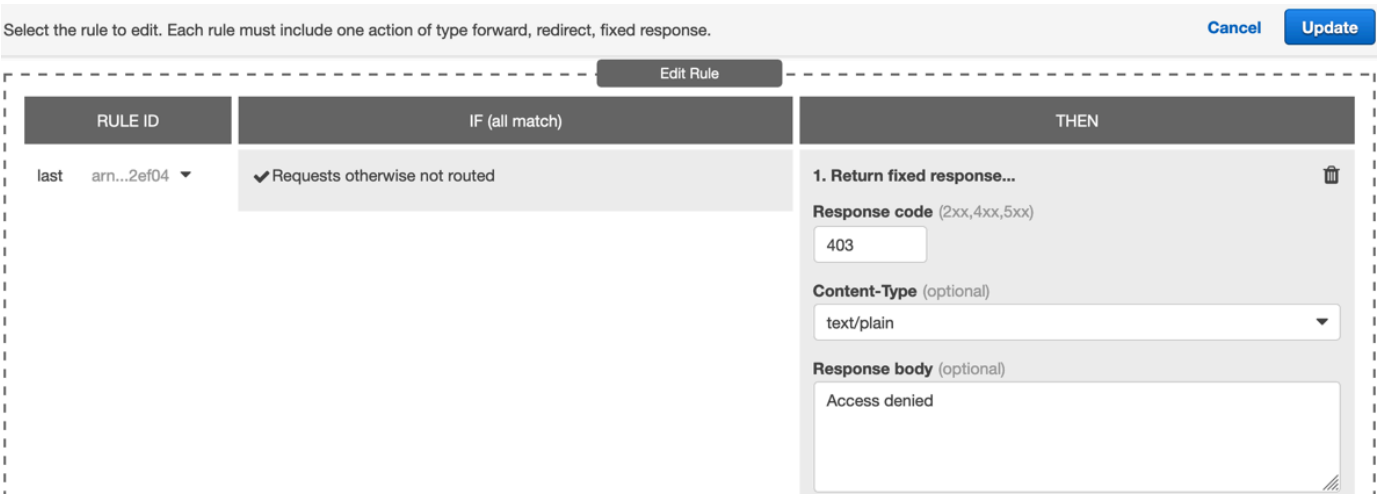
   a. Eliminare l'azione predefinita.

   b. Scegliere Aggiungi azione, quindi Restituisci risposta fissa.

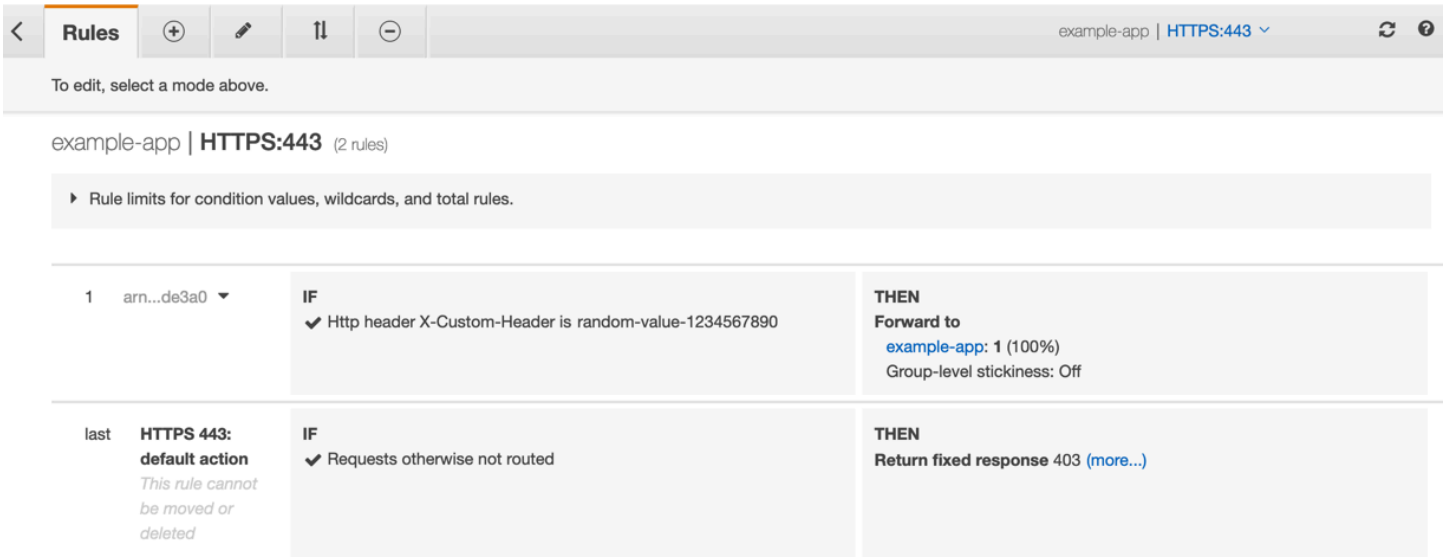
c. Per Codice risposta, immettere **`403`**.

d. Per Corpo risposta, immettere **`Access denied`**.

e. Scegliere Aggiorna per aggiornare la regola predefinita.



Dopo aver completato questi passaggi, il listener del sistema di bilanciamento del carico dispone di due regole, come illustrato nell'immagine seguente. La prima regola inoltra le richieste che contengono l'intestazione HTTP (richieste che provengono da). CloudFront La seconda 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 AWS 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.
- Assicuratevi che l'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 certificato SSL/TLS 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 i certificati SSL/TLS sia nella `ap-southeast-2` regione (per utilizzare HTTPS tra CloudFront e l'origine ALB) che nella regione (per utilizzare HTTPS tra i visualizzatori `us-east-1` e). CloudFront Entrambi i certificati devono corrispondere al nome di dominio indirizzato

all'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 AWS 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.

Limita la distribuzione geografica dei tuoi contenuti

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 le 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 Crea 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. Configurazione e utilizzo di registri standard (registri di accesso)

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 AWS Management Console 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).

Utilizza un servizio di geolocalizzazione di terze parti

Con la funzione di restrizioni CloudFront geografiche, controlli 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 URL CloudFront firmati, con i quali 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 su URL firmati e controllo di accesso origine, consulta Offri contenuti privati con URL firmati e cookie firmati.

La procedura seguente descrive come controllare l'accesso ai file utilizzando un servizio di geolocalizzazione di terza parte.

Utilizzare un servizio di geolocalizzazione di terze parti per limitare l'accesso ai file in 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 URL firmati e cookie 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 “Crea 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

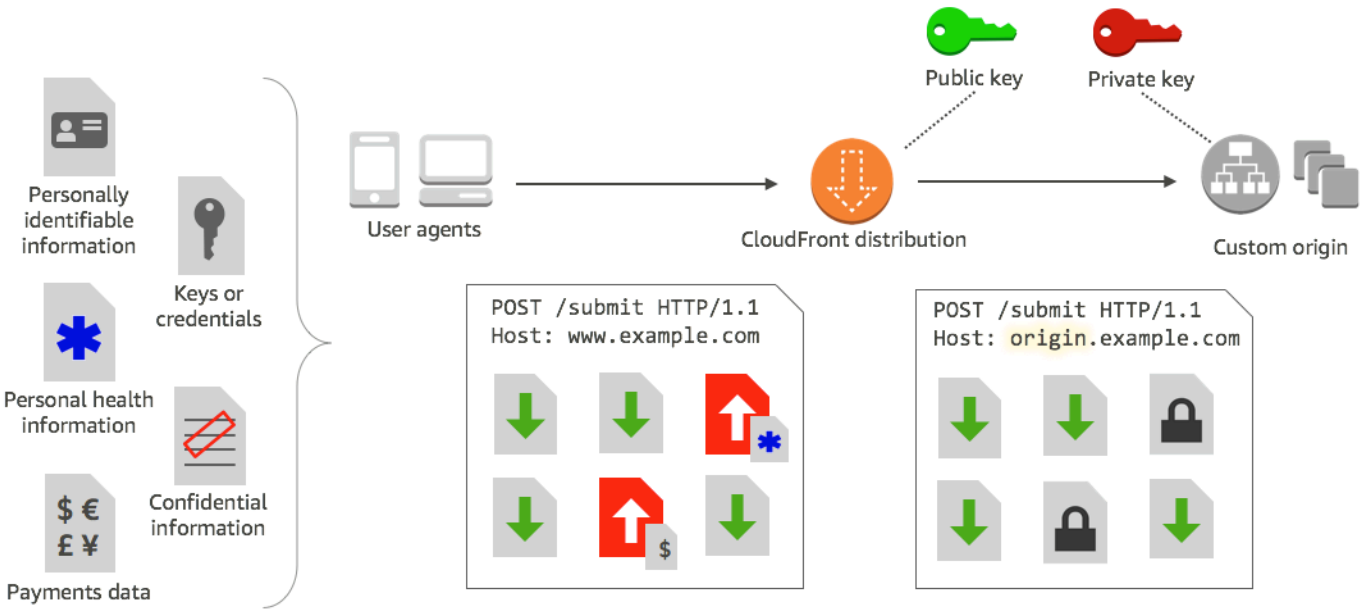
Con Amazon CloudFront, puoi applicare end-to-end connessioni sicure ai server di origine utilizzando HTTPS. La crittografia a livello di campo aggiunge un ulteriore livello di sicurezza che consente di proteggere dati specifici durante l'elaborazione del sistema, di modo che solo alcune applicazioni 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.

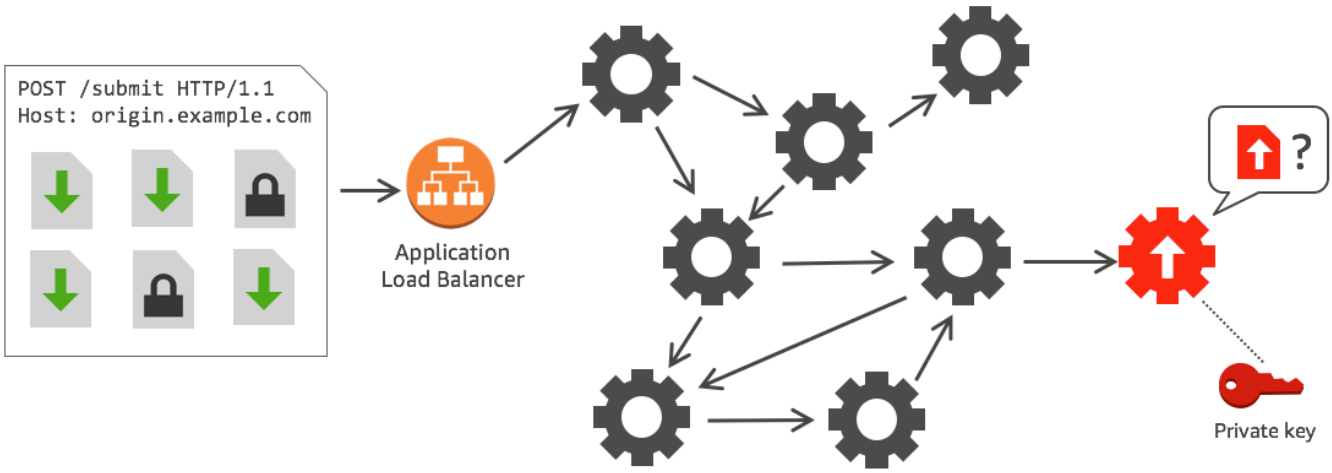
Per utilizzare la crittografia a livello di campo, quando configuri la CloudFront distribuzione, specifica il set di campi nelle richieste POST che desideri crittografare e la chiave pubblica da utilizzare per crittografarle. Puoi crittografare fino a 10 campi dati in una richiesta Non puoi crittografare 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
- Imposta la crittografia a livello di campo
- Decrittografa i campi dati alla tua 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 Imposta la crittografia a livello di campo.

1. Ottieni una coppia chiave pubblica-chiave privata. È necessario ottenere e aggiungere la chiave pubblica prima di iniziare a configurare la 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, creati in CloudFront, definiscono i campi che si desidera 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 di cache per una distribuzione, per specificare quando CloudFront crittografare i dati.

Imposta la 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 dell'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 AWS Management Console 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.

   Provider name (Nome 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 dei campi di dati, o i modelli che identificano i nomi dei campi di dati nella richiesta, che desideri CloudFront 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)

   Digita il valore che intendi includere negli URL per l'argomento di query `fle-profile`. Questo valore indica CloudFront di utilizzare l'ID del profilo (specificato nel campo successivo) associato a questo argomento di interrogazione per la crittografia a livello di campo per 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 se desideri consentire alla richiesta di passare all'origine se il profilo specificato in un argomento della 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 AWS 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 AWS 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 AWS CloudFormation o nell' CloudFront API, `OriginProtocolPolicy` deve essere impostato su `match-viewer` o`https-only`.)

Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.

Decrittografa i campi dati alla tua 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 gli spettatori 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 Pubblica 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 Configurare 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.

> **Tip**
>
> Puoi scoprire come utilizzare un AWS CloudFormation modello per implementare una AWS soluzione VOD insieme a tutti i componenti associati. Per vedere i passaggi per l'utilizzo del modello, consulta Distribuzione automatizzata nella guida Video on Demand di AWS.

Configurare 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 Aggiungere, rimuovere o sostituire i contenuti CloudFront distribuiti.

Per informazioni sui client Smooth Streaming, vedere Smooth Streaming nel sito Web della documentazione Microsoft.

Da utilizzare CloudFront per distribuire file Smooth Streaming quando un server Web Microsoft IIS non è l'origine

1. Codifica i tuoi file multimediali in formato MP4 frammentato Smooth Streaming.
2. Esegui una di queste operazioni:
   - Se utilizzi la CloudFront console: quando crei o aggiorni una distribuzione, abilita Smooth Streaming in uno o più comportamenti di 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 video in streaming live 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:

- Converti i tuoi contenuti nei formati richiesti e poi servili: se hai bisogno di contenuti in più formati, AWS Elemental MediaPackageusali per impacchettare i contenuti per diversi tipi di dispositivi. 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 CloudFront per fornire contenuti MediaPackage formattati, consultaPubblica 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 la tua origine utilizzando una di queste opzioni, puoi distribuire video in streaming live agli spettatori utilizzando 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

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 “Origin Path (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. Politica del protocollo Viewer: scegli Reindirizza HTTP a HTTPS. Per ulteriori informazioni, consulta the section called “Viewer Protocol Policy (Policy protocollo visualizzatore)”.

    e. Politica di cache e politica di richiesta Origin

        - 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 “Distribution Settings (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

Pubblica 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 processo seguente presuppone che tu abbia già creato un canale e aggiunto gli endpoint per l'utilizzo del tuo video in diretta. MediaPackage

Per creare MediaPackage manualmente una CloudFront distribuzione per, segui questi passaggi:

Fasi

- Passaggio 1: creare e configurare una CloudFront distribuzione
- Passaggio 2: aggiungi Origins per i domini dei tuoi endpoint MediaPackage
- Fase 3: configurazione dei comportamenti della cache per tutti gli endpoint
- Fase 4: Abilita l'autorizzazione CDN basata sull'intestazione MediaPackage
- Passaggio 5: utilizzare CloudFront per servire il canale di live streaming

Passaggio 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 AWS Management Console 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.

Il campo Percorso di origine non è stato compilato per l'utente. Devi immettere manualmente il percorso di origine corretto.

Per ulteriori informazioni su come funziona un percorso di origine, consulta the section called “Origin Path (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 “Distribution Settings (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 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 per gli URL. CloudFront Per ulteriori informazioni, consulta the section called “Personalizza gli URL dei file”.

Personalizza fino all'ultimo istante 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 un'estensione AWS Lambdache offre un'elaborazione potente e flessibile per funzioni complesse e una logica applicativa completa più vicina agli utenti ed è altamente sicura. 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. Funziona per le richieste e le risposte di Viewer e Origin.

Argomenti

- Differenze tra CloudFront Functions e Lambda @Edge
- Personalizza a 360° con CloudFront Functions
- Personalizzazione all'avanguardia 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 delle chiavi della cache: trasforma gli attributi della richiesta HTTP (intestazioni, stringhe di query, cookie e persino il percorso dell'URL) per creare una chiave di cache ottimale, in grado di migliorare il rapporto di accessi alla cache.
- Manipolazione dell'intestazione: inserisce, modifica o elimina le intestazioni HTTP nella richiesta o nella risposta. Ad esempio, è possibile aggiungere una intestazione `True-Client-IP` a ogni richiesta.
- Reindirizzamenti o riscritture degli URL: reindirizza gli utenti ad altre pagine in base alle informazioni contenute nella richiesta o riscrivi tutte le richieste da un percorso all'altro.
- Richiedi autorizzazione: convalida i token di autorizzazione con hash, come i token web JSON (JWT), esaminando le intestazioni di autorizzazione o altri metadati delle richieste.

Per CloudFront iniziare a usare Functions, consulta. Personalizza a 360° con CloudFront Functions

Lambda @Edge è ideale per i seguenti casi d'uso:

- Funzioni che richiedono diversi millisecondi o più per essere completate
- 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 all'avanguardia 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.

	CloudFront Funzioni	Lambda@Edge
Linguaggi di programmazione	JavaScript (conforme a ECMAScript 5.1)	Node.js e Python
Origini eventi	• Richiesta visualizzatore • Risposta visualizzatore	• Richiesta visualizzatore • Risposta visualizzatore • Richiesta origine • Risposta origine
Supporti Amazon CloudFront KeyValueStore	Sì CloudFront KeyValueStore supporta solo il JavaScript runtime 2.0	No
Dimensionare	10.000.000 di richieste al secondo o più	Fino a 10.000 richieste al secondo per regione
Durata della funzione	Submillisecondo	Fino a 5 secondi (richiesta del visualizzatore e risposta del visualizzatore) Fino a 30 secondi (richiesta origine e risposta origine)
Memoria massima Per ulteriori informazioni, consulta la pagina relativa alle quote di .	2 MB	128 MB — 10.240 MB (10 GB)
Dimensione massima del codice funzione e delle librerie incluse	10 KB	1 MB (richiesta del visualizzatore e risposta del visualizzatore)

	CloudFront Funzioni	Lambda@Edge
		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 e risposta del visualizzatore) Sì (richiesta di origine e risposta di origine)
Può creare e testare interamente all'interno CloudFront	Sì	No
Registrazione delle funzioni e parametri	Sì	Sì
Prezzi	Livello gratuito disponibile; addebito per richiesta	Nessun livello gratuito; addebito per richiesta e durata della funzione

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)

Per ulteriori informazioni sulle CloudFront funzioni, consultate i seguenti argomenti:

Argomenti

- Tutorial: crea una funzione semplice con CloudFront Functions
- Tutorial: crea una CloudFront funzione che includa valori chiave
- Scrivi il codice della funzione
- Creazione di funzioni
- Funzioni di test
- Funzioni di aggiornamento
- Funzioni di pubblicazione
- Associa le funzioni alle distribuzioni
- Amazon CloudFront KeyValueStore

Tutorial: crea una funzione semplice con CloudFront Functions

Questo tutorial mostra come iniziare a usare CloudFront Functions. Puoi creare una semplice funzione che reindirizza il visualizzatore a un URL diverso e che restituisca anche un'intestazione di risposta personalizzata.

Indice

Prerequisiti

Per utilizzare CloudFront Functions, è necessaria una distribuzione. CloudFront Se non disponi di un account, consulta Inizia con una CloudFront distribuzione di base.

Creazione della funzione

Puoi utilizzare la CloudFront console per creare una semplice funzione che reindirizza il visualizzatore a un URL diverso e restituisce anche un'intestazione di risposta personalizzata.

Per creare una funzione CloudFront

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Funzioni, quindi scegli Crea funzione.
3. Nella pagina Crea funzione, in Nome, inserisci un nome di funzione come *`MyFunctionName`*.
4. (Facoltativo) In Descrizione, inserite una descrizione per la funzione, ad esempio**`Simple test function`**.
5. Per Runtime, mantieni la JavaScript versione selezionata di default.
6. Scegli Crea funzione.
7. Copia il seguente codice di funzione. 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 il codice Function, incolla il codice nell'editor di codice per sostituire il codice predefinito.
9. Seleziona Salvataggio delle modifiche.
10. (Facoltativo) È possibile testare la funzione prima di pubblicarla. Questo tutorial non descrive come testare una funzione. Per ulteriori informazioni, consulta Funzioni di test.

11. Scegli la scheda Pubblica, quindi scegli la funzione Pubblica. È necessario pubblicare la funzione prima di poterla associare alla CloudFront distribuzione.
12. Successivamente, è possibile associare la funzione a un comportamento di distribuzione o cache. Nella *MyFunctionName*pagina, scegli la scheda Pubblica.

    > **Warning**
    >
    > Nei passaggi seguenti, scegli una distribuzione o un comportamento della cache da utilizzare per i test. Non associate questa funzione di test a un comportamento di distribuzione o cache utilizzato in produzione.

13. Scegliere Add Association (Aggiungi associazione).
14. Nella finestra di dialogo Associa, scegliete una distribuzione e/o un comportamento della cache. Per Tipo di evento, mantenete 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, seleziona la distribuzione nella tabella Distribuzioni associate, quindi scegli Visualizza distribuzione.

    Quando lo stato della distribuzione è Distribuito, sarà possibile verificare che la funzione funziona.

Verifica la funzione

Dopo aver distribuito la funzione, puoi verificare che funzioni per la tua distribuzione.

Per verificare la funzione

1. Nel tuo browser web, accedi al nome di dominio della tua 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 inviare una richiesta al nome di dominio della tua 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. La tua risposta potrebbe essere simile all'esempio seguente.

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: crea una CloudFront funzione che includa valori chiave

Questo tutorial mostra come includere i valori chiave nella CloudFront funzione. I valori chiave fanno parte di una coppia chiave-valore. Il nome (dalla 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 chiave. 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

- Crea il Key Value Store
- Aggiungi coppie chiave-valore all'archivio chiave-valore
- Associa l'archivio di valori chiave alla funzione
- Testate e pubblicate il codice della funzione

Prerequisiti

Se non conosci CloudFront le funzioni di Functions e l'archivio di valori chiave, ti consigliamo di seguire il tutorial in. the section called “Tutorial: Crea una CloudFront funzione semplice”

Dopo aver completato il tutorial, puoi seguire questo tutorial per estendere la funzione che hai creato. Per questo tutorial, ti consigliamo di creare prima l'archivio di valori chiave.

Crea il Key Value Store

Innanzitutto, crea l'archivio di valori chiave da utilizzare per la tua funzione.

Per creare l'archivio di valori chiave

1. Pianificate 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 chiave-valore.
2. Decidi l'ordine di lavoro. Puoi procedere in due modi:
   - Create un archivio chiave-valore e aggiungete coppie chiave-valore all'archivio. 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 chiave e aggiungi le coppie chiave-valore.
3. Accedi a AWS Management Console e apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
4. Nel riquadro di navigazione, scegli Funzioni, quindi scegli la KeyValueStoresscheda.
5. Scegli Crea KeyValueStore e inserisci i seguenti campi:
   - Inserisci un nome e una descrizione (opzionale) per il negozio.
   - Lascia vuoto l'URI S3. In questo tutorial inserirai manualmente le coppie chiave-valore.
6. Scegli 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.

Aggiungi coppie chiave-valore all'archivio chiave-valore

Quindi, aggiungi manualmente un elenco di coppie chiave-valore all'archivio chiave-valore creato in precedenza.

Per aggiungere coppie chiave-valore all'archivio chiave-valore

1. Nella sezione Coppie chiave-valore, scegli Aggiungi coppie chiave-valore.
2. Scegli Aggiungi coppia, quindi inserisci una chiave e un valore. Scegli il segno di spunta per confermare le modifiche e ripeti questo passaggio per aggiungerne altre.
3. Al termine, scegli Salva modifiche per salvare le coppie chiave-valore nell'archivio chiave-valore. Nella finestra di dialogo di conferma, scegli Fine.

Ora hai un archivio chiave-valore che contiene un gruppo di coppie chiave-valore.

Associa l'archivio di valori chiave 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.

Per associare l'archivio di valori chiave alla funzione

1. Nel riquadro di navigazione, seleziona Funzioni. Per impostazione predefinita, la scheda Funzioni viene visualizzata in alto.
2. Scegliete il nome della funzione e nella KeyValueStore sezione Associato, scegliete Associa esistente KeyValueStore.
3. Seleziona l'archivio di valori chiave e scegli Associa KeyValueStore.

> **Note**
>
> È possibile associare solo un archivio di valori chiave a ciascuna funzione.

Testate e pubblicate il codice della funzione

Dopo aver associato il key value store alla funzione, è possibile 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
- Modificate la funzione e il relativo archivio di valori chiave per includere una nuova coppia chiave-valore.
- Modifica il valore di una coppia chiave-valore.

Per testare e pubblicare il codice della funzione

1. Per ulteriori informazioni su come testare una funzione, consulta the section called “Funzioni di test”. Verifica di aver scelto di testare la funzione nella fase `DEVELOPMENT`.
2. Pubblica la funzione quando sei pronto per utilizzarla (con le coppie chiave-valore nuove o modificate) in un `LIVE` ambiente.

   Quando CloudFront pubblicate, copia la versione della funzione dallo `DEVELOPMENT` stage al live stage. 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 “Funzioni di pubblicazione”.

Scrivi il 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.

Argomenti

- JavaScript funzionalità di runtime per CloudFront Functions
- Metodi helper per archivi di valori delle chiavi
- Codice di esempio per CloudFront le funzioni

Determina lo scopo della tua 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
- 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.

Quando crei una funzione che modifica la richiesta HTTP, assicurati di scegliere il tipo di evento richiesta del visualizzatore . Ciò significa che la funzione viene eseguita ogni volta che si 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.

Informazioni correlate

Per ulteriori informazioni sull'utilizzo CloudFront delle funzioni, consultate i seguenti argomenti:

- Struttura degli eventi
- JavaScript funzionalità di runtime
- Codice di esempio
- 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
- 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 associata all'evento.

`distributionId`

L'ID della distribuzione (ad esempio, EDFDVBD6EXAMPLE) associata all'evento.

`eventType`

Il tipo di evento, `viewer-request` o `viewer-response`.

`requestId`

Una stringa che identifica in modo univoco una richiesta (e la risposta associata). CloudFront

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 da visualizzatore a HTTP. CloudFront 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 della funzione restituisce un`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 modifica il `uri` valore, 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 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 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 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 HTTP CloudFront -to-viewer. 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 della funzione, usa 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

denominataexample-header-name, la CloudFront converte nella richiesta o Example-Header-Name nella risposta HTTP.

Example Esempio

Considerate l'Hostintestazione seguente 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

Considerate una richiesta HTTP con le seguenti Accept intestazioni.

```
Accept: application/json
Accept: application/xml
Accept: text/html
```

Queste intestazioni sono rappresentate come segue nell'`request`oggetto.

```
"headers": {
    "accept": {
        "value": "application/json",
        "multiValue": [
            {
                "value": "application/json"
            },
            {
                "value": "application/xml"
            },
            {
                "value": "text/html"
            }
        ]
    }
}
```

> **Note**
>
> Il primo valore di 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

Consideriamo una richiesta con un'`Accept`intestazione che contiene tre valori.

```
Accept: application/json, application/xml, text/html
```

Questa intestazione è rappresentata come segue nell'`request`oggetto.

```
"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.

> **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"
                    }
                ]
            }
        }
    }
```

```
}
```

JavaScript funzionalità di runtime per CloudFront Functions

L'ambiente JavaScript di runtime CloudFront Functions è conforme alla versione 5.1 di ECMAScript (ES) e supporta anche alcune funzionalità delle versioni ES da 6 a 12.

Per la maggior parte delle up-to-date funzionalità, si consiglia di utilizzare runtime 2.0. JavaScript

Le funzionalità JavaScript di runtime 2.0 presentano le seguenti modifiche rispetto alla versione 1.0:

- Sono disponibili i 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 ritorno viene modificato in `Buffer` se non viene fornita alcuna codifica
  - `hmac.digest()`— Il tipo restituito viene modificato in `Buffer` se non viene fornita alcuna codifica
- Per ulteriori informazioni sulle nuove funzionalità aggiuntive, vedereJavaScript Funzionalità di runtime 2.0 per CloudFront Functions.

Argomenti

- JavaScript Funzionalità di runtime 1.0 per CloudFront Functions
- JavaScript Funzionalità di runtime 2.0 per CloudFront Functions

JavaScript Funzionalità di runtime 1.0 per CloudFront Functions

L'ambiente JavaScript di runtime di CloudFront Functions è conforme alla versione 5.1 di ECMAScript (ES) e supporta anche alcune funzionalità delle versioni ES 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 di runtime di CloudFront Functions, l'`Math.random()`implementazione utilizza `arc4random` OpenBSD con il timestamp di quando la funzione viene eseguita.

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**
>
> CloudFront Le funzioni non supportano la sintassi delle virgole, ad esempio. `console.log('a', 'b')` Utilizza invece il `console.log('a' + ' ' + 'b')` formato.

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 CloudFront Functions analizza automaticamente le stringhe di query URL per voi. 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 JavaScript linguistiche 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 alla rete

Non è disponibile alcun supporto per le chiamate di rete. Ad esempio, XHR, HTTP(S) e socket non sono supportati.

JavaScript Funzionalità di runtime 2.0 per CloudFront Functions

L'ambiente JavaScript di runtime di CloudFront Functions è conforme alla versione 5.1 di ECMAScript (ES) e supporta anche alcune funzionalità delle versioni ES 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:

- `async`
- `await`
- `const`
- `let`

> **Note**
>
> `async`, `await`const, e `let` sono nuovi nel runtime 2.0. JavaScript

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()`sono nuove nel JavaScript runtime 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 sono nuovi nel JavaScript runtime 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 di runtime di CloudFront Functions, l'`Math.random()`implementazione utilizza `arc4random` OpenBSD con il timestamp di quando la funzione viene eseguita.

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.stickye` `RegExp.prototype.flags` sono nuove in runtime 2.0. JavaScript

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]()`sono nuove nel JavaScript runtime 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()` sono nuove nel JavaScript runtime 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.proto`
> `TypedArray.prototype.findIndex()``TypedArray.prototype.forEach()`,`TypedArra`
> `TypedArray.prototype.reduceRight()``TypedArray.prototype.reverse()`,
> e `TypedArray.prototype.some()` sono nuovi nel JavaScript runtime 2.0.

ArrayBuffer

Sono supportati i seguenti metodi ES 6 su ArrayBuffer :

- `isView()`

Sono supportati i seguenti metodi prototipali 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()` sono nuovi nel JavaScript runtime 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 prototipali di Dataview ES 6 sono nuovi in JavaScript runtime 2.0.

Symbol

Sono supportati i seguenti metodi ES 6:

- `Symbol.for()`
- `Symbol.keyfor()`

> **Note**
>
> Tutti i metodi Symbol ES 6 sono nuovi in JavaScript runtime 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()` sono nuovi nel JavaScript runtime 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 sono nuovi in runtime 2.0. JavaScript

Stringa di query

> **Note**
>
> L'oggetto evento CloudFront Functions analizza automaticamente le stringhe di query URL per voi. 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 JavaScript linguistiche 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.

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

Questa sezione si applica se si utilizza CloudFront Key Value Store per includere valori chiave nella funzione creata. 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, assicuratevi di aver associato un archivio di valori chiave alla funzione.

Quindi, includete le seguenti istruzioni nelle prime righe del codice della funzione:

```
import cf from 'cloudfront';
const kvsId = "key value store ID";
const kvsHandle = cf.kvs(kvsId);
```

Il tuo *Key Value Store ID* potrebbe essere simile al seguente: `a1b2c3d4-5678-90ab-cdef-EXAMPLE1`

Metodo **`get()`**

Utilizzate questo metodo per restituire il valore della chiave per il nome di chiave specificato.

Richiesta

```
get("key", options);
```

- `key`: il nome della chiave di cui è necessario recuperare il valore
- `options`: C'è un'opzione,`format`. Assicura che la funzione analizzi correttamente i dati. Valori possibili:
  - `string`: con codifica UTF8 (impostazione predefinita)
  - `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.

Metodo **`exists()`**

Utilizzate questo metodo per identificare se la chiave esiste o meno nell'archivio dei valori della chiave.

Richiesta

```
exists("key");
```

Esempio di richiesta

```
const exist = await kvsHandle.exists("myFunctionkey");
```

Risposta

La risposta è una `promise` che restituisce un valore booleano (`trueofalse`). Questo valore specifica se la chiave esiste o meno nell'archivio dei valori della chiave.

Gestione degli errori

Il `get()` metodo restituirà un errore quando la chiave richiesta non esiste nell'archivio di valori chiave associato. Per gestire questo caso d'uso, puoi aggiungere un `catch` blocco `try` and al codice.

Metodo **`meta()`**

Utilizzate questo metodo per restituire i metadati relativi all'archivio di valori chiave.

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
```

Codice di esempio per CloudFront le funzioni

Per aiutarti a iniziare a scrivere codice funzionale per CloudFront Functions, consulta i seguenti esempi. Puoi trovare questi esempi anche nel amazon-cloudfront-functions repository su GitHub.

Argomenti

Aggiunta di una intestazione Cache-Control alla risposta

La seguente funzione di risposta del visualizzatore aggiunge un'intestazione `Cache-Control` HTTP alla risposta. L'intestazione utilizza la direttiva `max-age` per indicare ai browser Web di memorizzare

nella cache la risposta per un massimo di due anni (63.072.000 secondi). Per ulteriori informazioni, consulta Cache-Control nel sito Web MDN Web Docs.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    const response = event.response;
    const headers = response.headers;

    // Set the cache-control header
     headers['cache-control'] = {value: 'public, max-age=63072000'};

    // Return response to viewers
    return response;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set the cache-control header
    headers['cache-control'] = {value: 'public, max-age=63072000'};

    // Return response to viewers
    return response;
}
```

Aggiunta di una intestazione CORS (cross-origin resource sharing) alla risposta

La seguente funzione di risposta del visualizzatore aggiunge un'intestazione `Access-Control-Allow-Origin` HTTP alla risposta se la risposta non contiene già questa intestazione. Questa intestazione fa parte della condivisione delle risorse di origine incrociata (CORS). Il valore dell'intestazione (*) indica ai browser Web di consentire al codice da qualsiasi origine di accedere a questa risorsa. Per ulteriori informazioni, consulta Access-Control-Allow-Origin nel sito Web MDN Web Docs.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event)  {
    const request = event.request;
    const response  = event.response;

    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!response.headers['access-control-allow-origin'] &&
 request.headers['origin']) {
        response.headers['access-control-allow-origin'] = {value:
 request.headers['origin'].value};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

JavaScript runtime 1.0

```
function handler(event)  {
    var response  = event.response;
    var headers  = response.headers;

    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!headers['access-control-allow-origin']) {
        headers['access-control-allow-origin'] = {value: "*"};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

Aggiunta di una intestazione CORS (cross-origin resource sharing) alla richiesta

La seguente funzione di richiesta del visualizzatore aggiunge un'intestazione `Origin` HTTP alla richiesta se la richiesta non contiene già questa intestazione. Questa intestazione fa parte della condivisione delle risorse di origine incrociata (CORS). Questo esempio imposta il valore

dell'intestazione sul valore nell'intestazione `Host` della richiesta. Per ulteriori informazioni, consulta Origin nel sito Web MDN Web Docs.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const host = request.headers.host.value;

   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;

   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

Aggiunta di intestazioni di sicurezza alla risposta

La seguente funzione di risposta del visualizzatore aggiunge alla risposta diverse intestazioni HTTP comuni relative alla sicurezza. Per ulteriori informazioni, consulta le pagine seguenti nel sito Web MDN Web Docs:

- Strict-Transport-Security
- Content-Security-Policy

- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    const response = event.response;
    const headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'; frame-ancestors
 'none'"};
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};
    headers['referrer-policy'] = {value: 'same-origin'};

    // Return the response to viewers
    return response;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'"};
```

```
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};

    // Return the response to viewers
    return response;
}
```

Aggiunta di una intestazione True-Client-IP alla richiesta

La seguente funzione di richiesta del visualizzatore aggiunge un'intestazione `True-Client-IP` HTTP alla richiesta, con l'indirizzo IP del visualizzatore come valore dell'intestazione. Quando CloudFront invia una richiesta a un'origine, l'origine può determinare l'indirizzo IP dell' CloudFront host che ha inviato la richiesta ma non l'indirizzo IP del visualizzatore (client) a cui ha inviato la richiesta originale. CloudFront Questa funzione aggiunge l'intestazione `True-Client-IP` in modo che l'origine possa vedere l'indirizzo IP del visualizzatore.

> **Important**
>
> Per assicurarti che CloudFront includa questa intestazione nelle richieste di origine, devi aggiungerla all'elenco delle intestazioni consentite in una politica di richiesta di origine.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
```

```
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

Reindirizzamento del visualizzatore a un nuovo URL

La seguente funzione di richiesta del visualizzatore genera una risposta per reindirizzare lo spettatore a un URL specifico del paese quando la richiesta proviene da un determinato paese. Questa funzione si basa sul valore dell'intestazione `CloudFront-Viewer-Country` per determinare il paese del visualizzatore.

> **Important**
>
> Affinché questa funzione funzioni, è necessario configurare l'aggiunta dell'`CloudFront-Viewer-Country`intestazione CloudFront alle richieste in entrata aggiungendola alle intestazioni consentite in una politica di cache o in una politica di richiesta di origine.

Questo esempio reindirizza il visualizzatore a un URL specifico della Germania quando la richiesta del visualizzatore proviene dalla Germania. Se la richiesta del visualizzatore non proviene dalla Germania, la funzione restituisce la richiesta originale e non modificata.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const host = request.headers.host.value;
    const country = Symbol.for('DE'); // Choose a country code
    const newurl = `https://${host}/de/index.html`; // Change the redirect URL to
 your choice

    if (headers['cloudfront-viewer-country']) {
        const countryCode = Symbol.for(headers['cloudfront-viewer-country'].value);
```

```
        if (countryCode === country) {
            const response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;
    var country = 'DE' // Choose a country code
    var newurl = `https://${host}/de/index.html` // Change the redirect URL to your
 choice

    if (headers['cloudfront-viewer-country']) {
        var countryCode = headers['cloudfront-viewer-country'].value;
        if (countryCode === country) {
            var response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

Per ulteriori informazioni su riscritture e reindirizzamenti, consulta Gestione delle riscritture e dei reindirizzamenti utilizzando le funzioni edge in Workshop Studio. AWS

Aggiunta di index.html agli URL di richiesta che non includono un nome file

La seguente funzione di richiesta del visualizzatore viene aggiunta `index.html` alle richieste che non includono un nome di file o un'estensione nell'URL. Questa funzione può essere utile per applicazioni a pagina singola o siti Web generati staticamente che sono ospitati in un bucket Amazon S3.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
async function handler(event) {
    const request = event.request;
    const uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }

    return request;
}
```

JavaScript runtime 1.0

```
function handler(event) {
    var request = event.request;
    var uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }

    return request;
```

```
}
```

Convalida di un token semplice nella richiesta

La seguente funzione di richiesta del visualizzatore convalida un token web JSON (JWT) nella stringa di query di una richiesta. Se il token è valido, la funzione restituisce la richiesta originale non modificata a. CloudFront Se il token non è valido, la funzione genera una risposta di errore. Questa funzione utilizza il modulo `crypto`. Per ulteriori informazioni, consulta Moduli incorporati.

Questa funzione presuppone che le richieste contengano un valore JWT in un parametro stringa di query denominato `jwt`.

> **Warning**
>
> Per utilizzare questa funzione, è necessario inserire la chiave segreta nel codice funzione.

Vedi questo esempio su. GitHub

JavaScript runtime 2.0

```
const crypto = require('crypto');

//Response when JWT is not valid.
const response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    const segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
    }

    // All segment should be base64
```

```
    const headerSeg = segments[0];
    const payloadSeg = segments[1];
    const signatureSeg = segments[2];

    // base64 decode and parse JSON
    const header = JSON.parse(_base64urlDecode(headerSeg));
    const payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        const signingMethod = 'sha256';
        const signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        const signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType, signatureSeg)) {
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }

        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }

    return payload;
}

//Function to ensure a constant time comparison to prevent
//timing side channels.
function _constantTimeEquals(a, b) {
    if (a.length != b.length) {
        return false;
    }

    var xor = 0;
    for (var i = 0; i < a.length; i++) {
    xor |= (a.charCodeAt(i) ^ b.charCodeAt(i));
    }
```

```
    return 0 === xor;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return _constantTimeEquals(signature, _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}

function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return Buffer.from(str, 'base64url')
}

function handler(event) {
    const request = event.request;
    //Secret key used to verify JWT token.
    //Update with your own key.
    var key = "LzdWGpAToQ1DqYuzHxE6YOqi7G3X2yvNBot9mCXfx5k";

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        console.log("Error: No JWT in the querystring");
        return response401;
    }

    const jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, key);
    }
    catch(e) {
        console.log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
```

```
    delete request.querystring.jwt;
    console.log("Valid JWT token");
    return request;
}
```

JavaScript runtime 1.0

```
var crypto = require('crypto');

//Response when JWT is not valid.
var response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    var segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
    }

    // All segment should be base64
    var headerSeg = segments[0];
    var payloadSeg = segments[1];
    var signatureSeg = segments[2];

    // base64 decode and parse JSON
    var header = JSON.parse(_base64urlDecode(headerSeg));
    var payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        var signingMethod = 'sha256';
        var signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        var signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType, signatureSeg)) {
```

```
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }

        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }

    return payload;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return (signature === _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}

function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return String.bytesFrom(str, 'base64url')
}

function handler(event) {
    var request = event.request;

    //Secret key used to verify JWT token.
    //Update with your own key.
    var key = "LzdWGpAToQ1DqYuzHxE6YOqi7G3X2yvNBot9mCXfx5k";

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        console.log("Error: No JWT in the querystring");
```

```
        return response401;
    }

    var jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, key);
    }
    catch(e) {
        console.log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    console.log("Valid JWT token");
    return request;
}
```

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.

```
async function answer() {
    return 42;
}

// Note: async, await can be used only inside an async function.

async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
```

```
    let answer_value = await answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

Il JavaScript codice di esempio seguente mostra come visualizzare le promesse con il metodo `then` chain. È possibile utilizzare `catch` per visualizzare gli errori.

```
async function answer() {
    return 42;
}

async function squared_answer() {
   return answer().then(value => value * value)
}
// note async, await can be used only inside async function
async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await squared_answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

Normalizzazione dei parametri della stringa di query

È possibile normalizzare i parametri della stringa di query per migliorare la percentuale di riscontri nella cache.

L'esempio seguente funziona con i JavaScript runtime 1.0 e 2.0. L'esempio mostra come migliorare il rapporto di accessi alla cache inserendo le stringhe di query in ordine alfabetico prima di CloudFront inoltrare le richieste all'origine.

```
function handler(event) {
     var qs=[];
     for (var key in event.request.querystring) {
         if (event.request.querystring[key].multiValue) {
             event.request.querystring[key].multiValue.forEach((mv) => {qs.push(key +
 "=" + mv.value)});
         } else {
             qs.push(key + "=" + event.request.querystring[key].value);
```

```
        }
    };

    event.request.querystring = qs.sort().join('&');


    return event.request;
}
```

Usa coppie chiave-valore in una funzione

È possibile utilizzare coppie chiave-valore da un archivio chiave-valore in una funzione.

> **Note**
>
> È necessario utilizzare JavaScript runtime 2.0 per il seguente esempio di codice.

L'esempio mostra una funzione che utilizza il contenuto dell'URL nella richiesta HTTP per cercare un percorso personalizzato nell'archivio di valori chiave. CloudFront quindi utilizza quel percorso personalizzato per effettuare la richiesta. Questa funzione aiuta a gestire i percorsi multipli che fanno parte di un sito Web.

```
import cf from 'cloudfront';

// Declare the ID of the key value store that you have associated with this function
// The import fails at runtime if the specified key value store is not associated with
 the function

const kvsId = "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111";

const kvsHandle = cf.kvs(kvsId);

async function handler(event) {
    const request = event.request;
    // Use the first segment of the pathname as key
    // For example http(s)://domain/<key>/something/else
    const pathSegments = request.uri.split('/')
    const key = pathSegments[1]
    try {
        // Replace the first path of the pathname with the value of the key
```

```
        // For example http(s)://domain/<value>/something/else
        pathSegments[1] = await kvsHandle.get(key);
        const newUri = pathSegments.join('/');
        console.log(`${request.uri} -> ${newUri}`)
        request.uri = newUri;
    } catch (err) {
        // No change to the pathname if the key is not found
        console.log(`${request.uri} | ${err}`);
    }
    return request;
}
```

Creazione di funzioni

La creazione di una funzione avviene 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
   - the section called “Struttura degli eventi”
   - Codice di esempio per CloudFront le funzioni
2. CloudFront Utilizzatelo 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 CloudFront console all'indirizzo https://console.aws.amazon.com/cloudfront/v4/home#/functions e scegli la pagina Funzioni.
2. Scegli Crea funzione.
3. Inserisci un nome di funzione univoco all'interno di Account AWS, scegli la JavaScript versione, quindi scegli 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, scegliete la scheda Build e immettete il codice della funzione. Il codice di esempio incluso nella scheda Compila illustra la sintassi di base del codice funzione.
5. Seleziona Salvataggio delle modifiche.
6. Se il codice della funzione utilizza coppie chiave-valore, è necessario associare un archivio chiave-valore.

   È possibile associare l'archivio di valori chiave quando si crea la funzione per la prima volta. In alternativa, è possibile associarlo in un secondo momento, aggiornando la funzione.

   Per associare subito un archivio di valori delle chiavi, procedi come segue:

   - Vai alla KeyValueStore sezione Associa e scegli Associa esistente KeyValueStore.
   - Seleziona l'archivio chiave-valore che contiene le coppie chiave-valore nella funzione, quindi scegli Associa. KeyValueStore

   CloudFront associa immediatamente lo store 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 `fileb://` notazione 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, è possibile associare l'archivio chiave-valore quando si crea la funzione per la prima volta. In alternativa, è possibile associarla 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 ogni volta che si modifica l'archivio di valori chiave. Utilizzate questo valore e il nome della funzione per fare riferimento alla funzione in futuro. Assicuratevi di utilizzare sempre la corrente`ETag`.
> - `FunctionARN`— L'ARN per la tua CloudFront funzione.
> - 111122223333 — Il. Account AWS
> - `Stage`— Lo stadio della funzione (`LIVE`o`DEVELOPMENT`).
> - `Status`— Lo stato della funzione (`PUBLISHED`o`UNPUBLISHED`).

Dopo aver creato la funzione, questa viene aggiunta allo `DEVELOPMENT` stage. Ti consigliamo di testare la tua funzione prima di pubblicarla. Dopo aver pubblicato la funzione, la funzione passa allo `LIVE` stage.

Funzioni di test

Prima di implementare la funzione nella fase live (produzione), puoi testarla per verificare che funzioni come previsto. Per testare una funzione, specificate un oggetto evento che rappresenta una richiesta o una risposta HTTP che la CloudFront distribuzione potrebbe ricevere in produzione.

CloudFront Functions esegue le seguenti operazioni:

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 “Comprendi l'utilizzo del calcolo”.

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

È possibile configurare un oggetto evento nell'editor visivo della CloudFront console e non salvarlo.

È possibile utilizzare questo oggetto evento per testare la funzione dalla CloudFront console, anche se non è stato salvato.

Opzione 2: creazione di un oggetto evento nell'editor visuale

È possibile configurare un oggetto evento nell'editor visivo della CloudFront console e non salvarlo. È possibile creare 10 oggetti evento per ogni funzione, ad esempio per testare diversi input possibili.

Quando create l'oggetto evento in questo modo, potete utilizzare l'oggetto evento per testare la funzione nella CloudFront console. Non puoi usarlo per testare la funzione utilizzando un' AWS API o un SDK.

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. Ma non puoi usarlo per testare la funzione nella CloudFront console.

Per creare un oggetto evento (opzione 1 o 2)

1. Accedi alla CloudFront console 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, scegliete 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 la risposta del visualizzatore. Vengono visualizzate le sezioni Richiesta e Risposta.

4. Compila i campi da includere nell'evento. Puoi scegliere Modifica JSON per visualizzare il file JSON non elaborato.
5. (Facoltativo) Per salvare l'evento, scegliete Salva e nel campo Salva evento di test, inserite un nome, quindi scegliete Salva.

   Puoi anche scegliere Modifica JSON e copiare il file JSON non elaborato e salvarlo nel tuo file, all'esterno di. CloudFront

Per 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 seguire 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, vedere. Struttura degli eventi

Test della funzione

È possibile testare una funzione nella CloudFront console o con AWS Command Line Interface (AWS CLI).

Console

Per testare la funzione

1. Accedi alla CloudFront console 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, scegli un altro evento nel campo Seleziona evento di test.
5. Scegliete la funzione Test. La console mostra l'output della funzione, inclusi i registri delle funzioni e l'utilizzo del calcolo.

CLI

È possibile 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 `fileb://` notazione per passare il file dell'oggetto dell'evento. 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 “Comprendi l'utilizzo del calcolo”.
- `FunctionOutput` contiene l'oggetto evento restituito dalla funzione.

Comprendi l'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, limita la funzione CloudFront . L'elenco seguente illustra la probabilità che una funzione venga limitata in base al valore di utilizzo del calcolo.

Valore di utilizzo del calcolo:

- 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).
- Da 51 a 70: la funzione si sta avvicinando al tempo massimo consentito. Prendere in considerazione l'ottimizzazione del codice della funzione.
- 71-100: la funzione è molto vicina o supera il tempo massimo consentito. CloudFront è probabile che limiti questa funzione se la si associa a una distribuzione.

Funzioni di aggiornamento

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 dallo `DEVELOPMENT` stage a`LIVE`, è necessario pubblicare la funzione.

È possibile aggiornare il codice di una funzione nella CloudFront console o con AWS Command Line Interface (AWS CLI).

Console

Per aggiornare il codice della funzione

1. Accedi alla CloudFront console 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 seguenti modifiche:

   - Aggiorna tutti i campi nella sezione Dettagli.
   - Modifica o rimuovi l'archivio di valori chiave associato. Per ulteriori informazioni sugli archivi di valori delle chiavi, consulta the section called “Usando CloudFront KeyValueStore”.
   - Cambia il codice della funzione. Scegli la scheda Compila, apporta le modifiche, quindi scegli 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 `fileb://` notazione 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**
>
> - La funzione viene identificata tramite i rispettivi nomi e ETag (nel parametro `if-match`). Assicurati di utilizzare l'ETag corrente. Puoi recuperarlo tramite un'operazione di descrizione.
> - 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 dell'archivio di valori chiave (se presente), specificate il nome dell'archivio esistente.
>   - Per modificare l'associazione, specificare il nome del nuovo archivio di valori chiave.
>   - Per rimuovere l'associazione, omettete il `KeyValueStoreAssociations` parametro.

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 ogni volta che si modifica l'archivio di valori chiave.
> - `FunctionARN`— L'ARN per la tua CloudFront funzione.
> - `Stage`— Lo stage per la funzione (`LIVE`o`DEVELOPMENT`).
> - `Status`— Lo stato della funzione (`PUBLISHED`o`UNPUBLISHED`).

Funzioni di pubblicazione

Quando pubblicate la funzione, questa copia la funzione dallo `DEVELOPMENT` stage allo `LIVE` stage.

Se i comportamenti della cache non sono associati alla funzione, la pubblicazione consente di associarla a un comportamento della cache. Puoi associare i comportamenti della cache solo alle funzioni che si trovano nella fase `LIVE`.

> **Important**
>
> - Prima della pubblicazione, ti consigliamo di testare la funzione.
> - Dopo la pubblicazione della funzione, tutti i comportamenti della cache associati a tale funzione iniziano automaticamente a utilizzare la copia appena pubblicata, non appena le distribuzioni terminano la distribuzione.

È possibile pubblicare una funzione nella CloudFront console o con. AWS CLI

Console

Per pubblicare una funzione

1. Accedi alla CloudFront console 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 scegli Pubblica. Se la tua funzione è già associata a uno o più comportamenti della cache, scegli Pubblica e aggiorna.
4. (Facoltativo) Per vedere le distribuzioni associate alla funzione, scegliete CloudFront Distribuzioni associate per espandere la sezione.

In caso di successo, nella parte superiore della pagina viene visualizzato un banner che riporta il ***nome della funzione*** pubblicato con successo. Puoi anche scegliere la scheda Genera e quindi Live per visualizzare la versione live del codice funzione.

CLI

Per 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
```

Associa le funzioni alle distribuzioni

Per utilizzare una funzione in CloudFront Funzioni con una distribuzione, è necessario associare la funzione a uno o più comportamenti della cache nella distribuzione. Puoi associare una funzione a più comportamenti della cache in più distribuzioni.

Quando associ una funzione a un comportamento di cache, è necessario scegliere un tipo di evento. Il tipo di evento determina quando CloudFront Functions esegue la funzione. È possibile scegliere i seguenti tipi di eventi:

- Richiesta del visualizzatore: la funzione viene eseguita quando CloudFront riceve una richiesta da un visualizzatore.
- Risposta del visualizzatore: la funzione viene eseguita prima di CloudFront restituire una risposta al visualizzatore.

Non è possibile utilizzare tipi di eventi rivolti all'origine (richiesta di origine e risposta all'origine) con CloudFront Functions. Puoi invece usare Lambda @Edge. Per ulteriori informazioni, consulta la sezione CloudFront eventi che possono attivare una funzione Lambda @Edge.

> **Note**
>
> Prima di associare una funzione, è necessario pubblicarla nella fase `LIVE`.

È possibile associare una funzione a una distribuzione nella CloudFront console o alla AWS Command Line Interface (AWS CLI).

Console

È possibile utilizzare la CloudFront console per associare una funzione a un comportamento della cache esistente in una CloudFront distribuzione esistente. Per informazioni su come creare una distribuzione, consulta the section called “Creazione di una distribuzione”.

Per associare una funzione a un comportamento della cache esistente

1. Accedi alla CloudFront console 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 Funzione, scegliete la scheda Pubblica.
4. Scegliete la funzione Pubblica.
5. Scegliere Add Association (Aggiungi associazione). Nella finestra di dialogo che appare, scegli una distribuzione, un tipo di evento e/o un comportamento nella cache.

   Per il tipo di evento, scegli quando eseguire questa funzione:

   - Viewer Request: esegue la funzione ogni volta CloudFront che riceve una richiesta.
   - Viewer Response: esegue 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. Puoi scegliere Visualizza distribuzione nella pagina dei dettagli della funzione per controllare lo stato di avanzamento.

CLI

Puoi associare una funzione con uno qualsiasi di questi elementi:

- Un comportamento della cache esistente
- Un nuovo comportamento della cache in una distribuzione esistente
- Un nuovo comportamento della cache in una nuova distribuzione

Nella procedura seguente viene illustrato come associare una funzione a un comportamento della cache esistente.

Per associare una funzione a un comportamento della cache esistente

1. Aprire una finestra a riga di comando.
2. Immettete il comando seguente per salvare la configurazione di distribuzione per la distribuzione di cui desiderate associare il comportamento della 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
   ```

   Quando il comando ha successo, non AWS CLI restituisce alcun output.
3. Apri il file con il nome `dist-config.yaml` che hai 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. Non appena la nuova configurazione di distribuzione raggiunge una posizione CloudFront periferica, tale posizione inizia a utilizzare la funzione associata. Quando la distribuzione è completamente implementata, torna a `StatusDeployed`, il che indica che la CloudFront funzione associata è attiva in tutte le CloudFront edge location del mondo. In genere sono necessari pochi minuti.

Amazon CloudFront KeyValueStore

CloudFront KeyValueStore è un datastore di valori chiave sicuro, globale e a bassa latenza che consente l'accesso in lettura dall'interno di CloudFront Functions, abilitando una logica personalizzabile avanzata nelle sedi periferiche. CloudFront

Con CloudFront KeyValueStore, si effettuano aggiornamenti al codice della funzione e ai 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 essere utilizzata CloudFront KeyValueStore, la CloudFront funzione deve utilizzare JavaScript runtime 2.0.

La procedura generale per l'utilizzo delle coppie chiave-valore è la seguente:

- Crea archivi di valori chiave e compilali con un set di coppie chiave-valore. Puoi aggiungere i tuoi Key Value Store a un bucket Amazon S3 o inserirli manualmente.
- Associa gli archivi di valori chiave alla tua CloudFront funzione.
- 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 di supporto, vedere. the section called “Metodi helper per archivi di valori delle chiavi”

Per ulteriori informazioni su come iniziare CloudFront KeyValueStore, consulta il post del CloudFront KeyValueStore AWS blog Introducing Amazon.

Puoi utilizzare la CloudFront console, l' CloudFront API o un AWS SDK supportato. Per iniziare CloudFront KeyValueStore, consulta i seguenti argomenti.

Argomenti

Casi d'uso

I casi d'uso tipici delle coppie chiave-valore sono i seguenti:

- Riscritture o reindirizzamenti degli URL. La coppia chiave-valore potrebbe contenere gli URL riscritti o gli URL di reindirizzamento.
- Test A/B e flag di funzionalità. Puoi creare una funzione per condurre esperimenti assegnando una percentuale di traffico a una versione specifica del tuo sito Web.
- Autorizzazione di accesso. È possibile implementare il controllo degli accessi per consentire o rifiutare le richieste in base ai criteri definiti dall'utente e ai dati archiviati in un archivio di valori chiave.

Formati supportati per i valori

Il valore in una coppia chiave-valore può essere memorizzato in uno dei seguenti formati:

- Una stringa
- Una stringa con codifica in byte
- JSON

Sicurezza

La CloudFront funzione e tutti i relativi archivi di valori chiave vengono gestiti in modo sicuro, come segue:

- CloudFront crittografa ogni archivio di valori chiave quando è inattivo e durante il transito (durante la lettura o la scrittura negli archivi di valori chiave) quando si richiamano le CloudFront KeyValueStoreoperazioni API.
- Quando la funzione viene eseguita, CloudFront decripta ogni coppia chiave-valore in memoria nelle posizioni periferiche. CloudFront

Lavora con Key Value Store

È necessario creare un archivio di valori chiave per contenere le coppie chiave-valore che si desidera utilizzare in CloudFront Functions.

Dopo aver creato gli archivi di valori chiave e le coppie chiave-valore aggiunto, è possibile utilizzare i valori chiave nel codice della funzione. CloudFront Il JavaScript runtime 2.0 include alcuni metodi di supporto per lavorare con i valori chiave nel codice della funzione. Per ulteriori informazioni, consulta the section called “Metodi helper per archivi di valori delle chiavi”.

Argomenti

Crea un archivio di valori chiave

È possibile creare un archivio di valori chiave vuoto, quindi aggiungere coppie chiave-valore in un secondo momento. Oppure puoi creare contemporaneamente un archivio di valori chiave e le relative coppie chiave-valore.

> **Note**
>
> Se specifichi la tua origine dati da un bucket Amazon S3, devi disporre delle autorizzazioni `s3:GetObject` e delle `s3:GetBucketLocation` autorizzazioni per quel bucket. Se non disponi di queste autorizzazioni, non CloudFront puoi creare correttamente il tuo archivio di valori chiave.

Console

Per creare archivi di valori chiave (console)

1. Decidi se aggiungere coppie chiave-valore contemporaneamente alla creazione degli archivi di valori chiave. Questa funzionalità di importazione è supportata sia sulla CloudFront console che con CloudFront API e AWS SDK. Tuttavia, è supportata solo quando crei inizialmente gli archivi di valori chiave.

   Se vuoi usare un file, crealo ora.
2. Accedi AWS Management Console e apri la pagina Funzioni nella CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
3. Scegliere la scheda KeyValueStores. Scegli Crea KeyValueStore.
4. Inserisci un nome e una descrizione facoltativa per gli archivi di valori chiave.
5. Completa URI S3:
   - Se hai preparato 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.
6. Scegli Crea. L'archivio di valori chiave ora esiste.

   Viene visualizzata la pagina dei dettagli per i nuovi archivi di valori chiave. Le informazioni sulla pagina includono l'ID e l'ARN dell'archivio di valori delle chiavi.
   - L'ID è una stringa casuale di caratteri univoca nel tuo AWS account.
   - La sintassi dell'ARN è la seguente:

     Account AWS:key-value-store/il valore chiave memorizza l'ID

7. Osserva la sezione Coppie chiave-valore. Se hai importato un file, in questa sezione sono presenti alcune coppie. Altrimenti, è vuota. Puoi eseguire le operazioni indicate di seguito:

   - Se non hai importato un file da un bucket Amazon S3 e vuoi aggiungere subito coppie chiave-valore, puoi completare questa sezione.
   - Se hai importato un file, puoi anche aggiungere altri valori manualmente.
   - Puoi lasciare questa sezione vuota e aggiungere le coppie in un secondo momento, modificando gli archivi di valori chiave.

   Per aggiungere subito le coppie:

   - Scegli il pulsante Aggiungi coppie chiave-valore.
   - Scegli Aggiungi coppia e inserisci un nome e un valore.
   - Scegli il pulsante Aggiungi coppia per aggiungere altre coppie.

     Al termine, scegli Salva modifiche per salvare tutte le coppie chiave-valore nell'archivio. Nella finestra di conferma che si apre, scegli Fatto.

8. Completa la sezione Funzioni associate se desideri associare subito gli archivi di valori chiave a una funzione. È possibile creare questa associazione anche in un secondo momento, da questa pagina dei dettagli degli archivi di valori chiave o dalla pagina dei dettagli delle funzioni.

   Per creare subito l'associazione, scegli il pulsante Vai alle funzioni. Per ulteriori informazioni, consulta ??? o ???.

Programmatically

Per creare archivi di valori chiave

1. Decidi se aggiungere coppie chiave-valore contemporaneamente alla creazione degli archivi di valori chiave. (Puoi anche aggiungere una coppia chiave-valore in un secondo momento.) Questa funzionalità di importazione è supportata sia sulla CloudFront console che con CloudFront API e SDK. Ma è supportata solo quando si creano inizialmente gli archivi di valori chiave.

   Se vuoi usare un file, crealo ora.

2. Utilizza l'operazione di creazione dell' CloudFront API o del tuo AWS SDK preferito. Ad esempio, per l'API REST, usaCloudFront. CreateKeyValueStore. L'operazione richiede diversi parametri:
   - un nome;
   - un parametro `configuration` che includa un commento;
   - Un `import-source` parametro che consente di importare coppie chiave-valore da un file archiviato in un bucket Amazon S3. Tieni presente che puoi importare da un file solo durante la creazione iniziale degli archivi di valori chiave. Per informazioni sul formato del file, consulta the section called “Creare un file di 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, ETVABCEXAMPLE2), l'ARN che include il nome degli archivi di valori chiave (ad esempio,). `arn:aws:cloudfront::111122223333:key-value-store/MaxAge`

     Utilizzerai una combinazione di ETag, ARN e nome per lavorare con gli archivi di valori chiave a livello di codice.

Stati dei Key Value Store

Quando si crea un archivio di valori chiave, l'archivio dati può avere i seguenti valori di stato.

Valore	Descrizione
Approvvigionamento	L'archivio di valori chiave è stato creato e CloudFront sta elaborando l'origine dati specificata.
Pronto	L'archivio di valori chiave è stato creato e ha elaborato CloudFront correttamente l'origine dati specificata.
Importazione non riuscita	CloudFront non è stato in grado di elaborare l'origine dati specificata. Questo stato può apparire se il formato del file non è valido o se supera il limite

Valore	Descrizione
	di dimensione. Per ulteriori informazioni, consulta Creare un file di coppie chiave-valore.

Associa un archivio di valori chiave a una funzione

Per associare un archivio di valori delle chiavi a una funzione, devi intervenire sulla funzione. È necessario creare questa associazione per utilizzare le coppie chiave-valore di quell'archivio in quella funzione. Si applicano le regole seguenti:

- Una funzione può avere un solo archivio di valori delle chiavi.
- Un archivio di valori delle chiavi può essere associato a più funzioni.

Puoi utilizzare le associazioni nei modi seguenti.

- Puoi creare un'associazione tra una funzione e un archivio di valori delle chiavi:
  - Sulla CloudFront console, visualizza la pagina dei dettagli degli archivi di valori chiave e scegli il pulsante Vai alle funzioni. Viene aperta la pagina appropriata: l'elenco Funzioni (se al momento non è presente alcuna funzione associata) o la pagina dei dettagli della funzione (se al momento è presente un'associazione). Per ulteriori informazioni, consulta the section called “Associa un archivio di valori chiave a una funzione”.
  - A livello di codice, utilizza l'operazione di aggiornamento delle funzioni dell' CloudFront API o dell'SDK che preferisci.

  Dopo aver creato l'associazione (o in caso di modifiche), è consigliabile testare la funzione ed è necessario ripubblicarla.

- Se modifichi un archivio di valori chiave senza modificare le coppie chiave-valore, non è necessario rinnovare l'associazione (il che significa che non è necessario pubblicare nuovamente). Ma è consigliabile testare la funzione.
- Se modificate le coppie chiave-valore negli archivi chiave-valore, non è necessario rinnovare l'associazione (il che significa che non è necessario pubblicare nuovamente). Tuttavia, è necessario testare la funzione per verificare che funzioni con le modifiche alle coppie chiave-valore.
- È possibile visualizzare tutte le funzioni che utilizzano archivi di valori chiave specifici. Sulla CloudFront console, guarda la pagina dei dettagli degli archivi di valori chiave.

Modifica un archivio di valori chiave

È possibile utilizzare le coppie chiave-valore e modificare l'associazione tra gli archivi di valori chiave e la funzione.

Console

Per modificare un archivio di valori chiave

1. Accedi AWS Management Console e apri la pagina Funzioni nella CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Scegliere la scheda KeyValueStores. Seleziona l'archivio dei valori delle chiavi da modificare. Viene visualizzata la pagina dei dettagli.
   - Per lavorare con le coppie chiave-valore, scegli il pulsante Modifica nella sezione Coppie chiave-valore. È possibile aggiungere altre coppie chiave-valore, eliminare qualsiasi coppia chiave-valore e modificare il valore di una coppia chiave-valore esistente. Al termine, scegli Salva le modifiche.
   - Per utilizzare l'associazione per questi archivi di valori chiave, scegliete il pulsante Vai alle funzioni. Viene aperta la pagina appropriata: l'elenco Funzioni (se al momento non è presente alcuna funzione associata) o la pagina dei dettagli della funzione (se al momento è presente un'associazione). Per ulteriori informazioni, consulta the section called “Associa un archivio di valori chiave a una funzione”.

Programmatically

È possibile utilizzare gli archivi di valori chiave nei seguenti modi.

Modificate le coppie chiave-valore

È possibile aggiungere altre coppie chiave-valore, eliminare una o più coppie chiave-valore e modificare il valore di una coppia chiave-valore esistente. Per ulteriori informazioni, consulta the section called “Utilizzo programmatico di coppie chiave-valore”.

Modificare l'associazione delle funzioni per gli archivi di valori chiave

Per utilizzare l'associazione per questi archivi di valori chiave, vederethe section called “Funzioni di aggiornamento”. Avrai bisogno dell'ARN degli archivi di valori chiave. Per ulteriori informazioni, consulta the section called “Ottieni un riferimento a un archivio di valori chiave”.

Eliminare un archivio di valori chiave

Puoi eliminare il tuo archivio di valori chiave utilizzando la CloudFront console o l'API.

Console

Per eliminare un archivio di valori chiave

1. Accedi AWS Management Console e apri la pagina Funzioni nella CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Verifica se il valore chiave memorizzato è associato a una funzione. Se lo è, rimuovi l'associazione. Per ulteriori informazioni su questi due passaggi, consulta ???.
3. Scegliere la scheda KeyValueStores. Seleziona l'archivio di valori chiave che desideri modificare, quindi scegli Elimina.

Programmatically

Per eliminare un archivio di valori chiave

1. Ottieni l'ETag e il nome degli archivi di valori chiave. Per ulteriori informazioni, consulta the section called “Ottieni un riferimento a un archivio di valori chiave”.
2. Verifica se gli archivi di valori chiave sono associati a una funzione. Se lo è, rimuovi l'associazione. Per ulteriori informazioni su questi due passaggi, consulta ???.
3. Per eliminare gli archivi di valori chiave, utilizzate l'operazione di eliminazione dell' CloudFront API o dell'SDK preferito. Ad esempio, per l'API REST, usaCloudFront. DeleteKeyValueStore.

Ottieni un riferimento a un archivio di valori chiave

Per utilizzare gli archivi di valori chiave a livello di codice, sono necessari l'ETag e il nome dell'archivio di valori chiave. Per ottenere questi dati, utilizza l' CloudFront API o il tuo AWS SDK preferito e segui questi passaggi:

1. Utilizza l'operazione CloudFront.ListKeyValueStoresAPI per restituire un elenco di archivi di valori chiave. Trova il nome dell'archivio di valori chiave che desideri modificare.
2. Utilizza l'operazione CloudFront.DescribeKeyValueStoreAPI e specifica il nome dell'archivio di valori chiave che hai restituito dal passaggio precedente.

La risposta include un UUID, l'ARN degli archivi di valori chiave e l'ETag degli archivi di valori chiave.

- L'UUID è a 128 bit. Ad esempio, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`
- L'ARN include il Account AWS numero, la costante `key-value-store` e l'UUID. Per esempio:

  `arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`
- Un ETag si presenta in questo modo: `ETVABCEXAMPLE2`

Per ulteriori informazioni sull'`DescribeKeyValueStore`operazione, vedere. the section called “Informazioni su CloudFront KeyValueStore”

Creare un file di 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 tuo bucket Amazon S3, puoi aggiornare il file per rimuovere eventuali duplicati e quindi provare a creare nuovamente il tuo key value store.

Per ulteriori informazioni, consulta Crea un archivio di valori chiave.

> **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 chiave-valore

Puoi lavorare con le coppie chiave-valore in un archivio di valori chiave esistente nei seguenti modi:

- Utilizzando la CloudFront console Amazon.
- Utilizzando l' CloudFront KeyValueStore API o il tuo AWS SDK preferito.

Questa sezione descrive come aggiungere coppie chiave-valore a un archivio di valori chiave esistente. Per includere coppie chiave-valore quando crei inizialmente gli archivi chiave-valore, consulta. the section called “Crea un archivio di valori chiave”

Argomenti

Lavorare con coppie chiave-valore utilizzando la console CloudFront

È possibile utilizzare la CloudFront console per lavorare con le coppie chiave-valore.

Per lavorare con coppie chiave-valore

1. Accedi AWS Management Console e apri la pagina Funzioni nella CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home#/functions
2. Scegliere la scheda KeyValueStores. Seleziona l'archivio dei valori delle chiavi da modificare. Viene visualizzata la pagina dei dettagli.
3. Nella sezione Coppie chiave-valore, scegli Modifica.
4. È possibile aggiungere una coppia chiave-valore, eliminare una coppia chiave-valore o modificare il valore di una coppia chiave-valore esistente.
5. Al termine, scegli Salva le modifiche.

Utilizzo programmatico di coppie chiave-valore

> **Note**
>
> L'CloudFront KeyValueStoreAPI ha uno spazio dei nomi diverso dall'API. CloudFront

Argomenti

Recupero di un riferimento a un archivio di valori delle chiavi

Quando si immette un'operazione di scrittura utilizzando CloudFront KeyValueStore, è necessario passare l'ARN e l'ETag degli archivi di valori chiave. Per recuperare questo script, procedi in questo modo:

1. Utilizza l'operazione di elenco delle tue CloudFront API o SDK preferiti. Ad esempio, per REST API, utilizza CloudFront.ListKeyValueStores. La risposta include un elenco di archivi di valori delle chiavi. Trova il nome dell'archivio di valori delle chiavi da modificare.
2. Utilizza l'operazione di descrizione dell' CloudFront KeyValueStore API o dell'SDK che preferisci. Ad esempio, per REST API, utilizza CloudFrontKeyValueStore.DescribeKeyValueStore. Inserisci il nome recuperato nel passaggio precedente.

   > **Note**
   >
   > Utilizza l'operazione dall' CloudFront KeyValueStore API, non dall' CloudFront API. Per ulteriori informazioni, consulta the section called “Informazioni su CloudFront KeyValueStore”.

   La risposta include l'ARN e l'ETag degli archivi di valori chiave.

   - L'ARN include il Account AWS numero, la costante `key-value-store` e l'UUID. Per esempio:

`arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

- Un ETag si presenta in questo modo: `ETVABCEXAMPLE2`

Modifica delle coppie chiave-valore in un archivio di valori chiave

Puoi lavorare con le coppie chiave-valore utilizzando le seguenti operazioni dell'API o dell'SDK che preferisci CloudFront KeyValueStore . Tutte queste operazioni funzionano su uno specifico archivio di valori chiave:

- `CloudFrontKeyValueStore.DeleteKey`: elimina una chiave. Per informazioni, consulta DeleteKey.
- `CloudFrontKeyValueStore.GetKey`: recupera una chiave. Per informazioni, consulta GetKey.
- `CloudFrontKeyValueStore.ListKeys`: elenca le chiavi. Per informazioni, consulta ListKeys.
- `CloudFrontKeyValueStore.PutKey`: puoi eseguire due azioni:
  - Crea una nuova coppia chiave-valore in un unico archivio di valori chiave: in questo caso, passa un nuovo nome e valore di chiave.
  - Imposta un valore diverso in una coppia chiave-valore esistente: in questo caso, passa un nome chiave esistente e un nuovo valore chiave.

  Per informazioni, consulta PutKey.
- `CloudFrontKeyValueStore.UpdateKeys`: È possibile eseguire una o più delle seguenti azioni in un'unica all-or-nothing operazione:
  - Eliminare una o più coppie chiave-valore.
  - Crea una o più nuove coppie chiave-valore.
  - Impostazione di un valore diverso in una o più coppie chiave-valore esistenti.

  Per informazioni, consulta UpdateKeys.

Informazioni su CloudFront KeyValueStore

Per utilizzare le coppie chiave-valore in modo programmatico in un archivio di valori chiave esistente, si utilizza il servizio. CloudFront KeyValueStore

Per includere alcune coppie chiave-valore negli archivi di valori chiave quando si creano inizialmente gli archivi di valori chiave, si utilizza il servizio. CloudFront

Operazione di descrizione

Sia l' CloudFront API che l' CloudFront KeyValueStore API dispongono di un'operazione di descrizione che restituisce i dati sugli archivi di valori chiave:

- L' CloudFront API fornisce dati come lo stato e la data dell'ultima modifica apportata all'archivio stesso.
- L' CloudFront KeyValueStore API fornisce dati sul contenuto della risorsa di archiviazione: le coppie chiave-valore nell'archivio e la dimensione del contenuto.

Le operazioni di descrizione nelle due API restituiscono dati leggermente diversi che identificano gli archivi di valori chiave:

- L'operazione di descrizione nell' CloudFront API restituisce un ETag, l'UUID e l'ARN degli archivi di valori chiave.

- L'operazione di descrizione nell' CloudFront KeyValueStore API restituisce un ETag e l'ARN degli archivi di valori chiave.

> **Note**
>
> Ogni operazione di descrizione restituisce un ETag diverso. Gli ETag non sono intercambiabili.
> Quando esegui un'operazione in una delle API, devi trasmettere l'ETag dall'API appropriata. Ad esempio, nell'operazione delete in CloudFront KeyValueStore, passate l'ETag che avete ottenuto dall'operazione describe in. CloudFront KeyValueStore

Codice di esempio per CloudFront KeyValueStore

Example : Chiamata dell'operazione **`DescribeKeyValueStore`** API

Il codice di esempio seguente mostra come chiamare l'operazione `DescribeKeyValueStore` API per un archivio di valori chiave.

```
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);
  }
})();
```

Personalizzazione all'avanguardia 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).

Quindi aggiungi trigger in Lambda CloudFront o nella console che fanno funzionare le funzioni 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.

Argomenti

Scopri come Lambda @Edge funziona 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, consulta Lavora con richieste e risposte e Struttura dell'evento Lambda@Edge.

Modi per usare Lambda @Edge

L'elaborazione di Lambda @Edge con la tua distribuzione Amazon CloudFront può essere utilizzata in molti modi. Per esempio:

- Un funzione Lambda è in grado di ispezionare cookie e riscrivere URL in modo che gli utenti vedano versioni differenti di un sito per il test A/B.
- CloudFront possono 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 altre idee, incluso il codice di esempio, consulta. Esempi di funzioni Lambda@Edge

Per una procedura che mostra come configurare Lambda @Edge nella console, consulta. Tutorial: Creare una funzione Lambda @Edge di base

Inizia a usare le funzioni Lambda @Edge

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 più vicine ai tuoi spettatori per migliorare le prestazioni.

L'elenco seguente fornisce una panoramica di base su come creare e utilizzare le funzioni Lambda con. CloudFront Per un step-by-step tutorial, vediTutorial: Creare una funzione Lambda @Edge di base.

1. Nella AWS Lambda console, crea una funzione Lambda nella regione Stati Uniti orientali (Virginia settentrionale). (Oppure puoi creare la funzione a livello di codice utilizzando uno degli SDK.) AWS
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, pubblichi 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 CloudFront riceve una richiesta da un visualizzatore.
4. Quando crei un trigger, Lambda crea repliche della funzione in AWS diverse località del mondo.

> **Tip**
>
> Scopri di più su come utilizzare Lambda @Edge per le tue soluzioni personalizzate. Scopri di più sulla creazione e l'aggiornamento di funzioni, sulla struttura degli eventi e sull'aggiunta di CloudFront trigger. Puoi inoltre trovare ulteriori idee e ottenere esempi di codice in Esempi di funzioni Lambda@Edge.

Argomenti

- Tutorial: Creare una funzione Lambda @Edge di base

Tutorial: Creare una funzione Lambda @Edge di base

Questo tutorial mostra come iniziare a usare Lambda @Edge creando e configurando una funzione Node.js di esempio da eseguire in. CloudFront Questo esempio aggiunge intestazioni di sicurezza HTTP a una risposta quando CloudFront recupera un file. (Ciò può migliorare la sicurezza e la privacy di un sito Web.)

Non è necessario il proprio sito Web per questo tutorial. Tuttavia, quando scegli di creare la tua soluzione Lambda @Edge, segui passaggi simili e scegli tra le stesse opzioni.

Argomenti

- Fase 1: registrazione ad un Account AWS

Fase 1: registrazione ad un Account AWS

Se non l'hai già fatto, iscriviti a 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 questo passaggio, crei una funzione Lambda da un modello di blueprint nella console Lambda. La funzione aggiunge codice per aggiornare le intestazioni di sicurezza nella distribuzione. CloudFront

Per creare una funzione Lambda

1. Accedi a AWS Management Console e apri la AWS Lambda console all'indirizzohttps://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 Modify HTTP response header come modello per la tua 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.

   Role Name (Nome ruolo)

   Immettere un nome per il ruolo creato dal modello di policy.

Policy templates (Modelli di policy)

Lambda aggiunge automaticamente le autorizzazioni del modello di policy Basic Lambda @Edge permissions 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 Configura le autorizzazioni e i ruoli IAM per Lambda @Edge.

6. Selezionare Create function (Crea funzione).
7. Nel riquadro Deploy to Lambda @Edge visualizzato, scegli Annulla. (Per questo tutorial, devi modificare il codice della funzione prima di distribuirla su Lambda @Edge.)
8. Scorri verso il basso fino alla sezione Code source 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';
exports.handler = (event, context, callback) => {

    //Get contents of response
    const response = event.Records[0].cf.request;
    const headers = response.headers;

    //Set new headers
    headers['strict-transport-security'] = [{key: 'Strict-Transport-Security',
 value: 'max-age= 63072000; includeSubdomains; preload'}];
    headers['content-security-policy'] = [{key: 'Content-Security-Policy', value:
 "default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; object-
src 'none'"}];
    headers['x-content-type-options'] = [{key: 'X-Content-Type-Options', value:
 'nosniff'}];
    headers['x-frame-options'] = [{key: 'X-Frame-Options', value: 'DENY'}];
    headers['x-xss-protection'] = [{key: 'X-XSS-Protection', value: '1;
 mode=block'}];
    headers['referrer-policy'] = [{key: 'Referrer-Policy', value: 'same-origin'}];

    //Return modified response
    callback(null, response);
};
```

10. Scegli File, Salva per salvare il codice aggiornato.

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 di panoramica delle funzioni per la tua funzione, scegli Aggiungi trigger.
2. Per la configurazione di Trigger, scegli CloudFront.
3. Scegli Distribuisci su Lambda @Edge.
4. Nel riquadro Deploy to Lambda @Edge, in CloudFront Configura trigger, inserisci le seguenti informazioni:

   Distribuzione

   L'ID CloudFront di distribuzione da associare alla tua funzione. Nell'elenco a discesa, scegli l'ID di distribuzione.

   Cache behavior (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 alle impostazioni di distribuzione.

   CloudFront evento

   Il trigger che specifica quando sarà eseguita la funzione. Vogliamo che la funzione security headers venga eseguita ogni volta che CloudFront restituisce una risposta dall'origine. Quindi, nell'elenco a discesa, scegli Origin response. Per ulteriori informazioni, consulta Aggiungere trigger per una funzione Lambda @Edge.
5. Seleziona la casella di controllo Confirm deploy to Lambda @Edge.
6. Scegli Deploy (Distribuisci) per aggiungere il trigger and replicare la funzione per le sedi AWS in tutto il mondo.
7. Attendi che la funzione venga replicata. Questo richiede in genere diversi minuti.

Puoi verificare se la replica è terminata accedendo alla CloudFront console e visualizzando la distribuzione. Attendi che lo stato della distribuzione passi da Distribuzione a data e ora, il che significa che la funzione è stata replicata. Quindi segui la procedura nella sezione successiva per verificare che la funzione sia attiva.

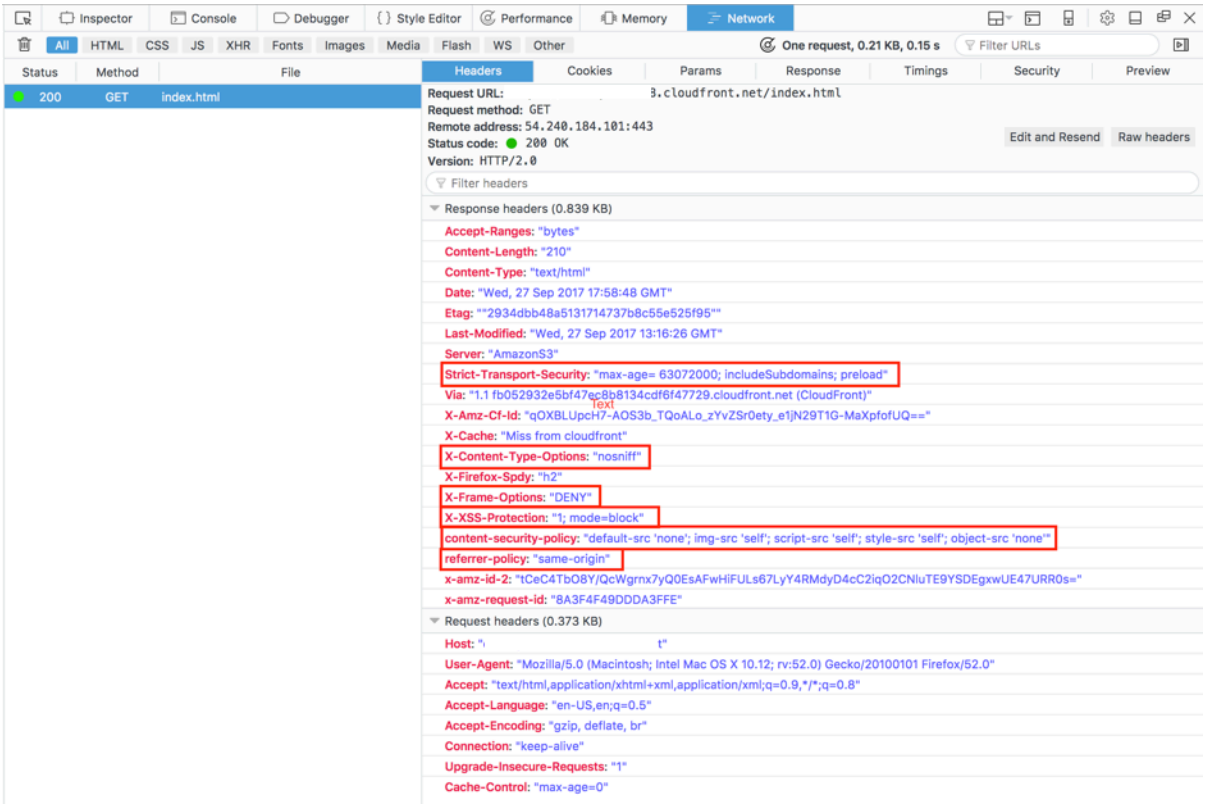
Fase 5: verificare che la funzione venga eseguita

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 che CloudFront restituiscono, per assicurarci che le intestazioni di sicurezza vengano aggiunte.

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. Personalizza il 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, vai al 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 CloudWatch i log per la tua funzione Lambda @Edge

1. Accedi AWS Management Console 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 CloudFront metriche 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
- Eliminare 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 su 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 di funzioni Lambda e, facoltativamente, la funzione stessa, vedere. Eliminare funzioni e repliche Lambda @Edge

Eliminare 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 disattivare ed eliminare una distribuzione CloudFront

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.

Risorse per l'approfondimento

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

Configura le autorizzazioni e i ruoli IAM per Lambda @Edge

Per configurare Lambda @Edge, devi disporre delle seguenti autorizzazioni e ruoli IAM per Lambda:

- Autorizzazioni IAM: queste autorizzazioni ti consentono di creare la tua AWS Lambda funzione e associarla alla tua distribuzione. CloudFront
- Un ruolo di esecuzione della funzione Lambda (ruolo IAM): i responsabili 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 a ottenere informazioni di configurazione per la funzione Lambda e un URL predefinito per scaricare `.zip` un file che contiene la funzione.
- `lambda:EnableReplication*`— Concede l'autorizzazione alla politica 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 politica delle risorse in modo che il servizio di replica Lambda possa eliminare la funzione.

  > **Important**
  >
  > È necessario aggiungere l'asterisco (`*`) alla fine delle azioni and. `lambda:EnableReplication*` `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 per te. Non è necessario aggiungere questa autorizzazione ad altre distribuzioni che utilizzano Lambda @Edge.

- `cloudfront:UpdateDistribution`o `cloudfront:CreateDistribution` — Concede l'autorizzazione ad 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 Developer Guide AWS Lambda

Ruolo di esecuzione della funzione per i principali del servizio

Devi creare un ruolo IAM che i responsabili del `lambda.amazonaws.com` `edgelambda.amazonaws.com` servizio possano assumere quando eseguono la tua 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. Questo passaggio aggiunge automaticamente le autorizzazioni Lambda @Edge richieste per eseguire la funzione. Vedi il Passaggio 5 del tutorial: Creazione di una semplice funzione Lambda @Edge.

Per ulteriori informazioni sulla creazione manuale di un ruolo IAM, consulta Creating roles and attaching policies (console) nella IAM User Guide.

Example Esempio: politica di fiducia dei ruoli

Puoi aggiungere questo ruolo nella scheda Trust Relationship nella console IAM. Non aggiungere questa politica nella scheda Autorizzazioni.

```
{
   "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 le autorizzazioni di accesso alle risorse Lambda nella AWS Lambda Developer Guide.

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 È possibile utilizzare il valore predefinito AWSLambdaBasicExecutionRole 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 quell'azione.

Ruoli collegati ai servizi per Lambda@Edge

Lambda @Edge utilizza ruoli collegati ai servizi 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 utilizza i seguenti ruoli collegati ai servizi 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 Questo ruolo è necessario per utilizzare le funzioni Lambda @Edge. L'ARN per il AWSServiceRoleForLambdaReplicator ruolo è simile al seguente esempio:

  ```
  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 registro per eseguire il debug degli errori di convalida 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 di ruolo collegate al servizio 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 politica di autorizzazione dei ruoli consente a Lambda @Edge di completare le seguenti azioni sulla `arn:aws:logs:*:*:log-group:/aws/cloudfront/*` risorsa 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 di 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 AWSServiceRoleForLambdaReplicator ruolo (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 AWSServiceRoleForLambdaReplicator o i ruoli collegati ai AWSServiceRoleForCloudFrontLogger servizi. Dopo che il servizio ha creato un ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché diverse entità potrebbero fare riferimento al ruolo. Puoi tuttavia utilizzare IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Supportato Regioni AWS per i ruoli collegati al servizio CloudFront

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 tua AWS Lambda funzione. Successivamente, configuri Lambda per eseguire la funzione in base a CloudFront eventi specifici, chiamati trigger.

Puoi utilizzarlo AWS Management Console per lavorare con le funzioni e i CloudFront trigger Lambda oppure puoi lavorare con Lambda @Edge a livello di codice utilizzando l'API.

Argomenti

Scrivi la tua funzione Lambda @Edge

Per aiutarti a scrivere le funzioni Lambda @Edge, consulta le seguenti risorse:

- Struttura dell'evento Lambda@Edge— Comprendi la struttura degli eventi da usare con Lambda @Edge.
- Esempi di funzioni Lambda@Edge— Funzioni di esempio, come il test A/B e la generazione di un reindirizzamento HTTP.

Il modello di programmazione per l'utilizzo di Node.js o Python con Lambda @Edge è lo stesso dell'utilizzo di Lambda in un. Regione AWSPer ulteriori informazioni, consulta Creazione di funzioni Lambda con Node.js o Creazione di funzioni Lambda con Python nella Developer Guide.AWS Lambda

Nella funzione Lambda @Edge, includi il `callback` parametro e restituisci l'oggetto applicabile per gli eventi di richiesta o 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 Genera risposte HTTP nei trigger di richiesta.
- Eventi di risposta - È necessario includere l'oggetto `cf.response` nella risposta.

Creare 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 (console)

1. Accedi AWS Management Console 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. Crea una funzione usando il tuo codice o crea una funzione a partire da un CloudFront blueprint.
   - Per creare una funzione utilizzando il proprio codice, selezionare Author from scratch (Crea da zero).

- Per visualizzare un elenco di progetti per CloudFront, digita 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: inserisci un nome per la tua 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 le istruzioni per completare le informazioni di questa sezione.

   c. Nome ruolo: inserisci un nome per il ruolo.

   d. Modelli di policy: scegli le autorizzazioni Basic Edge Lambda.

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**
   >
   > Ti consigliamo di testare ed eseguire il debug della funzione prima di aggiungere i trigger. Se aggiungi un trigger ora, la funzione verrà eseguita non appena la crei, terminerà la replica in AWS diverse 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. Digitare una descrizione per la nuova versione della funzione.
14. Seleziona Publish (Pubblica).
15. Eseguire il test e il debugging della funzione. Per ulteriori informazioni sui test nella console Lambda, consulta Richiamo della funzione Lambda e verifica dei risultati, dei log e dei parametri in Creazione di una funzione Lambda con 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 Aggiungere trigger per una funzione Lambda @Edge.

Usa l'API o AWS CLI lavora con Lambda @Edge

Puoi anche utilizzare le operazioni Lambda e CloudFront API per configurare le funzioni e i trigger Lambda @Edge a livello di codice. CloudFront Per ulteriori informazioni, consulta i seguenti argomenti:

- AWS Lambda Documentazione di riferimento delle API
- Riferimento alle CloudFront API Amazon
- Puoi anche utilizzare i seguenti comandi AWS Command Line Interface (AWS CLI):
  - Funzione di creazione Lambda
  - CloudFront crea-distribuzione
  - CloudFront create-distribution-with-tags
  - CloudFront distribuzione degli aggiornamenti
- AWS SDK (consulta la sezione SDK e toolkit).
- AWS Tools for PowerShell Riferimento al cmdlet

Cambia la tua 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.

Per modificare una funzione Lambda (console)

1. Accedi AWS Management Console 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. Nell'elenco delle 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 nella sezione Versione nell'angolo superiore sinistro della pagina.
9. Selezionare la scheda Triggers (Trigger).
10. Selezionare Add trigger (Aggiungi trigger).
11. Nella finestra di dialogo Aggiungi trigger, scegliete la casella punteggiata, quindi scegliete. 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 di distribuzione: scegli l'ID della distribuzione a cui desideri aggiungere il trigger.

    b. Comportamento della cache: scegli il comportamento della cache che specifica gli oggetti su cui desideri eseguire la funzione.

    c. CloudFront evento — Scegliete l' CloudFront evento che causa l'esecuzione della funzione.

    d. Abilita attivazione e replica: seleziona questa casella di controllo in modo che Lambda replichi la funzione a livello globale. Regioni AWS
13. Scegli Invia.
14. Per aggiungere più trigger per questa funzione, ripetere le fasi da 10 a 13.

Aggiungere 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. È possibile specificare uno o più CloudFront trigger che causano l'esecuzione della funzione. Ad esempio, potete creare un trigger che provochi l'esecuzione della funzione quando si CloudFront riceve una richiesta da un visualizzatore per uno specifico comportamento della cache impostato per la distribuzione.

> **Tip**
>
> Quando crei una CloudFront distribuzione, specifichi le impostazioni che indicano CloudFront come rispondere quando riceve richieste diverse. Le impostazioni predefinite sono denominate comportamento predefinito della cache 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 Impostazioni del comportamento cache.

Al momento della creazione di una funzione Lambda, è possibile 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.

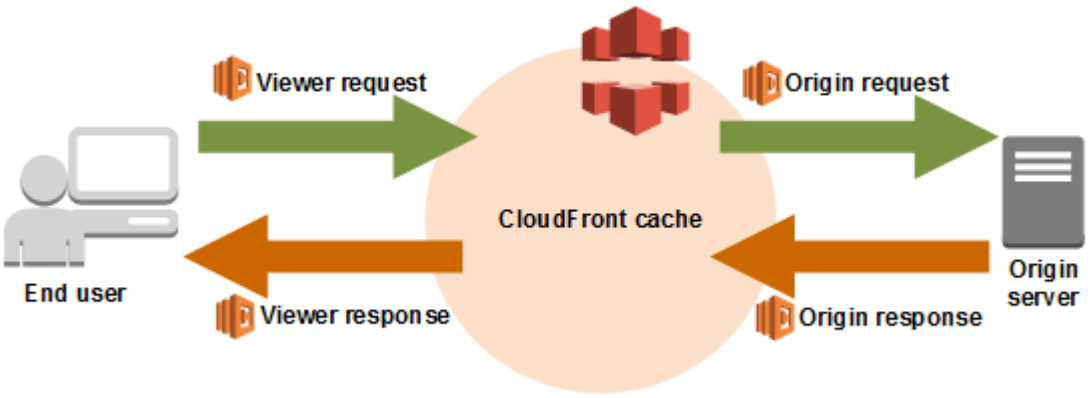
> **Note**
>
> Per lavorare con Lambda @Edge a livello di codice, consulta. Usa l'API o AWS CLI lavora con Lambda @Edge

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.

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; di conseguenza è consigliabile che la funzione venga eseguita il più rapidamente possibile.

Decidi quale CloudFront evento usare per attivare una funzione Lambda @Edge

Quando decidi quale CloudFront evento utilizzare per attivare una funzione Lambda, considera quanto segue:

Vuoi CloudFront memorizzare nella cache gli oggetti che vengono modificati da una funzione Lambda?

Se desideri CloudFront inserire 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, usa la richiesta di origine o l'evento 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.

Vuoi che la funzione venga eseguita per ogni richiesta?

Se desideri che la funzione venga eseguita per ogni richiesta CloudFront ricevuta per la distribuzione, utilizza 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.

La funzione deve modificare la chiave di cache?

Se vuoi che la funzione modifichi un valore che stai utilizzando 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: https://example.com/en/index.html
- URL se la richiesta proviene da un indirizzo IP in Germania: https://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:
>
> - Contenuto della cache basato sui cookie
> - Contenuto della cache in base alle intestazioni delle richieste

La funzione influisce sulla risposta dall'origine?

Se vuoi che la funzione modifichi la richiesta in un modo che influisce 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.

Aggiungere 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 tua funzione (non per $LATEST).

Lambda console

Per aggiungere trigger a una funzione Lambda @Edge

1. Accedi AWS Management Console 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 di panoramica delle funzioni, 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, scegliete Seleziona una fonte, immettete**`cloudfront`**, quindi scegliete 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 desideri aggiungere il trigger.

b. Comportamento della cache: scegli il comportamento della cache che specifica gli oggetti su cui desideri eseguire la funzione.

> **Note**
>
> Se specifichi * per il comportamento cache, la funzione Lambda effettua la distribuzione al comportamento cache predefinito.

c. CloudFront evento — Scegliete l'CloudFront evento che causa l'esecuzione della funzione.

d. Includi corpo: seleziona questa casella di controllo se desideri accedere al corpo della richiesta nella tua funzione.

e. Conferma la distribuzione su Lambda @Edge: seleziona questa casella di controllo in AWS Lambda modo da replicare la funzione a livello globale. Regioni AWS

10. Scegli 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 viene distribuita una distribuzione, il valore della colonna Status per la distribuzione cambia da Deploying alla data e all'ora di distribuzione.

CloudFront console

Per aggiungere trigger per CloudFront eventi a una funzione Lambda

1. Ottieni l'ARN della funzione Lambda a cui desideri aggiungere dei trigger:

   a. Accedi AWS Management Console 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 di panoramica delle funzioni, scegli la scheda Versioni e scegli la versione numerata a cui desideri aggiungere i trigger.

e. Scegli il pulsante Copia ARN per copiare l'ARN negli appunti. L'ARN per la funzione Lambda ha un aspetto simile al seguente:

```
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'indirizzo. https://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 della cache a cui desideri aggiungere i trigger, quindi scegli Modifica.
6. Per le associazioni di funzioni, nell'elenco Tipo di funzione, scegli Lambda @Edge per quando desideri che la funzione venga eseguita: per le richieste dei visualizzatori, le risposte dei visualizzatori, le richieste di origine o le risposte di origine.

   Per ulteriori informazioni, consulta Decidi quale CloudFront evento usare per attivare una funzione Lambda @Edge.
7. Nella casella di testo Function ARN/Name, incolla l'ARN della funzione Lambda che desideri eseguire quando si verifica l'evento scelto. Questo è il valore che hai copiato dalla console Lambda.
8. Seleziona Includi corpo se desideri accedere al corpo della richiesta nella tua 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 eventi, ripeti i passaggi 6 e 7.
10. Seleziona Salvataggio delle 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 viene distribuita una distribuzione, il valore della colonna Status per la distribuzione cambia da Deploying all'ora e alla data di distribuzione.

Test ed esegui il debug delle funzioni Lambda @Edge

Questo argomento include sezioni che descrivono strategie per il test e il 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 “ Determina la regione Lambda @Edge”.

Argomenti

Testa le tue 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 sui test nella console Lambda, consulta Richiamo della funzione Lambda e verifica dei risultati, dei log e dei parametri in Creazione di una funzione Lambda con 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. Assicurati che la funzione sia attivata per l'evento giusto e restituisca una risposta valida e corretta per CloudFront. Ad esempio, assicuratevi che la struttura dell'evento sia corretta, che siano incluse solo 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.

Per verificare se la replica è terminata la distribuzione

1. Apri la CloudFront console all'indirizzo. https://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 di risposte di errore dall'origine

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). Per ulteriori informazioni, consulta Errori della funzione Lambda nella Guida per gli AWS Lambda sviluppatori.

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.

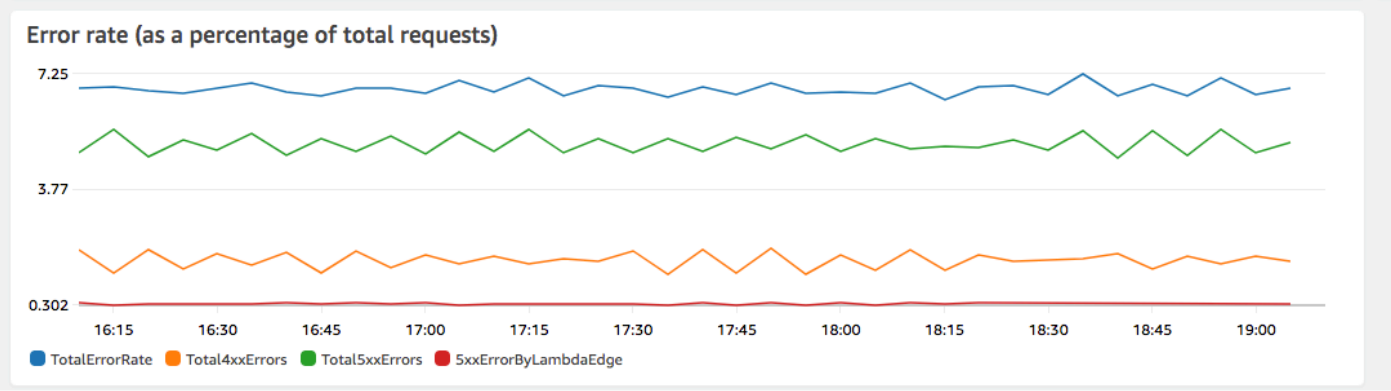
Come stabilire il tipo di errore

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. AWS Management Console Per ulteriori informazioni sulla visualizzazione dei grafici nella sezione Monitoraggio della CloudFront console, consulta. Monitoraggio delle CloudFront metriche 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 di risposte di errore dall'origine.

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 per. Regione AWS

Per semplificare la risoluzione dei problemi, è possibile cercare problemi specifici aprendo ed esaminando i file di registro per individuare funzioni specifiche per regione.

Per visualizzare i file di registro per una funzione specifica per regione

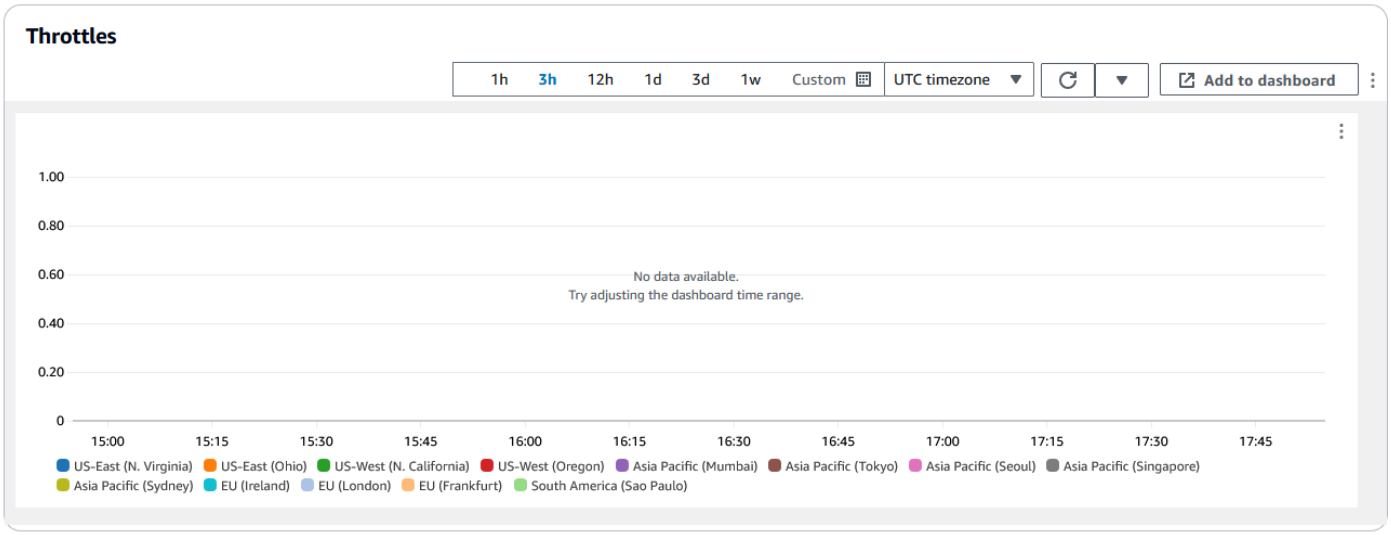
1. Nella scheda Errori Lambda @Edge, in Funzioni associate Lambda @Edge, scegli il nome della funzione, quindi scegli Visualizza metriche.
2. Successivamente, nella pagina con il nome della funzione, nell'angolo in alto a destra, scegli Visualizza registri delle funzioni, quindi scegli una regione.

   Ad esempio, se vedi problemi nel grafico degli errori per la regione Stati Uniti occidentali (Oregon), scegli quella 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 identifichi 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, vedi Determinare se il tuo account invia i log a CloudWatch più avanti nell'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.

Risolvi gli 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.

Determina la 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. AWS Management Console 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 CloudFront metriche 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 controllare nella regione in cui è stata eseguita la funzione Lambda@Edge. Per ulteriori informazioni, consulta Determina la regione Lambda @Edge.
- Stabilisci se il ruolo collegato al servizio relativo esiste nel tuo account in IAM. A tale scopo, aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/, quindi scegliere Ruoli per visualizzare l'elenco dei ruoli collegati al servizio per l'account. Individuare il seguente ruolo: `AWSServiceRoleForCloudFrontLogger`.

Eliminare funzioni e 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 per la 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 CloudFront distribuzione (console)

1. Accedi AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegli l'ID della distribuzione con l'associazione di funzioni Lambda @Edge che desideri eliminare.
3. Scegli la scheda Behaviors (Comportamenti).
4. Seleziona il comportamento della cache con l'associazione di funzioni Lambda @Edge che desideri eliminare, quindi scegli Modifica.
5. In Associazioni di funzioni, Tipo di funzione, scegli Nessuna associazione per eliminare l'associazione di funzioni Lambda @Edge.
6. Seleziona Salvataggio delle 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 qualche ora dopo aver eliminato l'associazione di funzioni in modo che le repliche delle funzioni Lambda @Edge possano essere pulite. Dopodiché, potrai 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 qualche ora. Quindi sarai in grado di 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

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,
              "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 nell'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 un visualizzatore su una richiesta. CloudFront Il `requestId` valore appare anche nei CloudFront log di accesso come. `x-edge-request-id` Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso) e Campi del file di registro standard.

Campi nell'oggetto richiesta

Nella seguente lista sono descritti i campi nell'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` 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 Contenuto della cache in base ai parametri della stringa 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 si specifica `encoding` come `base64` ma il corpo non è validobase64, 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. La struttura di origine può contenere i seguenti campi:

`customHeaders` (lettura/scrittura) (origini personalizzate e Amazon S3)

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 non CloudFront possono essere aggiunte 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 `awsexamplebucket.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 60, inclusi.

`port` (lettura/scrittura) (solo origini personalizzate)

La porta a cui CloudFront dovresti connetterti 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) (solo origini personalizzate)

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 risposta prima di ricevere il pacchetto successivo. Il valore deve essere un numero compreso tra 4 e 60, inclusi.

Se il tuo caso d'uso richiede più di 60 secondi, puoi richiedere una quota più alta per. `Response timeout per origin` Per ulteriori informazioni, consulta Quote generali sulle distribuzioni.

`sslProtocols` (lettura/scrittura) (solo origini personalizzate)

Il protocollo SSL/TLS minimo che CloudFront puoi utilizzare per stabilire una connessione HTTPS con la tua 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

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,
            "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 nell'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 il destinatario della CloudFront richiesta a cui è associata questa risposta. Il `requestId` valore appare anche nei CloudFront log di accesso come. `x-edge-request-id` Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso) e Campi del file di registro standard.

Campi nell'oggetto risposta

Nella seguente lista sono descritti i campi nell'oggetto `response` (`Records.cf.response`). Per informazioni sull'utilizzo di una funzione Lambda @Edge per generare una risposta HTTP, vedere Genera risposte HTTP nei 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 dell'intestazione con distinzione tra maiuscole e minuscole così come appare nella risposta HTTP, ad esempio, `Content-Type` `Content-LengthCookie`, 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.

Lavora con richieste e risposte

Gli argomenti di questa sezione illustrano i modi per utilizzare le richieste e le risposte Lambda@Edge.

Argomenti

Usa le 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: Crea un gruppo di origine
- Come funziona il failover di origine con Lambda@Edge: Utilizzo del failover di origine con le funzioni Lambda@Edge

Genera risposte HTTP nei 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 CloudFront eventi:

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, 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 Aggiorna le risposte HTTP nei trigger di risposta di 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`

L'eventuale corpo 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 si specifica `bodyEncoding` come `base64` ma il corpo non è valido base64, CloudFront restituisce un errore.

`headers`

Intestazioni che si desidera CloudFront restituire nella risposta generata. 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` (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 Configurazione e utilizzo di registri standard (registri di accesso)

Se il `status` valore non è compreso tra 200 e 599, CloudFront restituisce un errore al visualizzatore.

`statusDescription`

La descrizione che desideri CloudFront restituire nella risposta, che accompagna il 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.

Aggiorna le risposte HTTP nei trigger di risposta di origine

Quando CloudFront riceve una risposta HTTP dal server di origine, se è presente un trigger di risposta di origine associato al comportamento della cache, puoi 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: utilizza un trigger di risposta di origine per aggiornare il codice di stato dell'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: utilizza un trigger di risposta di origine per aggiornare il codice di stato dell'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 Genera risposte HTTP nei 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.

Accedi al corpo della richiesta scegliendo l'opzione include body

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 abilitare questa opzione, scegli Includi Body quando crei un CloudFront trigger per la tua funzione che riguarda una richiesta del visualizzatore o un evento di richiesta di origine. Per ulteriori informazioni, consulta Aggiungere 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

Consulta le seguenti sezioni per esempi di utilizzo delle funzioni Lambda con Amazon. CloudFront

> **Note**
>
> Se scegli runtime Node.js 18 o versione successiva per la tua funzione Lambda @Edge, viene creato automaticamente un `index.mjs` file. Per utilizzare i seguenti esempi di codice, rinomina invece il `index.mjs` file in`index.js`.

Argomenti

- Esempi generali
- Genera risposte: esempi
- Stringhe di query: esempi
- Esempi di personalizzazione del contenuto in base alle intestazioni del paese o del tipo di dispositivo
- Esempi di selezione dinamica dell'origine in funzione del contenuto
- Aggiornare gli stati di errore: esempi
- Accedi al corpo della richiesta: esempi

Esempi generali

Gli esempi in questa sezione illustrano alcuni modi comuni di usare Lambda @Edge in. CloudFront

Argomenti

- Esempio: test A/B
- Esempio: sovrascrivi un'intestazione di risposta

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 il visualizzatore a uno degli URL in modo casuale.

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: sovrascrivi 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

```
'use strict';

exports.handler = (event, context, callback) => {
   const response = event.Records[0].cf.response;
   const headers = response.headers;

   const headerNameSrc = 'X-Amz-Meta-Last-Modified';
   const headerNameDst = 'Last-Modified';

   if (headers[headerNameSrc.toLowerCase()]) {
      headers[headerNameDst.toLowerCase()] = [
         headers[headerNameSrc.toLowerCase()][0],
      ];
      console.log(`Response header "${headerNameDst}" was set to ` +
               `"${headers[headerNameDst.toLowerCase()][0].value}"`);
   }

   callback(null, response);
};
```

Python

```
import json

def lambda_handler(event, context):
    response = event["Records"][0]["cf"]["response"]
    headers = response["headers"]

    headerNameSrc = "X-Amz-Meta-Last-Modified"
    headerNameDst = "Last-Modified"
```

```
    if headers.get(headerNameSrc.lower(), None):
        headers[headerNameDst.lower()] = [headers[headerNameSrc.lower()][0]]
        print(f"Response header {headerNameDst.lower()} was set to
{headers[headerNameSrc.lower()][0]}")

    return response
```

Genera risposte: esempi

Gli esempi di questa sezione illustrano come è possibile usare Lambda@Edge per generare le risposte.

Argomenti

- Esempio: pubblica contenuti statici (risposta generata)
- Esempio: generazione di un reindirizzamento HTTP (risposta generata)

Esempio: pubblica contenuti statici (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 “Genera risposte HTTP nei 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 “Aggiorna le risposte HTTP nei trigger di risposta di 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 Genera risposte HTTP nei 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 di questa sezione illustrano i modi in cui è possibile usare Lambda@Edge con le stringhe di query.

Argomenti

Esempio: aggiungere un'intestazione basata su un parametro della 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: normalizza i parametri della stringa di query per migliorare il rapporto di accesso alla cache

L'esempio seguente mostra come migliorare il rapporto di accessi 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 Contenuto della cache in base ai parametri della stringa 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: reindirizzare gli utenti non autenticati a una 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 in questa sezione illustrano come utilizzare Lambda@Edge per personalizzare il comportamento in base alla posizione o al tipo di dispositivo usato dal visualizzatore.

Argomenti

- Esempio: reindirizza le richieste degli spettatori a un URL specifico del Paese
- Esempio: servi versioni diverse di un oggetto in base al dispositivo

Esempio: reindirizza le richieste degli spettatori a un URL specifico del 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: servi versioni diverse 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 in questa sezione mostrano in che modo è possibile usare Lambda@Edge per l'instradamento a diverse origini in base alle informazioni nella richiesta.

Argomenti

- Esempio: utilizza un trigger di richiesta di origine per passare da un'origine personalizzata a un'origine Amazon S3
- Esempio: utilizza un trigger di richiesta di origine per modificare la regione di origine di Amazon S3
- Esempio: utilizza un trigger di richiesta di origine per passare da un'origine Amazon S3 a un'origine personalizzata
- Esempio: utilizza un trigger di richiesta di origine per trasferire gradualmente il traffico da un bucket Amazon S3 a un altro
- Esempio: utilizza un trigger di richiesta di origine per modificare il nome di dominio di origine in base all'intestazione del paese

Esempio: utilizza un trigger di richiesta di 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 = 'my-bucket.s3.amazonaws.com';

             /* Set S3 origin fields */
             request.origin = {
                 s3: {
                     domainName: s3DomainName,
                     region: '',
                     authMethod: 'none',
                     path: '',
                     customHeaders: {}
                 }
             };
             request.headers['host'] = [{ key: 'host', value: s3DomainName}];
         }
     }

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    '''
    Reads query string to check if S3 origin should be used, and
    if true, sets S3 origin properties
    '''
    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}
    if params.get('useS3Origin') == 'true':
        s3DomainName = 'my-bucket.s3.amazonaws.com'

        # Set S3 origin fields
        request['origin'] = {
            's3': {
                'domainName': s3DomainName,
                'region': '',
                'authMethod': 'none',
                'path': '',
                'customHeaders': {}
            }
        }
        request['headers']['host'] = [{'key': 'host', 'value': s3DomainName}]
    return request
```

Esempio: utilizza un trigger di richiesta di origine per modificare la regione di origine di 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.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    /**
     * This blueprint demonstrates how an origin-request trigger can be used to
     * change the origin from which the content is fetched, based on request
 properties.
     * In this example, we use the value of the CloudFront-Viewer-Country header
     * to update the S3 bucket domain name to a bucket in a Region that is closer to
     * the viewer.
     *
     * This can be useful in several ways:
     *      1) Reduces latencies when the Region specified is nearer to the viewer's
     *         country.
     *      2) Provides data sovereignty by making sure that data is served from an
     *         origin that's in the same country that the request came from.
     *
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Viewer-Country header. For more information, see
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    const countryToRegion = {
```

```
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    };

    if (request.headers['cloudfront-viewer-country']) {
        const countryCode = request.headers['cloudfront-viewer-country'][0].value;
        const region = countryToRegion[countryCode];

        /**
         * If the viewer's country is not in the list you specify, the request
         * goes to the default S3 bucket you've configured.
         */
        if (region) {
            /**
             * If you've set up OAI, the bucket policy in the destination bucket
             * should allow the OAI GetObject operation, as configured by default
             * for an S3 origin with OAI. Another requirement with OAI is to provide
             * the Region so it can be used for the SIGV4 signature. Otherwise, the
             * Region is not required.
             */
            request.origin.s3.region = region;
            const domainName = `my-bucket-in-${region}.s3.amazonaws.com`;
            request.origin.s3.domainName = domainName;
            request.headers['host'] = [{ key: 'host', value: domainName }];
        }
    }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    This blueprint demonstrates how an origin-request trigger can be used to
    change the origin from which the content is fetched, based on request
 properties.
```

```
    In this example, we use the value of the CloudFront-Viewer-Country header
    to update the S3 bucket domain name to a bucket in a Region that is closer to
    the viewer.

    This can be useful in several ways:
        1) Reduces latencies when the Region specified is nearer to the viewer's
            country.
        2) Provides data sovereignty by making sure that data is served from an
            origin that's in the same country that the request came from.

    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    }

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        region = countryToRegion.get(countryCode)

        # If the viewer's country in not in the list you specify, the request
        # goes to the default S3 bucket you've configured
        if region:
            '''
            If you've set up OAI, the bucket policy in the destination bucket
            should allow the OAI GetObject operation, as configured by default
            for an S3 origin with OAI. Another requirement with OAI is to provide
            the Region so it can be used for the SIGV4 signature. Otherwise, the
            Region is not required.
            '''
            request['origin']['s3']['region'] = region
            domainName = 'my-bucket-in-%s.s3.amazonaws.com' % region
```

```
            request['origin']['s3']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Esempio: utilizza un trigger di richiesta di 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: utilizza un trigger di richiesta di origine per trasferire gradualmente il traffico da un bucket Amazon S3 a un altro

Questa funzione dimostra come trasferire gradualmente 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: utilizza un trigger di richiesta di origine per modificare il nome di dominio di 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
```

Aggiornare gli stati di errore: esempi

Gli esempi di questa sezione forniscono indicazioni su come è possibile usare Lambda@Edge per modificare lo stato di errore che viene restituito agli utenti.

Argomenti

Esempio: utilizza un trigger di risposta di origine per aggiornare il codice di stato dell'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: utilizza un trigger di risposta di origine per aggiornare il codice di stato dell'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
```

Accedi al corpo della richiesta: esempi

Gli esempi in questa sezione 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 Includi corpo nella Lambda Function Association.
> - Per abilitare questa impostazione nell' CloudFront API o con AWS CloudFormation, imposta il `IncludeBody` campo su `true` in`LambdaFunctionAssociation`.

Argomenti

Esempio: utilizza 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 CloudFront visualizzazione o in una richiesta di 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: utilizzate 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 di CloudFront visualizzazione 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

I seguenti argomenti descrivono le restrizioni che si applicano a CloudFront Functions e Lambda @Edge. Alcune restrizioni si applicano a tutte le funzioni edge, mentre altre si applicano solo a CloudFront Functions o Lambda @Edge.

Per ulteriori informazioni sulle quote (precedentemente denominate limiti), consulta Quote sulle funzioni CloudFront e Quote di Lambda@Edge.

Argomenti

- Restrizioni su tutte le funzioni edge
- Restrizioni sulle funzioni CloudFront
- Restrizioni su Lambda@Edge

Restrizioni su tutte le funzioni edge

Le seguenti restrizioni si applicano a tutte le funzioni edge, sia CloudFront Functions che Lambda @Edge.

Argomenti

- Proprietà di Account AWS
- Combinazione di CloudFront funzioni con Lambda @Edge
- Codici di stato HTTP
- Intestazioni HTTP
- Stringhe di query
- URI
- Codifica di URI e stringa di query
- Microsoft Smooth Streaming

- Assegnazione di tag

Proprietà di Account AWS

Per associare una funzione edge a una CloudFront distribuzione, la funzione e la distribuzione devono essere di proprietà della stessa Account AWS.

Combinazione di CloudFront funzioni 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 CloudFront Functions e Lambda @Edge negli eventi del visualizzatore (richiesta e risposta del visualizzatore).

Sono consentite tutte le altre combinazioni di funzioni edge. Nella tabella seguente sono descritte le combinazioni consentite.

		CloudFront Funzioni	
		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 richiama le funzioni edge per gli eventi di risposta del visualizzatore quando 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 Aggiorna le risposte HTTP nei trigger di risposta di 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 le funzioni possono leggerle ma non possono aggiungerle o modificarle.

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 funzione aggiunge una di queste intestazioni, non riesce la CloudFront convalida e CloudFront restituisce il codice di stato HTTP 502 (Bad Gateway) 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 funzione aggiunge o modifica un'intestazione di sola lettura, la richiesta non viene CloudFront convalidata e CloudFront restituisce il codice di stato HTTP 502 (Bad Gateway) 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 sia per Functions che per Lambda CloudFront @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 e stringa di query.

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 e stringa di query

I valori di URI e stringa di query passati alle funzioni edge sono codificati in UTF-8. La tua funzione dovrebbe utilizzare la codifica UTF-8 per i valori di URI e stringa di query restituiti. La codifica percentuale è compatibile con la codifica UTF-8.

L'elenco seguente spiega come CloudFront gestisce la codifica dei valori degli URI e delle stringhe di query:

- Quando i valori nella richiesta sono codificati in UTF-8, CloudFront inoltra i valori alla funzione senza modificarli.
- Quando i valori nella richiesta sono codificati in ISO-8859-1, CloudFront converte i valori nella codifica UTF-8 prima di inoltrarli alla tua funzione.

- Quando i valori nella richiesta vengono codificati utilizzando un'altra codifica di caratteri, CloudFront presuppone che siano codificati in ISO-8859-1 e tenta di 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 e della stringa di query che vengono inoltrati all'origine dipendono dal fatto che una funzione modifichi i valori: CloudFront

- Se una funzione non modifica l'URI o la stringa di query, CloudFront inoltra i valori ricevuti nella richiesta all'origine.
- Se una funzione modifica l'URI o la stringa di query, CloudFront inoltra i valori codificati UTF-8.

Microsoft Smooth Streaming

Non è possibile utilizzare le funzioni edge con una CloudFront distribuzione utilizzata per lo streaming di file multimediali transcodificati nel formato Microsoft Smooth Streaming.

Assegnazione di tag

Non è possibile aggiungere tag alle funzioni edge. Per ulteriori informazioni sull'aggiunta di tag, consulta CloudFront. Etichettare una distribuzione

Restrizioni sulle funzioni CloudFront

Le seguenti restrizioni si applicano solo alle CloudFront funzioni.

Per informazioni sulle quote (precedentemente denominate limiti), vedere. Quote sulle funzioni CloudFront

Log

I registri delle CloudFront funzioni in Funzioni vengono troncati a 10 KB.

Corpo della richiesta

CloudFront Le funzioni non possono accedere al corpo della richiesta HTTP.

AWS Security Token Service Endpoint regionali quando si utilizza l'API CloudFront KeyValueStore

Quando chiami l'CloudFront KeyValueStore API utilizzando Signature Version 4A (Sigv4A) con credenziali di sicurezza temporanee, ad esempio quando usi ruoli AWS Identity and Access Management (IAM), assicurati di richiedere le credenziali temporanee da un endpoint regionale in. AWS STS Se utilizzi l'endpoint globale for AWS STS (`sts.amazonaws.com`), AWS STS genererà credenziali temporanee da un endpoint globale, che non è supportato da SigV4A. Di conseguenza, riceverai un errore di autenticazione. Per risolvere questo problema, utilizza uno degli endpoint regionali elencati AWS STS nella Guida per l'utente IAM. Se stai configurando SAML per l'utilizzo di endpoint AWS STS regionali, consulta il post sul blog Come utilizzare gli endpoint SAML regionali per il failover.

Runtime

L'ambiente di runtime CloudFront Functions non supporta la valutazione dinamica del codice e limita l'accesso alla rete, al file system e ai timer. Per ulteriori informazioni, consulta Funzionalità con restrizioni.

> **Note**
>
> Per essere utilizzata CloudFront KeyValueStore, la CloudFront funzione deve utilizzare JavaScript runtime 2.0.

Utilizzo di calcolo

CloudFront Le funzioni hanno un limite al tempo che possono impiegare per l'esecuzione, misurato come utilizzo del 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, puoi visualizzare la metrica di utilizzo del calcolo nella pagina Monitoraggio della console o in. CloudFront CloudWatch

Restrizioni su Lambda@Edge

A Lambda@Edge si applicano le seguenti restrizioni.

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 per il tuo dominio presenta problemi e non CloudFront riesce a risolvere il nome di dominio per ottenere l'indirizzo IP, la funzione Lambda @Edge non verrà richiamata. CloudFrontrestituirà un codice di stato HTTP 502 (Bad Gateway) al client. Per ulteriori informazioni, consulta Errore DNS () `NonS3OriginDnsError`.

Per ulteriori informazioni sulla gestione del failover DNS, consulta la sezione Configurazione del failover DNS nella Amazon Route 53 Developer Guide.

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, indipendentemente dal fatto che la risposta provenga dall'origine o dalla CloudFront cache.

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 Configura le autorizzazioni e i ruoli 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 alle risorse all'interno del VPC
- Code di lettere morte per la funzione Lambda
- Variabili di ambiente Lambda (ad eccezione delle variabili di ambiente riservate, che sono supportate automaticamente)
- Funzioni Lambda con livelli AWS Lambda
- Uso di AWS X-Ray
- Concorrenza con provisioning di Lambda

> **Note**
>
> Le funzioni Lambda @Edge hanno le stesse funzionalità di concorrenza regionale delle funzioni Lambda. Tuttavia, quando la quota viene aumentata per le esecuzioni Lambda @Edge simultanee, la quota viene aumentata per tutte le aree Regioni AWS in cui viene replicata la funzione Lambda @Edge. Per ulteriori informazioni, consulta Quote di Lambda@Edge.

- Funzioni Lambda definite come immagini del contenitore
- Funzioni Lambda che utilizzano l'architettura arm64
- Funzioni Lambda con oltre 512 MB di storage temporaneo
- Acquisizione dei log delle funzioni Lambda in formato strutturato JSON
- Controllo della granularità a livello di log dei log delle funzioni Lambda
- Impostazione del gruppo di CloudWatch log Amazon a cui Lambda invia i log

Runtime supportati

Lambda@Edge supporta le funzioni Lambda con i seguenti runtime:

Node.js	Python
• Node.js 20	• Python 3.12

Node.js	Python
• Node.js 18 • Node.js 16[1] • Node.js 14 m[2] • Node.js 12[2] • Node.js 10[2] • Node.js 8 m[2] • Node.js 6 m[2]	• Python 3.11 • Python 3.10 • Python 3.9 • Python 3.8 • Python 3.7

[1] Questa versione di Node.js ha raggiunto la fine del ciclo di vita e sarà presto obsoleta da. AWS Lambda

[2]Questa versione di Node.js ha raggiunto la fine del ciclo di vita ed è completamente obsoleta da. AWS Lambda

Non è possibile creare o aggiornare funzioni con versioni obsolete di Node.js. È possibile associare le funzioni esistenti a queste versioni solo alle distribuzioni. CloudFront Le funzioni con queste versioni associate alle distribuzioni continueranno a funzionare. Tuttavia, si consiglia di spostare la funzione su versioni più recenti di Node.js. Per ulteriori informazioni, consulta la politica di deprecazione del Runtime nella AWS Lambda Developer Guide e la pianificazione del rilascio di Node.js su. GitHub

> **Tip**
>
> Come procedura ottimale, utilizzate le versioni più recenti dei runtime forniti per migliorare le prestazioni e aggiungere nuove funzionalità.

CloudFrontintestazioni

Le funzioni Lambda @Edge possono leggere, modificare, rimuovere o aggiungere qualsiasi CloudFront intestazione elencata in. Aggiungi intestazioni CloudFront di richiesta

> **Note**
>
> • Se desideri CloudFront aggiungere queste intestazioni, devi configurarle CloudFront per aggiungerle utilizzando una politica di cache o una politica di richiesta di origine.

- CloudFront aggiunge le intestazioni dopo l'evento di richiesta del visualizzatore, il che significa che le intestazioni non sono disponibili per le funzioni Lambda @Edge in una richiesta del visualizzatore. Le intestazioni sono disponibili solo per le funzioni Lambda @Edge in una richiesta di origine e una risposta di origine.
- Se la richiesta del visualizzatore include intestazioni con questi nomi e hai configurato CloudFront per aggiungere queste intestazioni utilizzando una policy di cache o una policy di richiesta di origine, CloudFront sovrascrive i valori di intestazione presenti nella richiesta del visualizzatore. Le funzioni rivolte al visualizzatore vedono il valore dell'intestazione della richiesta del visualizzatore, mentre le funzioni rivolte all'origine vedono il valore di intestazione aggiunto. CloudFront
- Se una funzione di richiesta del visualizzatore aggiunge l'`CloudFront-Viewer-Country`intestazione, non riesce la convalida e CloudFront restituisce il codice di stato HTTP 502 (Bad Gateway) 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 le seguenti quote di dimensioni per le parti del corpo che vengono esposte o sostituite.

- CloudFront sempre base64 codifica il corpo della richiesta prima di esporlo a Lambda @Edge.
- Se il corpo della richiesta è grande, lo CloudFront tronca prima di esporlo a Lambda @Edge, come segue:
  - 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 modalità di sola lettura, CloudFront invia il corpo completo della richiesta originale all'origine.
- Se la funzione Lambda@Edge sostituisce il corpo della richiesta, si applicano le seguenti quote di dimensioni per il corpo restituito dalla funzione:
  - Se la funzione Lambda@Edge restituisce il corpo come testo semplice:
    - 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 la funzione Lambda@Edge restituisce il corpo codificato in base64:
    - Per gli eventi di richiesta del visualizzatore, il corpo è troncato a 53,2 KB.

- Per gli eventi di richiesta di origine, il corpo è troncato a 1,33 MB.

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 della distribuzione, verifica di specificare un valore che l'origine può supportare. Per ulteriori informazioni, consulta Quote di 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 visualizzare e scaricare report per visualizzare l'utilizzo e l'attività delle tue CloudFront distribuzioni, inclusi report di fatturazione, statistiche sulla cache, contenuti popolari e referrer principali.
- Puoi monitorare e tracciare CloudFront, comprese le tue funzioni di edge computing, direttamente nella CloudFront console o utilizzando Amazon CloudWatch. CloudFront invia diverse metriche CloudWatch per le distribuzioni e le funzioni edge, sia Lambda @Edge che Functions. CloudFront
- Puoi visualizzare i log delle richieste dei visualizzatori che le tue CloudFront distribuzioni ricevono con log standard o log 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
- Puoi tenere traccia delle modifiche alla configurazione CloudFront delle tue risorse utilizzando AWS Config.

Per ulteriori informazioni su ciascuna di 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 AWS Billing and Cost Management console.

Per visualizzare il rapporto di AWS fatturazione

1. Accedi AWS Management Console e apri la AWS Billing console all'indirizzo https://console.aws.amazon.com/billing/.
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 rapporto di fatturazione dettagliato in formato CSV, scegli Scarica tutto in 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 AWS Management Console e apri la AWS Billing console all'indirizzo https://console.aws.amazon.com/billing/.
2. Nel riquadro di navigazione, scegli Costi e rapporti.
3. Nella sezione Rapporto AWS sull'utilizzo, scegli Crea un rapporto sull'utilizzo.

4. Nella pagina Scarica il report sull'utilizzo, in Servizi, scegli Amazon CloudFront
5. Scegli il tipo di utilizzo.
6. Scegli l'operazione.
7. Scegli il periodo di tempo per il rapporto. Se scegli Intervallo di date personalizzato, devi specificare manualmente l'intervallo di date per il rapporto.
8. In Granularità del rapporto, scegli Oraria, Giornaliera o Mensile.
9. Scegli Scarica, quindi scegli Rapporto XML o Rapporto CSV.

Per ulteriori informazioni sul rapporto sull' AWS utilizzo, consulta Report AWS sull'utilizzo nella Guida per l'Esportazioni di dati AWS 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 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 “Utilizzo dei registri standard (log di accesso)”.

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, la *`regione`* in un codice viene sostituita nella AWS fattura e nel rapporto sull'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 fatture e gli elementi del rapporto sull'utilizzo.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
regione - DataTransfer -Out-Bytes Byte totali serviti dalle CloudFront edge location *della regione* in risposta a utenti e richieste . `GET HEAD`	*region*-Out-Bytes-HTTP-Static: Byte forniti tramite HTTP per oggetti con TTL ≥ 3.600 secondi. *region*-Out-Bytes-HTTPS-Static: Byte forniti tramite HTTPS per oggetti con TTL ≥ 3.600 secondi. *region*-Out-Bytes-HTTP-Dynamic: Byte forniti tramite HTTP per oggetti con TTL < 3.600 secondi. *region*-Out-Bytes-HTTPS-Dynamic: Byte forniti tramite HTTPS per oggetti con TTL < 3.600 secondi. *region*-Out-Bytes-HTTP-Proxy:

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
	Byte restituiti CloudFront ai visualizzatori tramite HTTP in risposta a`DELETE`,, `OPTIONS` `PATCH``POST`, e richieste. `PUT`  *region*-Out-Bytes-HTTPS-Proxy:  Byte restituiti CloudFront ai visualizzatori tramite HTTPS in risposta a`DELETE`,, `OPTIONS``PATCH`, `POST` e richieste. `PUT`
region - -out-OBytes DataTransfer Byte totali trasferiti dalle CloudFront edge location alla funzione di origine o periferica in risposta a`DELETE`,`OPTIONS`, `PATCH` e richieste . `POST` `PUT` I costi includono il trasferimento dei WebSocket dati dal client al server.	*region*-Out-OBytes-HTTP-Proxy Byte totali trasferiti tramite HTTP dalle CloudFront edge location alla funzione di origine o periferica in risposta a `DELETE``OPTIONS`, `PATCH``POST`, e `PUT` richieste .  *region*-Out-OBytes-HTTPS-Proxy  Byte totali trasferiti tramite HTTPS dalle CloudFront edge location alla funzione di origine o periferica in risposta a`DELETE`, `OPTIONS` `PATCH``POST`, e `PUT` richieste.
region-Requests-Tier1 Numero di richieste HTTP `GET` e `HEAD`.	*region*-Requests-HTTP-Static Numero di richieste HTTP `GET` e `HEAD` fornite per oggetti con TTL ≥ 3600 secondi. *region*-Requests-HTTP-Dynamic Numero di richieste HTTP `GET` e `HEAD` fornite per oggetti con TTL < 3600 secondi

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
region-Requests-Tier2-HTTPS Numero di richieste HTTPS `GET` e `HEAD`.	*region*-Requests-HTTPS-Static Numero di richieste HTTPS `GET` e `HEAD` fornite per oggetti con TTL ≥ 3600 secondi. *region*-Requests-HTTPS-Dynamic Numero di richieste HTTPS `GET` e `HEAD` fornite per oggetti con TTL < 3600 secondi.
regione-Requests-HTTP-Proxy Numero di `PUT` richieste `HTTPDELETE`,`OPTIONS`, `PATCHPOST`, e che vengono CloudFront inoltrate alla funzione di origine 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.	*regione*-Requests-HTTP-Proxy Uguale all'articolo corrispondente nella fattura CloudFront .
regione-Requests-HTTPS-Proxy Numero di `HTTPSDELETE`,, `OPTIONS` `PATCHPOST`, e `PUT` richieste che vengono CloudFront inoltrate alla funzione di origine o edge. Include anche il numero di WebSocketrichieste HTTPS (`GET`richieste con l'`Upgrade: websocket` intestazione) che vengono CloudFront inoltrate all'origine o alla funzione edge.	*regione*-Requests-HTTPS-Proxy Uguale all'articolo corrispondente nella fattura CloudFront .

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
regione-Requests-HTTPS-Proxy-FLE Numero di HTTPS DELETE e POST richieste elaborate con crittografia a livello di campo che CloudFront inoltra alla funzione di origine o edge. OPTIONSPATCH	*regione*-Requests-HTTPS-Proxy-FLE Uguale all'articolo corrispondente nella fattura. CloudFront
regione -Bytes- OriginShield Byte totali trasferiti dall'origine a qualsiasi edge cache regionale, inclusa la cache edge regionale abilitata come Origin Shield.	***regione -Bytes- OriginShield*** Uguale all'articolo corrispondente nella fattura CloudFront .
regione -OBytes- OriginShield Byte totali trasferiti all'origine da qualsiasi edge cache regionale, inclusa la cache edge regionale abilitata come Origin Shield.	*regione* -OBytes- OriginShield Uguale all'articolo corrispondente nella fattura CloudFront .
regione -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”.	*regione -Richieste* - OriginShield Uguale all'articolo corrispondente nella CloudFront fattura.

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
Invalidations L'addebito per l'invalidazione degli oggetti (rimozione degli oggetti dai CloudFront bordi). Per ulteriori informazioni, consulta Paga 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 alternativo 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 log in tempo reale.	RealTimeLog-KinesisDataStream Uguale all'articolo corrispondente nella CloudFront fattura.
Esecuzioni- CloudFrontFunctions Il costo per il numero di chiamate di CloudFront Functions.	Esecuzioni- CloudFrontFunctions Uguale all'articolo corrispondente nella CloudFront fattura.
regione -Lambda-Edge-Request Il costo per il numero di chiamate alla funzione Lambda @Edge.	***regione -Lambda-Edge-Request*** Uguale all'articolo corrispondente nella fattura. CloudFront
regione -Lambda-edge-GB-secondo L'addebito per la durata dal momento in cui la funzione Lambda @Edge viene richiamata a quando ritorna o termina.	***regione -Lambda-edge-GB-secondo*** Uguale all'articolo corrispondente nella fattura. CloudFront

CloudFront addebiti in fattura AWS	Valori nella UsageType colonna del rapporto sull' AWS utilizzo
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- Operazioni API L'addebito per il numero di chiamate all'CloudFront KeyValueStoreAPI.	KeyValueStore- Operazioni API Uguale alla voce corrispondente nella fattura CloudFront .

Visualizza CloudFront i report nella console

Puoi visualizzare i seguenti report sulla tua CloudFront attività nella console:

Argomenti

- Visualizza i report sulle statistiche CloudFront della cache
- Visualizza i report sugli oggetti CloudFront più diffusi
- Visualizza i report CloudFront sui principali referrer
- Visualizza i report sull'utilizzo CloudFront
- CloudFront Visualizza i report degli spettatori

La maggior parte di questi report si basa sui dati contenuti nei registri di CloudFront accesso, che contengono informazioni dettagliate su ogni richiesta utente CloudFront ricevuta. Non è necessario attivare i log di accesso per visualizzare i report. Per ulteriori informazioni, consulta Configurazione e utilizzo di registri standard (registri di accesso).

Visualizza i report sulle statistiche CloudFront della cache

Il rapporto sulle statistiche CloudFront della cache di Amazon include le seguenti informazioni:

- Total Requests (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 degli spettatori per tipo di risultato: mostra gli accessi, gli errori mancati e gli errori come percentuale del totale delle richieste degli spettatori per la CloudFront distribuzione selezionata.
- Bytes Transferred to Viewers (Byte trasferiti a visualizzatori): mostra il totale dei byte e i byte dai mancati riscontri.
- HTTP Status Codes (Codici di stato HTTP): mostra le richieste visualizzatore per codice di stato HTTP.
- Percentage of GET Requests that Didn't Finish Downloading (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 fonte dei log di CloudFront accesso, ma 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 è possibile visualizzare i dati sulle richieste CloudFront ricevute fino a un'ora fa, ma a volte i dati possono subire ritardi fino a 24 ore.

Argomenti

- Visualizza i report sulle statistiche della CloudFront cache nella console
- Scarica i dati in formato CSV
- In che modo i grafici statistici della cache sono correlati ai dati nei log CloudFront standard (log di accesso)

Visualizza i report sulle statistiche della CloudFront cache nella console

È possibile visualizzare il rapporto sulle statistiche della CloudFront cache nella console.

Per visualizzare le statistiche sulla CloudFront cache

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Cache Statistics.

3. Nel riquadro Rapporti sulle statistiche della CloudFront cache, per Data di inizio e Data di fine, seleziona l'intervallo di date per il quale desideri visualizzare i grafici delle 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 delle statistiche della cache includono i dati relativi alle richieste CloudFront ricevute dalla posizione specificata.
6. Nell'elenco Distribution (Distribuzione), seleziona le distribuzioni per le quali intendi visualizzare i dati nei grafici di utilizzo:

   - Una distribuzione individuale: i grafici mostrano i dati per la CloudFront distribuzione 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 mostrano i dati sommati per tutte le distribuzioni associate al AWS conto corrente, escluse le distribuzioni eliminate.
7. Scegli Aggiorna.

Per visualizzare i dati relativi a un punto dati giornaliero o orario all'interno di un grafico, passa il mouse sopra il punto dati.

Per i grafici che mostrano i dati trasferiti, puoi impostare la scala verticale su gigabyte, megabyte o kilobyte per ogni grafico.

Scarica i 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 rapporto 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 di visualizzatori per le quali l'oggetto viene servito da una cache CloudFront edge.

MissCount

Il numero di richieste di visualizzazione per le quali l'oggetto non si trova attualmente in una cache edge, quindi è CloudFront necessario recuperare l'oggetto dall'origine.

ErrorCount

Il numero di richieste dei visualizzatori che hanno generato un errore, quindi, CloudFront non sono servite all'oggetto.

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 forniti ai visualizzatori CloudFront 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 cache di origine alle cache edge. CloudFront Tuttavia, esclude le richieste per oggetti già presenti nella cache edge, ma scaduti.

In che modo i grafici statistici della cache sono correlati ai dati nei log CloudFront standard (log di accesso)

La tabella seguente mostra come i grafici delle statistiche della cache nella CloudFront console corrispondano ai valori nei log di CloudFront accesso. Per ulteriori informazioni sui log di CloudFront accesso, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 mostra accessi, mancati ed errori come percentuale delle richieste totali degli spettatori per la distribuzione selezionata CloudFront :

- Hit: una richiesta del visualizzatore per la quale l'oggetto viene fornito da una cache CloudFront edge. Nei log di accesso, si tratta delle richieste per le quali il valore di `x-edge-response-result-type` è `Hit`.
- Miss: una richiesta del visualizzatore per la quale l'oggetto non si trova attualmente in una cache edge, quindi è CloudFront necessario recuperare 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`.
- Errore: una richiesta del visualizzatore che ha provocato un errore, quindi CloudFront non è servita all'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:

- Byte totali: il numero totale di byte forniti agli utenti CloudFront in risposta a tutte le richieste per tutti i metodi HTTP. Nei log di CloudFront accesso, Total Bytes è la somma dei valori nella `sc-bytes` colonna per tutte le richieste nello 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 CloudFront accesso, i byte mancanti sono la somma dei valori nella `sc-bytes` colonna per le richieste per le quali il valore di è. `x-edge-result-type` `Miss` Questo valore è una buona approssimazione dei byte trasferiti dalla cache di origine alle cache edge. 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 registri di CloudFront accesso, i codici di stato vengono 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 registri di CloudFront accesso, queste richieste hanno un valore di `200` nella `sc-status` colonna e un valore di `Error` nella `x-edge-result-type` colonna.

Visualizza i report sugli oggetti CloudFront più diffusi

Visualizza il report Amazon CloudFront popular objects per vedere i 50 oggetti più popolari per una distribuzione in un intervallo di date specificato nei 60 giorni precedenti. Puoi anche visualizzare le statistiche su tali oggetti, tra cui:

- Numero di richieste per l'oggetto
- Numero di riscontri e mancati
- Hit Ratio (Percentuale di riscontri)
- Numero di byte serviti in caso di errori
- Numero totale di byte 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 fonte dei log di CloudFront accesso, ma non è necessario abilitare la registrazione degli accessi per visualizzare gli oggetti più diffusi.

Argomenti

- Visualizza i report sugli oggetti CloudFront più diffusi nella console

- Come CloudFront calcola le statistiche sugli oggetti più diffusi
- Scarica i dati in formato CSV
- In che modo i dati del report Popular Objects sono correlati ai dati nei log CloudFront standard (log di accesso)

Visualizza i report sugli oggetti CloudFront più diffusi nella console

È possibile visualizzare il report sugli oggetti CloudFront più diffusi nella console.

Per visualizzare gli oggetti più diffusi per una CloudFront distribuzione

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Oggetti popolari.
3. Nel riquadro del rapporto Oggetti CloudFront popolari, per Data di inizio e Data di 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. Scegli Aggiorna.

Come CloudFront calcola le statistiche sugli oggetti più diffusi

Per ottenere un conteggio accurato dei primi 50 oggetti della distribuzione, CloudFront conta le richieste per tutti gli oggetti a intervalli di 10 minuti a partire da mezzanotte e mantiene attivo un totale dei primi 150 oggetti per le 24 ore successive. (conserva CloudFront inoltre i totali giornalieri dei primi 150 oggetti per 60 giorni.)

Nella parte inferiore dell'elenco, gli oggetti salgono o scendono costantemente dall'elenco, quindi i totali di tali oggetti sono approssimativi. I 50 oggetti in cima all'elenco dei 150 oggetti possono salire e scendere all'interno dell'elenco, ma raramente vengono eliminati del tutto dall'elenco, quindi i totali di tali oggetti sono più affidabili.

Quando un oggetto esce dall'elenco dei primi 150 oggetti e poi sale nuovamente nell'elenco nel corso di una giornata, CloudFront aggiunge un numero stimato di richieste per il periodo in cui l'oggetto

mancava dall'elenco. La stima si basa sul numero di richieste ricevute da qualsiasi oggetto nella parte bassa dell'elenco durante tale periodo di tempo.

Se l'oggetto rientra tra i primi 50 oggetti nel corso della giornata, le stime del numero di richieste CloudFront ricevute mentre l'oggetto non rientrava tra i primi 150 oggetti in genere fanno sì che il numero di richieste nel report Popular Objects superi il numero di richieste che compaiono nei log di accesso per quell'oggetto.

Scarica i 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 diffusi, 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 di visualizzatori per le quali l'oggetto viene servito da una cache CloudFront edge.

MissCount

Il numero di richieste di visualizzazione per le quali l'oggetto non si trova attualmente in una cache edge, quindi è CloudFront necessario recuperare 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 forniti agli spettatori da CloudFront questo 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).

In che modo i dati del report Popular Objects sono correlati ai dati nei log CloudFront standard (log di accesso)

L'elenco seguente mostra come i valori nel report Popular Objects nella CloudFront console corrispondano ai valori nei log di CloudFront accesso. Per ulteriori informazioni sui log di CloudFront accesso, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 generalmente corrisponde strettamente al numero di `GET` richieste per l'oggetto nei log di CloudFront accesso.

Hits (occorrenze)

Il numero di richieste di visualizzazione per le quali l'oggetto è stato fornito da una cache CloudFront edge. 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 dei visualizzatori per le quali l'oggetto non era in una cache edge, quindi l'oggetto è stato CloudFront recuperato dall'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 CloudFront accesso, i byte mancanti sono la somma dei valori nella `sc-bytes` colonna per le richieste per le quali il valore di è. `x-edge-result-type` `Miss`

Total Bytes (Totale byte)

Il numero totale di byte CloudFront forniti agli utenti in risposta a tutte le richieste dell'oggetto per tutti i metodi HTTP. Nei log di CloudFront accesso, i byte totali sono la somma dei valori nella `sc-bytes` colonna per tutte le richieste nello 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 registri di CloudFront accesso, queste richieste hanno un valore di `200` nella `sc-status` colonna e un valore di `Error` nella colonna. `x-edge-result-type`

2xx

Il numero di richieste per le quali il codice di stato HTTP è `2xx`, `Successful`. Nei registri di CloudFront accesso, i codici di stato vengono visualizzati nella `sc-status` colonna.

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.

Visualizza i report CloudFront sui principali referrer

Il rapporto sui CloudFront principali referrer include quanto segue per qualsiasi intervallo di date negli ultimi 60 giorni:

- I 25 principali referrer (domini di siti Web che hanno originato il maggior numero di richieste HTTP e HTTPS relative a oggetti distribuiti per la distribuzione dell'utente) CloudFront
- Numero di richieste provenienti da un referente
- Numero di richieste provenienti da un referente come percentuale del numero totale di richieste durante il periodo specificato

I dati del rapporto sui principali referrer provengono dalla stessa fonte dei log di CloudFront accesso, ma non è necessario abilitare la registrazione degli accessi per visualizzare i principali referrer.

I principali referrer possono essere i motori di ricerca, altri siti web che rimandano direttamente ai tuoi oggetti o il tuo sito web. Ad esempio, se `https://example.com/index.html` rimanda a 10 immagini, `example.com` è il referente per tutte le 10 immagini.

> **Note**
>
> Se un utente immette un URL direttamente nella riga dell'indirizzo di un browser, non esistono referrer per l'oggetto richiesto.

Argomenti

- Visualizza i report dei CloudFront principali referrer nella console

- Come calcola le statistiche CloudFront dei principali referrer
- Scarica i dati in formato CSV
- In che modo i dati del rapporto sui principali referrer sono correlati ai dati nei log CloudFront standard (log di accesso)

Visualizza i report dei CloudFront principali referrer nella console

Puoi visualizzare il rapporto sui CloudFront principali referrer nella console.

Per visualizzare i principali referrer di una distribuzione CloudFront

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Nel riquadro di navigazione, scegli Top Referrers.
3. Nel riquadro del rapporto CloudFront Top Referrer, per Data di inizio e Data di fine, seleziona l'intervallo di date per il quale desideri visualizzare un elenco dei principali referrer.

   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. Scegli Aggiorna.

Come calcola le statistiche CloudFront dei principali referrer

Per ottenere un conteggio accurato dei primi 25 referrer, CloudFront conta le richieste per tutti gli oggetti a intervalli di 10 minuti e mantiene un totale aggiornato dei primi 75 referrer. Nella parte inferiore dell'elenco, i referrer salgono o scendono costantemente dall'elenco, quindi i totali di tali referrer sono approssimativi.

I 25 referrer in cima all'elenco dei 75 referrer possono salire e scendere all'interno dell'elenco, ma raramente vengono eliminati del tutto dall'elenco, quindi i totali di tali referrer sono in genere più affidabili.

Scarica i 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 rapporto Top Referrers, 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.

In che modo i dati del rapporto sui principali referrer sono correlati ai dati nei log CloudFront standard (log di accesso)

L'elenco seguente mostra in che modo i valori nel rapporto Top Referrers nella CloudFront console corrispondono ai valori nei log di accesso. CloudFront Per ulteriori informazioni sui log di CloudFront accesso, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 generalmente corrisponde strettamente al numero di `GET` richieste provenienti dal referente nei log di CloudFront accesso.

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.

Visualizza i report sull'utilizzo CloudFront

I report CloudFront sull'utilizzo includono le seguenti informazioni:

- Numero di richieste: mostra il numero totale di richieste a cui CloudFront risponde dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata CloudFront .
- Dati trasferiti tramite protocollo e dati trasferiti per destinazione: entrambi mostrano la quantità totale di dati trasferiti dalle CloudFront edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata. CloudFront 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: verso i tuoi spettatori o verso la tua origine.

Il rapporto CloudFront sull'utilizzo si basa sul rapporto AWS sull'utilizzo per CloudFront, che non richiede alcuna configurazione speciale. Per ulteriori informazioni, consulta Visualizza il report sull'utilizzo per AWS CloudFront.

Puoi visualizzare i report per un intervallo di date specificato negli ultimi 60 giorni, con punti dati ogni ora o ogni giorno. In genere è possibile visualizzare i dati sulle richieste CloudFront ricevute non più di quattro ore fa, ma a volte i dati possono subire ritardi fino a 24 ore.

Per ulteriori informazioni, consulta In che modo le tabelle di utilizzo sono correlate ai dati nel rapporto sull' CloudFront utilizzo.

Argomenti

Visualizza i report di CloudFront utilizzo nella console

È possibile visualizzare il rapporto CloudFront sull'utilizzo nella console.

Per visualizzare i report CloudFront sull'utilizzo

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Rapporti di utilizzo.
3. Nel riquadro Rapporti sull'CloudFront utilizzo, per Data di inizio e Data di 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 Regione di fatturazione, scegli l'area di CloudFront fatturazione con i dati che desideri visualizzare oppure scegli Tutte le regioni. I grafici di utilizzo includono i dati relativi alle richieste CloudFront elaborate nelle sedi periferiche della regione specificata. La regione in cui CloudFront elabora le richieste potrebbe corrispondere o meno alla posizione dei tuoi spettatori.

   Seleziona solo le regioni incluse nella fascia di prezzo per la tua distribuzione. Altrimenti, i grafici di utilizzo probabilmente non conterranno alcun dato. Ad esempio, se hai scelto la classe di prezzo 200 per la tua distribuzione, le aree di fatturazione del Sud America e dell'Australia non sono incluse, quindi in CloudFront genere non elaboriamo le tue richieste da tali aree. Per ulteriori informazioni sulle classi di prezzo, consulta la pagina CloudFront dei prezzi.
6. Nell'elenco Distribution (Distribuzione), seleziona le distribuzioni per le quali intendi visualizzare i dati nei grafici di utilizzo:

   - Una distribuzione individuale: i grafici mostrano i dati per la CloudFront distribuzione 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 mostrano i dati sommati per tutte le distribuzioni associate all' AWS account corrente e che sono state eliminate negli ultimi 60 giorni.

7. Scegli Aggiorna grafici.

Per visualizzare i dati relativi a un punto dati giornaliero o orario all'interno di un grafico, passa il mouse sopra il punto dati.

Per i grafici che mostrano i dati trasferiti, puoi impostare la scala verticale su gigabyte, megabyte o kilobyte per ogni grafico.

Scarica i dati in formato CSV

Puoi scaricare il rapporto sull'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 rapporto sull'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

L'area di CloudFront fatturazione per cui hai eseguito il rapporto, 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 hanno risposto dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata. CloudFront I valori includono:

- Il numero di `HEAD` richieste `GET` e, che causano il trasferimento CloudFront di dati ai tuoi spettatori

- Il numero diDELETE,OPTIONS, PATCHPOST, e PUT richieste che causano CloudFront il trasferimento dei dati all'origine

HTTPS

Il numero di richieste HTTPS a cui CloudFront hanno risposto dalle edge location nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata CloudFront . I valori includono:

- Il numero di HEAD richieste GET e, che causano il trasferimento CloudFront di dati ai tuoi spettatori
- Il numero diDELETE,OPTIONS, PATCHPOST, e PUT richieste che causano CloudFront il trasferimento dei dati all'origine

HTTPBytes

La quantità totale di dati trasferiti tramite HTTP dalle CloudFront edge location nella regione di fatturazione selezionata durante il periodo di tempo della CloudFront distribuzione specificata. I valori includono:

- Dati trasferiti dai CloudFront tuoi spettatori in risposta a GET richieste e richieste HEAD
- Dati trasferiti dai tuoi spettatori a CloudFront forDELETE,, OPTIONS PATCHPOST, e richieste PUT
- Dati CloudFront trasferiti dai tuoi spettatori in risposta aDELETE,, OPTIONS PATCHPOST, e richieste PUT

HTTPSBytes

La quantità totale di dati trasferiti tramite HTTPS dalle CloudFront edge location nella regione di fatturazione selezionata durante il periodo di tempo per la distribuzione specificata CloudFront . I valori includono:

- Dati trasferiti dai CloudFront tuoi spettatori in risposta a GET richieste e richieste HEAD
- Dati trasferiti dai tuoi spettatori a CloudFront forDELETE,, OPTIONS PATCHPOST, e richieste PUT
- Dati CloudFront trasferiti dai tuoi spettatori in risposta aDELETE,, OPTIONS PATCHPOST, e richieste PUT

BytesIn

La quantità totale di dati trasferiti dall' CloudFront origine perDELETE,, OPTIONS PATCHPOST, e PUT le richieste nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata CloudFront .

BytesOut

La quantità totale di dati trasferiti tramite HTTP e HTTPS dai CloudFront visualizzatori nella regione selezionata durante ogni intervallo di tempo per la distribuzione specificata. CloudFront I valori includono:

- Dati trasferiti dai CloudFront tuoi spettatori in risposta a richieste e richieste `GET` `HEAD`
- Dati CloudFront trasferiti dai tuoi spettatori in risposta a`DELETE`,, `OPTIONS` `PATCH``POST`, e richieste `PUT`

In che modo le tabelle di utilizzo sono correlate ai dati nel rapporto sull' CloudFront utilizzo

L'elenco seguente mostra come i grafici di utilizzo nella CloudFront console corrispondono ai valori nella colonna Tipo di utilizzo del rapporto CloudFront sull'utilizzo.

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 dalle edge location nella regione selezionata durante ogni intervallo di tempo per la CloudFront distribuzione specificata, separate per 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
- *`region`* -requests-HTTP-Proxy: numero di HTTP`DELETE`,, `OPTIONS``PATCH`, e richieste che vengono inoltrate all'`POST`origine `PUT` CloudFront

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
- *region* -requests-HTTPS-Proxy: numero di HTTPS`DELETE`,,, e richieste inoltrate all'origine `OPTIONS` `PATCH` `POST` `PUT` CloudFront

Data Transferred by Protocol (Dati trasferiti per protocollo)

Questo grafico mostra la quantità totale di dati trasferiti dalle CloudFront edge location nella regione selezionata durante ogni intervallo di tempo per la CloudFront distribuzione 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
- *region* -out-Bytes-HTTP-proxy: byte restituiti CloudFront ai visualizzatori tramite HTTP in risposta a,, e richieste `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-obytes-HTTP-Proxy: byte totali trasferiti tramite HTTP dalle edge location all'origine in risposta a,, e richieste CloudFront `DELETE` `OPTIONS` `PATCH` `POST` `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
- *region* -out-Bytes-HTTPS-Proxy: byte restituiti ai visualizzatori tramite HTTPS in risposta a,, e richieste CloudFront `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-obytes-HTTPS-Proxy: byte totali trasferiti tramite HTTPS dalle edge location all'origine in risposta a,, e richieste CloudFront `DELETE` `OPTIONS` `PATCH` `POST` `PUT`

Data Transferred by Destination (Dati trasferiti per destinazione)

Questo grafico mostra la quantità totale di dati trasferiti dalle CloudFront edge location nella regione selezionata durante ogni intervallo di tempo per la CloudFront distribuzione specificata, separati per destinazione (visualizzatori o origine), protocollo (HTTP o HTTPS) e tipo (statico, dinamico o proxy).

Dati trasferiti dai tuoi CloudFront spettatori

- *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
- *region* -out-Bytes-HTTP-Proxy: byte restituiti CloudFront ai visualizzatori tramite HTTP in risposta a,,, e richieste `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-Bytes-HTTPS-Proxy: byte restituiti ai visualizzatori tramite HTTPS in risposta a,, e richieste CloudFront `DELETE` `OPTIONS` `PATCH` `POST` `PUT`

Dati CloudFront trasferiti dall'origine

- *region* -out-obytes-HTTP-Proxy: byte totali trasferiti tramite HTTP dalle CloudFront edge location all'origine in risposta a,,, e richieste `DELETE` `OPTIONS` `PATCH` `POST` `PUT`
- *region* -out-obytes-HTTPS-Proxy: byte totali trasferiti tramite HTTPS dalle edge location all'origine in risposta a,, e richieste CloudFront `DELETE` `OPTIONS` `PATCH` `POST` `PUT`

CloudFront Visualizza i report degli spettatori

CloudFront I rapporti sugli spettatori includono le seguenti informazioni per qualsiasi intervallo di date dei 60 giorni precedenti:

- Dispositivi: i tipi di dispositivi utilizzati più frequentemente per accedere ai contenuti dell'utente (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 (come Linux, macOS o Windows)
- Località: le prime 50 località (paesi o stati/territori degli Stati Uniti) degli spettatori che accedono più frequentemente ai tuoi contenuti
  - Può anche visualizzare le sedi con punti dati orari per qualsiasi intervallo di date fino a 14 giorni nei 60 giorni precedenti

Non è necessario abilitare la registrazione degli accessi per visualizzare i grafici e i report degli utenti.

Argomenti

- Visualizza i grafici e i report degli spettatori nella console
- Scarica i dati in formato CSV
- Dati inclusi nei report degli spettatori
- In che modo i dati nel rapporto sulle sedi sono correlati ai dati nei registri CloudFront standard (registri di accesso)

Visualizza i grafici e i report degli spettatori nella console

Puoi visualizzare CloudFront i grafici e i report degli spettatori nella console.

Per visualizzare grafici e CloudFront report sugli spettatori

1. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Nel riquadro di navigazione, scegli Visualizzatori.
3. Nel riquadro CloudFront Visualizzatori, per Data di inizio e Data di fine, seleziona l'intervallo di date per il quale desideri visualizzare i grafici e i report dei 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 distribuzione individuale: i grafici mostrano i dati per la CloudFront distribuzione 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 mostrano i dati sommati per tutte le distribuzioni associate al AWS conto corrente, escluse le distribuzioni eliminate.
8. Scegli Aggiorna.

Per visualizzare i dati relativi a un punto dati giornaliero o orario all'interno di un grafico, passa il mouse sopra il punto dati.

Scarica i 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 rapporto Viewer, 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 degli spettatori

Le prime righe di ogni rapporto 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 report dei diversi 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 CloudFront ricevute da ciascun tipo di dispositivo.

RequestsPct

Il numero di richieste CloudFront ricevute da ciascun tipo di dispositivo come percentuale del numero totale di richieste CloudFront ricevute da tutti i dispositivi.

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 CloudFront ricevute dai computer desktop durante il periodo.

Mobile

Il numero di richieste CloudFront ricevute dai dispositivi mobili durante il periodo. I dispositivi mobili possono includere tablet e cellulari. Se non è CloudFront possibile determinare se una richiesta proviene da un dispositivo mobile o da un tablet, viene conteggiata nella `Mobile` colonna.

Smart TV

Il numero di richieste CloudFront ricevute dalle smart TV durante il periodo.

Tablet

Il numero di richieste CloudFront ricevute dai tablet durante il periodo. Se non è CloudFront possibile determinare se una richiesta proviene da un dispositivo mobile o da un tablet, viene conteggiata nella `Mobile` colonna.

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 CloudFront ricevute che non includevano un valore nell'`User-Agent`intestazione HTTP 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 hanno 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.
- Altro: browser che si sono CloudFront identificati ma che non sono tra i più diffusi. 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 CloudFront ricevute da ciascun tipo di browser.

RequestsPct

Il numero di richieste CloudFront ricevute da ciascun tipo di browser come percentuale del numero totale di richieste CloudFront ricevute 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.
- Altro: browser che si sono CloudFront identificati ma che non sono tra i più diffusi. 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 sono CloudFront state ricevute 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.
- Altro: sistemi operativi CloudFront identificati ma che non sono tra i più diffusi. 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 CloudFront ricevute da ciascun tipo di sistema operativo.

RequestsPct

Il numero di richieste CloudFront ricevute da ciascun tipo di sistema operativo come percentuale del numero totale di richieste CloudFront ricevute 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.
- Altro: sistemi operativi CloudFront identificati ma che non sono tra i più diffusi. 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

Abbreviazione della località da cui sono CloudFront state ricevute le richieste. Per ulteriori informazioni sui possibili valori, consulta la descrizione di Location (Ubicazione) in In che modo i dati nel rapporto sulle sedi sono correlati ai dati nei registri CloudFront standard (registri di accesso).

LocationName

Il nome della posizione da cui sono CloudFront state ricevute le richieste.

Richieste

Il numero di richieste CloudFront ricevute da ciascuna sede.

RequestsPct

Il numero di richieste CloudFront ricevute da ciascuna sede come percentuale del numero totale di richieste CloudFront ricevute da tutte le sedi durante il periodo di tempo.

TotalBytes

Il numero di byte CloudFront forniti agli spettatori 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 colonne rimanenti del rapporto elencano le località da cui CloudFront hanno ricevuto le richieste. Per ulteriori informazioni sui possibili valori, consulta la descrizione di Location (Ubicazione) in In che modo i dati nel rapporto sulle sedi sono correlati ai dati nei registri CloudFront standard (registri di accesso).

In che modo i dati nel rapporto sulle sedi sono correlati ai dati nei registri CloudFront standard (registri di accesso)

L'elenco seguente mostra in che modo i dati nel rapporto Posizioni nella CloudFront console corrispondono ai valori nei registri di CloudFront accesso. Per ulteriori informazioni sui log di CloudFront accesso, vedere. Configurazione e utilizzo di registri standard (registri di accesso)

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 ubicazioni per paese, nota che 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. Gli spettatori potrebbero trovarsi in paesi ad alto 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) come impostazione predefinita.

- 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/Pacifico (Unknown) come impostazione predefinita.

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 non è CloudFront possibile determinare la posizione di un utente, la posizione verrà visualizzata come Sconosciuta nei report degli utenti.

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 generalmente corrisponde strettamente al numero di `GET` richieste provenienti da indirizzi IP di quel paese o stato nei registri di CloudFront accesso.

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 CloudFront forniti agli spettatori in questo Paese o stato, per la distribuzione e il periodo specificati. Per visualizzare i dati in questa colonna in KB, MB o GB, fai clic sul collegamento nell'intestazione della colonna.

Monitoraggio delle CloudFront metriche con Amazon CloudWatch

Amazon CloudFront è integrato con Amazon CloudWatch e pubblica automaticamente i parametri operativi per le distribuzioni e le funzioni edge (sia Lambda @Edge che Functions). CloudFront Molte di queste metriche vengono visualizzate in un set di grafici nella CloudFront console e sono accessibili anche tramite l' CloudFront API o la CLI. Tutte queste metriche sono disponibili nella CloudWatch console o tramite l' CloudWatch API o la CLI. Le CloudFront metriche non vengono conteggiate ai fini delle CloudWatch quote (precedentemente note come limiti) e non comportano costi aggiuntivi.

Oltre alle metriche predefinite per le CloudFront distribuzioni, puoi attivare metriche aggiuntive a un costo aggiuntivo. Le metriche aggiuntive si applicano alle CloudFront distribuzioni e devono essere attivate separatamente per ciascuna distribuzione. Per ulteriori informazioni sui costi, consulta the section called “Stima del costo delle metriche aggiuntive CloudFront ”.

La visualizzazione di queste metriche consente di risolvere, tenere traccia ed eseguire il debug dei problemi. Per visualizzare queste metriche nella CloudFront console, consulta la pagina Monitoraggio. Per visualizzare i grafici sull'attività per una specifica funzione di CloudFront distribuzione o periferica, scegline una, quindi scegli Visualizza metriche di distribuzione o Visualizza metriche.

Puoi anche impostare allarmi in base a queste metriche nella console o nella CloudFront console, nell'API o nella CLI (si applicano i prezzi standard CloudWatch). CloudWatch 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. Per ulteriori informazioni, consulta Creazione di allarmi.

> **Note**
>
> Quando crei un CloudWatch allarme nella CloudFront console, ne crea uno per te nella regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1` Se crei un allarme dalla CloudWatch console, devi usare la stessa regione. Poiché CloudFront si tratta di un servizio globale, le metriche relative al servizio vengono inviate agli Stati Uniti orientali (Virginia settentrionale).

Argomenti

Visualizzazione CloudFront e metriche delle funzioni edge

È possibile visualizzare le metriche operative relative alle CloudFront distribuzioni e alle funzioni edge nella console. CloudFront Per visualizzare queste metriche, consulta la pagina Monitoraggio nella console. CloudFront Per visualizzare i grafici sull'attività per una specifica funzione di CloudFront distribuzione o periferica, scegline una, quindi scegli Visualizza metriche di distribuzione o Visualizza metriche.

Argomenti

Visualizzazione delle metriche di distribuzione predefinite CloudFront

Le seguenti metriche predefinite sono incluse per tutte le CloudFront distribuzioni, senza costi aggiuntivi:

Richieste

Il numero totale di richieste di visualizzatori ricevute da CloudFront, per tutti i metodi HTTP e per entrambe le richieste HTTP e HTTPS.

Byte scaricati

Il numero di byte scaricati dai visualizzatori per le richieste `GET`, `HEAD` e `OPTIONS`.

Byte caricati

Il numero totale di byte caricati CloudFront, utilizzati `POST` e `PUT` richiesti dagli spettatori.

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 CloudFront distribuzione 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.

Puoi personalizzare i grafici nel modo seguente:

- 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.
- Per modificare la frequenza di CloudFront aggiornamento delle informazioni nel grafico, scegli la freccia rivolta verso il basso accanto all'icona di aggiornamento, quindi scegli una frequenza di aggiornamento. La velocità di aggiornamento di default è di 1 minuto, ma è possibile scegliere 10 secondi, 2 minuti o altre opzioni.

Per visualizzare CloudFront i grafici nella CloudWatch console, scegli Aggiungi alla dashboard.

Attivazione di metriche di CloudFront distribuzione aggiuntive

Oltre ai parametri predefiniti, è possibile attivare ulteriori parametri a un costo aggiuntivo. Per ulteriori informazioni sui costi, consulta the section called “Stima del costo delle metriche aggiuntive CloudFront ”.

Tali parametri aggiuntivi devono essere attivati separatamente per ogni distribuzione:

Percentuale di riscontri nella cache

La percentuale di tutte le richieste memorizzabili nella cache per le quali è CloudFront stato fornito il contenuto della cache. Le richieste HTTP `POST` e `PUT` e gli errori non sono considerati memorizzabili nella cache.

Latenza di origine

Il tempo totale impiegato 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 CloudFront cache. Questa è anche nota come latenza del 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`.

Attivazione di parametri aggiuntivi

Puoi attivare metriche aggiuntive nella CloudFront console, con AWS CloudFormation, con AWS Command Line Interface (AWS CLI) o con l'API. CloudFront

Console

Attivazione di parametri aggiuntivi (console)

1. Accedi AWS Management Console e apri la pagina di monitoraggio nella CloudFront console.
2. Scegliere la distribuzione per cui attivare ulteriori parametri, quindi scegliere View distribution metrics (Visualizza parametri di distribuzione).
3. Scegliere Manage additional metrics (Gestisci parametri aggiuntivi).
4. 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.

Puoi personalizzare i grafici nel modo seguente:

- 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.
- Per modificare la frequenza di CloudFront aggiornamento delle informazioni nel grafico, scegli la freccia rivolta verso il basso accanto all'icona di aggiornamento, quindi scegli una frequenza di aggiornamento. La velocità di aggiornamento di default è di 1 minuto, ma è possibile scegliere 10 secondi, 2 minuti o altre opzioni.

Per visualizzare CloudFront i grafici nella CloudWatch console, scegli Aggiungi alla dashboard.

AWS CloudFormation

Per attivare metriche aggiuntive con AWS CloudFormation, usa il tipo di `AWS::CloudFront::MonitoringSubscription` risorsa. L'esempio seguente mostra la sintassi del AWS CloudFormation modello, in formato YAML, per abilitare metriche aggiuntive.

```
Type: AWS::CloudFront::MonitoringSubscription
Properties:
  DistributionId: EDFDVBD6EXAMPLE
  MonitoringSubscription:
    RealtimeMetricsSubscriptionConfig:
      RealtimeMetricsSubscriptionStatus: Enabled
```

CLI

Per gestire metriche aggiuntive con AWS Command Line Interface (AWS CLI), utilizzate uno dei seguenti comandi:

Attivazione di parametri aggiuntivi per una distribuzione (CLI)

- Utilizza il comando create-monitoring-subscription come nell'esempio seguente. Sostituire *EDFDVBD6EXAMPLE* con l'ID della distribuzione per la quale si stanno attivando metriche aggiuntive.

```
aws cloudfront create-monitoring-subscription --
distribution-id EDFDVBD6EXAMPLE --monitoring-subscription
 RealtimeMetricsSubscriptionConfig={RealtimeMetricsSubscriptionStatus=Enabled}
```

Per verificare se sono abilitati parametri aggiuntivi aggiuntive per una distribuzione (CLI)

- Utilizza il comando get-monitoring-subscription come nell'esempio seguente. Sostituire *EDFDVBD6EXAMPLE* con l'ID della distribuzione che si sta controllando.

```
aws cloudfront get-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

Disattivazione di parametri aggiuntivi per una distribuzione (CLI)

- Utilizza il comando delete-monitoring-subscription come nell'esempio seguente. Sostituire *EDFDVBD6EXAMPLE* con l'ID della distribuzione per la quale si stanno disattivando parametri aggiuntivi.

```
aws cloudfront delete-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

API

Per gestire metriche aggiuntive con l' CloudFront API, utilizzate una delle seguenti operazioni API.

- Per attivare metriche aggiuntive per una distribuzione, usa. CreateMonitoringSubscription
- Per vedere se le metriche aggiuntive sono attivate per una distribuzione, usa. GetMonitoringSubscription
- Per disattivare metriche aggiuntive per una distribuzione, usa. DeleteMonitoringSubscription

Per ulteriori informazioni su queste chiamate API, consulta la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Stima del costo delle metriche aggiuntive CloudFront

Quando attivi metriche aggiuntive per una distribuzione, CloudFront invia fino a 8 metriche CloudWatch nella regione Stati Uniti orientali (Virginia settentrionale). CloudWatch applica 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, quindi il costo rimane invariato indipendentemente dal numero di richieste o risposte ricevute o inviate dalla CloudFront distribuzione.

Per la tariffa metrica, consulta la pagina CloudWatch dei prezzi di Amazon e il calcolatore dei prezzi. CloudWatch Quando recuperi le metriche con l'API, vengono applicati costi API aggiuntivi. CloudWatch

Visualizzazione dei parametri predefiniti della funzione Lambda@Edge

Puoi utilizzare le CloudWatch metriche 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 CloudFront distribuzione, Lambda inizia a inviare automaticamente le metriche a. CloudWatch Le metriche sono disponibili per tutte le regioni Lambda, ma per visualizzare le metriche nella CloudWatch console o ottenere i dati delle metriche dall'API, devi utilizzare CloudWatch la regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1` Il nome del gruppo di metriche è formattato come:`AWS/CloudFront/`*`distribution-ID`*, dove *`Distribution-ID`* è l'ID della distribuzione a cui è CloudFront associata la funzione Lambda @Edge. Per ulteriori informazioni sui CloudWatch parametri, consulta la Amazon CloudWatch User Guide.

Le seguenti metriche predefinite sono 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 una granularità di 1 minuto, raggruppati per regione. AWS

Se si verifica un picco di errori che si desidera esaminare, è possibile scegliere una funzione e quindi visualizzare i file di registro per AWS regione, fino a determinare quale funzione 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 su AWS

Puoi personalizzare i grafici nel modo seguente:

- 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.
- Per modificare la frequenza di CloudFront aggiornamento delle informazioni nel grafico, scegliete la freccia rivolta verso il basso accanto all'icona di aggiornamento, quindi scegliete una frequenza di aggiornamento. La velocità di aggiornamento di default è di 1 minuto, ma è possibile scegliere 10 secondi, 2 minuti o altre opzioni.

Per visualizzare i grafici nella CloudWatch console, scegli Aggiungi alla dashboard. È necessario utilizzare la regione Stati Uniti orientali (Virginia settentrionale) (us-east-1) per visualizzare i grafici nella console. CloudWatch

Visualizzazione delle metriche predefinite delle funzioni CloudFront

CloudFront Functions invia metriche operative 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 le seguenti metriche 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 è vicino 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%, si consiglia di esaminarla per ridurre i tempi di esecuzione e migliorarne l'utilizzo. Ad esempio, potresti voler registrare solo gli errori, semplificare le espressioni regex 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

CloudFront KeyValueStore invia anche le seguenti metriche operative ad Amazon CloudWatch:

- Richieste di lettura (`KvsReadRequests`): il numero di volte in cui la funzione è stata letta correttamente dall'archivio di valori chiave 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 chiave entro un determinato periodo di tempo.

Per visualizzare queste metriche nella CloudFront console, vai alla pagina Monitoraggio. Per visualizzare i grafici relativi a una funzione specifica, seleziona Funzioni, scegli la funzione, quindi seleziona Visualizza parametri funzione.

Tutte queste metriche vengono pubblicate CloudWatch nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), nel namespace. CloudFront Puoi anche visualizzare queste metriche nella console. CloudWatch Nella CloudWatch console, puoi visualizzare le metriche per funzione o per funzione per distribuzione.

Puoi anche utilizzare CloudWatch per impostare allarmi in base a queste metriche.
Ad esempio, puoi impostare un avviso in base al parametro del tempo di esecuzione (`FunctionComputeUilization`), che rappresenta la percentuale di tempo disponibile impiegato dalla funzione per l'esecuzione. Quando il tempo di esecuzione raggiunge un determinato valore per un certo periodo di tempo, ad esempio, superiore al 70% del tempo disponibile per 15 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**
>
> CloudFront Functions invia le metriche CloudWatch solo per le funzioni nella `LIVE` fase che vengono eseguite in risposta alle richieste e alle risposte di produzione. Quando testate una funzione, CloudFront non invia alcuna metrica 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

Per informazioni su come ottenere queste metriche con l' CloudWatch API, consulta. the section called “Ottenimento di parametri mediante l'API”

Creazione di allarmi per i parametri

Nella CloudFront console, puoi impostare allarmi per ricevere notifiche tramite Amazon Simple Notification Service (Amazon SNS) in base a parametri specifici. CloudFront Puoi impostare un allarme nella pagina Allarmi della console. CloudFront

Quando si crea un allarme nella console, si specificano i seguenti valori:

Parametro

La metrica per la quale si sta creando l'allarme.

Distribuzione

La CloudFront distribuzione per la quale stai creando l'allarme.

Name of alarm (Nome allarme)

Un nome per l'allarme.

Invia una notifica a

L'Argomento Amazon SNS a cui inviare una notifica se questa metrica attiva un avviso.

Whenever ***<metric> <operator> <value>***

Specificate 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:

Ogni volta: media di 5 xxErrorRate **>** **1**

Nota quanto segue sulla specifica di valori:

- Inserisci solo 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.

For at least ***<number>*** consecutive periods of ***<time period>***

Specificate per quanti periodi di tempo consecutivi della durata specificata la metrica deve soddisfare i criteri prima di CloudWatch attivare un allarme. Quando si sceglie un valore, puntare a un giusto equilibrio tra un valore che non allarmi per problemi temporanei o fugaci, ma allarmi per problemi sostenuti o reali.

Download di parametri in formato CSV

Puoi scaricare i dati delle CloudWatch metriche per una CloudFront distribuzione in formato CSV. Puoi scaricare i dati quando visualizzi le metriche di distribuzione per una particolare distribuzione nella console. CloudFront

Informazioni sul report

Le prime righe del report includono le seguenti informazioni:

Versione

La versione CloudFront di report.

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.

4 ottobre xxErrorRate

La percentuale di richieste per le quali il codice di stato HTTP era un errore `4xx` per la distribuzione specificata durante l'intervallo temporale.

5 xxErrorRate Pct

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:

401 ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `401` per la distribuzione specificata durante l'intervallo temporale.

403 ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `403` per la distribuzione specificata durante l'intervallo temporale.

404 ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `404` per la distribuzione specificata durante l'intervallo temporale.

502 ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `502` per la distribuzione specificata durante l'intervallo temporale.

503 ErrorRatePct

La percentuale di richieste per le quali il codice di stato HTTP era un errore `503` per la distribuzione specificata durante l'intervallo temporale.

504 ErrorRatePct

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 impiegato, 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 Questa è anche nota come latenza del primo byte, o. time-to-first-byte

CacheHitRate

La percentuale di tutte le richieste memorizzabili nella cache che hanno fornito il CloudFront contenuto della cache. Le richieste HTTP `POST` e `PUT` e gli errori non sono considerati memorizzabili nella cache.

Ottenere le metriche utilizzando l'API CloudWatch

Puoi utilizzare l' CloudWatch API o la CLI di Amazon per ottenere i CloudFront parametri nei programmi o nelle applicazioni che crei. È possibile utilizzare i dati grezzi per creare dashboard personalizzati, strumenti di avviso e così via.

Per ottenere i CloudFront parametri dall' CloudWatch API, devi utilizzare la regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1` È inoltre necessario conoscere determinati valori e tipi per ogni parametro.

Argomenti

- Valori per tutte le metriche CloudFront
- Valori per le metriche di distribuzione CloudFront
- Valori per le metriche CloudFront delle funzioni

Valori per tutte le metriche CloudFront

I seguenti valori si applicano a tutte le CloudFront metriche:

`Namespace`

Il valore per `Namespace` è sempre `AWS/CloudFront`.

Dimensioni

Ogni CloudFront metrica ha le due dimensioni seguenti:

`DistributionId`

L'ID della CloudFront distribuzione per la quale desideri ottenere le metriche.

`FunctionName`

Il nome della funzione (in CloudFront Funzioni) per la quale desideri ottenere le metriche.

Questa dimensione si applica solo alle funzioni.

`Region`

Il valore per `Region` è sempre`Global`, perché CloudFront è un servizio globale.

> **Note**
>
> Per ottenere le CloudFront metriche dall' CloudWatch API, devi utilizzare la regione Stati Uniti orientali (Virginia settentrionale) (us-east-1).

Valori per le metriche di distribuzione CloudFront

Utilizza le informazioni del seguente elenco per ottenere dettagli su metriche di CloudFront distribuzione specifiche dall' CloudWatch API. 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 di byte scaricati dai visualizzatori per le richieste `GET`, `HEAD` e `OPTIONS`.

- Nome parametro: `BytesDownloaded`
- Statistiche valide:: `Sum`
- Unità: `None`

Byte caricati

Il numero totale di byte con cui gli spettatori hanno caricatoCloudFront, utilizzato `POST` e richiesto sulla tua pagina di origine. `PUT`

- Nome parametro: `BytesUploaded`
- Statistiche valide:: `Sum`
- Unità: `None`

Percentuale di riscontri nella cache

La percentuale di tutte le richieste memorizzabili nella cache per le quali è CloudFront stato fornito il contenuto della 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 impiegato, 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 Questa è anche nota come latenza del 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 `Percentile` statistica dall' CloudWatch API, usa il `ExtendedStatistics` parametro, not. `Statistics` Per ulteriori informazioni, GetMetricStatisticsconsulta Amazon CloudWatch API Reference o la documentazione di riferimento per gli AWS SDK.

Richieste

Il numero totale di richieste di visualizzatori ricevute da CloudFront, per tutti i metodi HTTP e per entrambe 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 le metriche CloudFront delle funzioni

Utilizza le informazioni del seguente elenco per ottenere dettagli sulle metriche di CloudFront funzioni specifiche dall' CloudWatch API.

> **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`

Throttles

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. È anche possibile ottenere i registri delle funzioni di edge computing.

Richieste di registrazione

CloudFront offre i seguenti modi per registrare le richieste che arrivano alle tue distribuzioni.

Registri standard (registri di accesso)

CloudFront i registri standard forniscono registrazioni dettagliate su ogni richiesta effettuata a una distribuzione. Questi registri sono utili per molti scenari, tra cui controlli di sicurezza e accesso.

CloudFront i log standard vengono inviati al bucket Amazon S3 di tua scelta. CloudFrontnon prevede costi per i log standard, tuttavia sono previsti costi di Amazon S3 per l'archiviazione e l'accesso ai file di registro.

Per ulteriori informazioni, consulta Utilizzo dei registri standard (log di accesso).

Registri in tempo reale

CloudFront i log in tempo reale forniscono informazioni sulle richieste fatte a una distribuzione, in tempo reale (i record di log vengono consegnati entro pochi secondi dalla ricezione delle richieste). Puoi scegliere la frequenza di campionamento per i log in tempo reale, ossia la percentuale di richieste per cui desideri ricevere log in tempo reale. Puoi anche scegliere i campi specifici che desideri siano riportati nei record di log.

CloudFront i log in tempo reale vengono inviati al flusso di dati di tua scelta in Amazon Kinesis Data Streams. CloudFront addebiti per i log in tempo reale, oltre ai costi sostenuti per l'utilizzo di Kinesis Data Streams.

Per ulteriori informazioni, consulta Registri in tempo reale.

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 delle chiamate CloudFront API Amazon tramite AWS CloudTrail.

Argomenti

- Configurazione e utilizzo di registri standard (registri di accesso)
- Registri in tempo reale
- Registri delle funzioni Edge
- Registrazione delle chiamate CloudFront API Amazon tramite AWS CloudTrail

Configurazione e utilizzo di registri standard (registri di accesso)

È possibile CloudFront configurare la creazione di file di registro che contengono informazioni dettagliate su ogni richiesta utente CloudFront ricevuta. Questi sono detti registri standard, noti anche come registri di accesso. Se abiliti i log standard, puoi anche specificare il bucket Amazon S3 in cui CloudFront vuoi salvare i file.

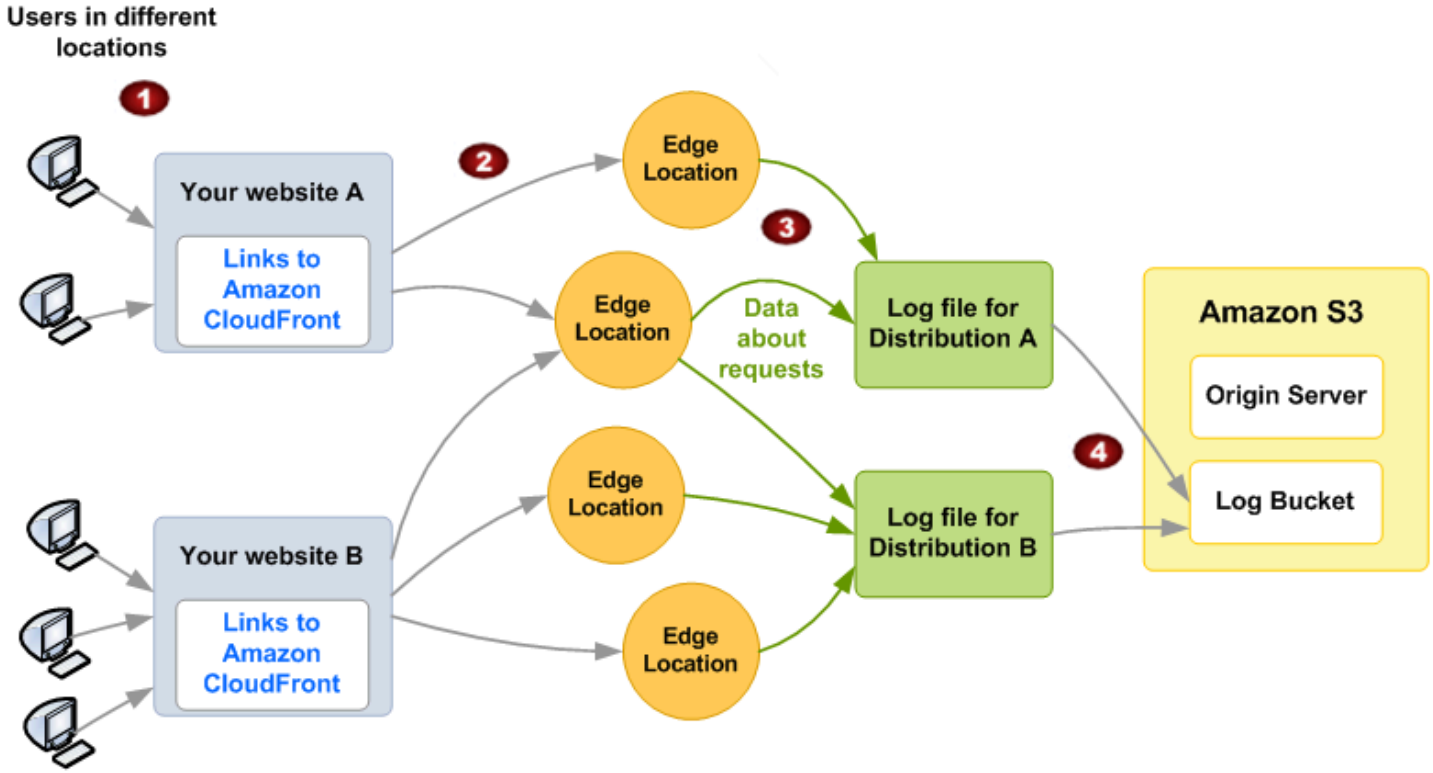
È possibile abilitare i registri standard quando si crea o si aggiorna una distribuzione. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.

CloudFront offre anche log in tempo reale, che forniscono 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 registri in tempo reale per monitorare, analizzare e agire in base alle prestazioni di distribuzione dei contenuti. Per ulteriori informazioni, consulta Registri in tempo reale.

Argomenti

Come funziona la registrazione standard

Il diagramma seguente mostra come CloudFront registra le informazioni sulle richieste relative agli oggetti.



Di seguito viene illustrato come vengono CloudFront registrate le informazioni sulle richieste relative agli oggetti, come illustrato nel diagramma precedente.

1. In questo diagramma sono presenti due siti Web, A e B, e due distribuzioni corrispondenti. CloudFront Gli utenti richiedono i tuoi oggetti utilizzando gli URL associati alle distribuzioni.
2. CloudFront indirizza ogni richiesta verso la posizione periferica 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 e le informazioni sulle richieste relative alla distribuzione B sono registrate in un file di log riservato alla 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 nessun utente accede al tuo contenuto durante una determinata ora, non ricevi alcun file di log per quell'ora.

Ogni voce in un file di log fornisce informazioni dettagliate su una singola richiesta. Per ulteriori informazioni sul formato dei file di log, consulta Formato file registro standard.

> **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 registri di accesso non corrisponderà all'utilizzo visualizzato nei report di fatturazione e utilizzo. AWS

Scelta di un bucket Amazon S3 per i log standard

Quando abiliti la registrazione per una distribuzione, specifichi il bucket Amazon S3 in cui CloudFront desideri archiviare i file di registro. Se si utilizza Amazon S3 come origine, consigliamo di non utilizzare lo stesso bucket per i file di log; l'utilizzo di un bucket separato semplifica la manutenzione.

> **Important**
>
> 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, CloudFront impedendo così la consegna dei file di log al bucket.

> **Important**
>
> Non scegliere un bucket Amazon S3 in nessuna delle seguenti regioni, perché CloudFront non fornisce 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)

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.

Autorizzazioni richieste per configurare la registrazione standard e per accedere ai file di log

Important

A partire da aprile 2023, dovrai abilitare le liste di controllo degli accessi (ACL) S3 per i nuovi bucket S3 utilizzati per i log standard. CloudFront Gli ACL possono essere abilitati durante le fasi di creazione del bucket o dopo che un bucket è stato creato.
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.

Il tuo AWS account deve disporre delle seguenti autorizzazioni per il bucket specificato per i file di registro:

- La Access Control List (ACL) S3 per il bucket deve concederti 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`

Tieni presente quanto segue:

ACL per il bucket

Quando crei o aggiorni una distribuzione e abiliti la registrazione, CloudFront utilizza queste autorizzazioni per aggiornare l'ACL del bucket e concedere l'autorizzazione all'account. `awslogsdelivery` `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 i log di accesso in un bucket S3 e non riesci più a ricevere i log in quel bucket, controlla le autorizzazioni sul bucket per assicurarti che disponga delle autorizzazioni necessarie. CloudFront

Ripristino dell'ACL per il bucket

Se rimuovi le autorizzazioni per l'`awslogsdelivery`account, CloudFront non potrai salvare i log nel bucket S3. Per consentire di CloudFront ricominciare a salvare i log per la tua distribuzione, ripristina l'autorizzazione ACL effettuando una delle seguenti operazioni:

- Disabilita la registrazione per la tua distribuzione CloudFront, quindi abilitala nuovamente. Per ulteriori informazioni, consulta Riferimento alle impostazioni di distribuzione.
- 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 S3 bucket, consulta Come impostare le autorizzazioni del bucket ACL? nella Guida per l'utente di Amazon Simple Storage Service.

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 disabiliti la registrazione, CloudFront non elimina gli ACL né per il bucket né per i file di registro. Se lo desideri, puoi eseguire questa operazione manualmente.

Policy chiave necessarie per i bucket SSE/KMS

Se il S3 bucket 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 per la chiave gestita dal cliente. Ciò consente di CloudFront scrivere file di registro nel bucket. (Non è possibile utilizzare SSE-KMS con il Chiave gestita da AWS perché CloudFront non sarà possibile scrivere file di registro 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 S3 bucket per i log standard utilizza SSE-KMS con una chiave di S3 bucket, è necessario anche aggiungere l'autorizzazione `kms:Decrypt` all'istruzione della 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": "*"
}
```

Formato del nome file

Il nome di ogni file di registro CloudFront salvato nel bucket Amazon S3 utilizza il seguente formato di nome 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 includi un valore per il prefisso del file di registro e il prefisso non termina con una barra (`/`), ne aggiunge una automaticamente. CloudFront Se il prefisso termina con una barra, CloudFront non ne aggiunge un'altra.

La `.gz` fine del nome del file indica che il file di registro CloudFront è stato compresso utilizzando gzip.

Tempi di recapito dei file di registro standard

CloudFront fornisce log standard 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 di solito consegna il file di log per quel periodo di tempo al tuo bucket Amazon S3 entro un'ora dagli eventi che appaiono nel log. 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 immissioni 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.

CloudFront offre anche registri 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 registri in tempo reale per monitorare, analizzare e agire in base alle prestazioni di distribuzione dei contenuti. Per ulteriori informazioni, consulta Registri in tempo reale.

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 gli 8192 byte, non è possibile analizzare completamente la richiesta e non è CloudFront possibile registrarla. 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.

Analisi dei log standard

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 del AWS blog illustrano alcuni modi per analizzare i log di accesso.

- Amazon CloudFront Request Logging (per contenuti forniti tramite HTTP)
- Log CloudFront ottimizzati, ora con stringhe di query

> **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 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 registri di accesso non corrisponderà all'utilizzo visualizzato nei rapporti di utilizzo e fatturazione AWS .

Modifica delle impostazioni di registrazione standard

Puoi abilitare o disabilitare la registrazione, modificare il bucket Amazon S3 in cui sono archiviati i log e modificare il prefisso per i file di registro utilizzando CloudFront la console o l'API. CloudFront 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 console, consulta. CloudFront Aggiornamento di una distribuzione
- Per aggiornare una distribuzione utilizzando l' CloudFront API, UpdateDistributionconsulta Amazon CloudFront API Reference.

Eliminazione di file di log standard da un bucket Amazon S3

CloudFront non elimina automaticamente i file di registro dal bucket Amazon S3. Per informazioni sull'eliminazione dei file di log da un bucket Amazon S3, consulta i seguenti argomenti:

- Utilizzo della console Amazon S3: Eliminazione degli oggetti nella Guida per l'utente di Amazon Simple Storage Service Console.
- Utilizzo dell'API REST: DeleteObjectnel riferimento all'API di Amazon Simple Storage Service.

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	%
%7B	{
%7D	}
%7C	|
%5C	\
%5E	^
%7E	~
%5B	[
%5D	]
%60	`
%27	'

Valore con codifica URL	Carattere
%20	spazio

Campi del file di registro standard

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 in cui la connessione è stata chiusa.

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, questa è l'ora in cui la connessione viene chiusa.

3. **`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).

4. **`sc-bytes`**

   Il numero totale di byte che il server ha inviato al visualizzatore in risposta alla richiesta, incluse le intestazioni. Per WebSocket le connessioni, si tratta del 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 di domanda (?) in URL e stringhe di query non sono inclusi nel log.

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 Contenuto della cache in base ai parametri della stringa 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 Contenuto della cache basato sui 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 le connessioni avranno un valore di `Miss` per questo campo perché il contenuto non è memorizzabile nella cache e viene inviato 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 respinta 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.

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 negli URL degli oggetti (come d111111abcdef8.cloudfront.net), questo campo contiene quel nome di dominio. Se si utilizzano nomi di dominio alternativi (CNAME) negli URL di oggetti, ad esempio http://example.com, il campo contiene il nome di dominio 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`, `ws` o `wss`).

18 **`cs-bytes`**

Numero totale di byte di dati che il visualizzatore ha incluso nella richiesta, incluse le intestazioni. Per le WebSocket connessioni, questo è il numero totale di byte inviati dal client al server tramite la 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 indirizzo IPv4 (ad esempio,`192.0.2.183`) o un indirizzo IPv6 (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 ha utilizzato HTTPS, questo campo contiene il protocollo SSL/TLS negoziato dal visualizzatore e dal server per la trasmissione della richiesta e della risposta. Per un elenco dei valori possibili, vedere i protocolli SSL/TLS 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 ha utilizzato HTTPS, questo campo contiene la crittografia SSL/TLS che il visualizzatore e il server hanno negoziato per crittografare la richiesta e la risposta. Per un elenco dei valori possibili, vedere le crittografie SSL/TLS supportate 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 (-).

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 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.

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 certificato SSL/TLS in base al 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.

Di seguito è riportato un esempio di file di registro 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 - -
```

Addebiti per registri standard

La registrazione standard è una funzionalità opzionale di. CloudFront L'attivazione di questa registrazione standard non comporta costi aggiuntivi. 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 CloudFront prezzi, consulta la sezione CloudFront Prezzi.

Registri in tempo reale

Con i log 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 registri in tempo reale per monitorare, analizzare e agire in base alle prestazioni di distribuzione dei contenuti.

CloudFront i log in tempo reale sono configurabili. È possibile scegliere:

- Puoi scegliere la frequenza di campionamento per i log in tempo reale, ossia la percentuale di richieste per cui desideri ricevere log 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 in tempo reale vengono inviati 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 addebiti per i log 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 relative ai tuoi contenuti, non come contabilità completa di tutte le richieste. CloudFront fornisce log in tempo reale 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

in tempo reale, il numero di voci nei registri in tempo reale non corrisponderà all'utilizzo visualizzato nei report di fatturazione e utilizzo. AWS

Informazioni sulle configurazioni dei log in tempo reale

Per utilizzare i log CloudFront in tempo reale, iniziate con la creazione di una configurazione dei log in tempo reale. La configurazione del registro in tempo reale contiene informazioni sui campi di registro che si desidera ricevere, la frequenza di campionamento per i record di registro e il flusso di dati Kinesis in cui si desidera consegnare i registri.

In particolare, una configurazione di registro in tempo reale contiene le seguenti impostazioni:

- Nome
- Velocità di campionamento
- Campi
- Endpoint (flusso di dati Kinesis)
- Ruolo IAM

Nome

Un nome per identificare la configurazione del registro in tempo reale.

Velocità di campionamento

La frequenza di campionamento è un numero intero compreso tra 1 e 100 (incluso) che determina la percentuale di richieste di visualizzatore inviate a Kinesis Data Streams come record di registro in tempo reale. Per includere ogni richiesta di visualizzatore nei registri in tempo reale, specificare 100 per la frequenza di campionamento. È possibile scegliere una frequenza di campionamento inferiore per ridurre i costi pur ricevendo un campione rappresentativo di dati di richiesta nei registri in tempo reale.

Campi

Un elenco di campi inclusi in ogni record di log 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) che i client dei lettori multimediali possono inviare alle CDN a ogni richiesta. È possibile utilizzare questi dati per comprendere ogni richiesta, ad esempio il tipo di file multimediale (audio, video), la velocità di riproduzione e la durata dello streaming. Questi campi verranno visualizzati nei registri 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. **`time-to-first-byte`**

   Il numero di secondi tra la ricezione della richiesta e la scrittura del primo byte della risposta, misurato sul server.

4. **`sc-status`**

   Il codice di stato HTTP della risposta del server (ad esempio, `200`).

5. **`sc-bytes`**

   Il numero totale di byte che il server ha inviato al visualizzatore in risposta alla richiesta, incluse le intestazioni. Per WebSocket le connessioni, si tratta del numero totale di byte inviati dal server al client tramite la connessione.

6. **`cs-method`**

   Il metodo di richiesta HTTP ricevuto dal visualizzatore.

7. **`cs-protocol`**

   Protocollo della richiesta del visualizzatore (`http`, `https`, `ws` o `wss`).

8. **`cs-host`**

   Il valore che il visualizzatore ha incluso nell'intestazione `Host` per questa richiesta. Se utilizzi il nome di CloudFront dominio negli URL degli oggetti (ad esempio d111111abcdef8.cloudfront.net), questo campo contiene quel nome di dominio. Se si utilizzano nomi di dominio alternativi (CNAME) negli URL di oggetti, ad esempio http://example.com, il campo contiene il nome di dominio alternativo.

9. **`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.

10. **`cs-bytes`**

    Numero totale di byte di dati che il visualizzatore ha incluso nella richiesta, incluse le intestazioni. Per le WebSocket connessioni, questo è il numero totale di byte inviati dal client al server tramite la connessione.

11. **`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).

12. **`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.

13. **`x-host-header`**

    Il nome di dominio della CloudFront distribuzione (ad esempio, d111111abcdef8.cloudfront.net).

14. **`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.

15 **`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`.

16 **`c-ip-version`**

La versione IP della richiesta (IPv4 o IPv6).

17 **`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.

18 **`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.

19 **`cs-cookie`**

L'intestazione `Cookie` nella richiesta, incluse le coppie nome-valore e gli attributi associati.

> **Note**
>
> Questo campo viene troncato a 800 byte.

20 **`cs-uri-query`**

L'eventuale parte della stringa di query nell'URL.

21 **`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.

22**`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 indirizzo IPv4 (ad esempio,`192.0.2.183`) o un indirizzo IPv6 (ad esempio,). `2001:0db8:85a3::8a2e:0370:7334`

23**`ssl-protocol`**

Quando la richiesta ha utilizzato HTTPS, questo campo contiene il protocollo SSL/TLS negoziato dal visualizzatore e dal server per la trasmissione della richiesta e della risposta. Per un elenco dei valori possibili, vedere i protocolli SSL/TLS supportati in Protocolli e cifrari supportati tra visualizzatori e CloudFront.

24**`ssl-cipher`**

Quando la richiesta ha utilizzato HTTPS, questo campo contiene la crittografia SSL/TLS che il visualizzatore e il server hanno negoziato per crittografare la richiesta e la risposta. Per un elenco

dei valori possibili, vedere le crittografie SSL/TLS supportate in Protocolli e cifrari supportati tra visualizzatori e CloudFront.

25 **`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 le connessioni avranno un valore di `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 respinta 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.

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`

27. **`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.

28 **`sc-content-type`**

Il valore dell'intestazione HTTP `Content-Type` della risposta.

29 **`sc-content-len`**

Il valore dell'intestazione HTTP `Content-Length` della risposta.

30 **`sc-range-start`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore iniziale dell'intervallo.

31 **`sc-range-end`**

Quando la risposta contiene l'intestazione HTTP `Content-Range`, questo campo contiene il valore finale dell'intervallo.

32 **`c-port`**

Il numero di porta della richiesta del visualizzatore.

33 **`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 certificato SSL/TLS in base al 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.

34 **`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.

35 **`cs-accept-encoding`**

Il valore dell'intestazione `Accept-Encoding` nella richiesta del visualizzatore.

36 **`cs-accept`**

Il valore dell'intestazione `Accept` nella richiesta del visualizzatore.

37 **`cache-behavior-path-pattern`**

Il modello di percorso che identifica il comportamento della cache corrispondente alla richiesta del visualizzatore.

38 **`cs-headers`**

Le intestazioni HTTP (nomi e valori) nella richiesta del visualizzatore.

> **Note**
>
> Questo campo viene troncato a 800 byte.

39 **`cs-header-names`**

I nomi delle intestazioni HTTP (non dei valori) nella richiesta del visualizzatore.

> **Note**
>
> Questo campo viene troncato a 800 byte.

40 **`cs-headers-count`**

Il numero di intestazioni HTTP nella richiesta del visualizzatore.

41 **`origin-fbl`**

Il numero di secondi di latenza del primo byte tra e CloudFront l'origine.

42 **`origin-lbl`**

Il numero di secondi di latenza dell'ultimo byte tra e l'origine. CloudFront

43 **`asn`**

Il numero di sistema autonomo (ASN) del visualizzatore.

44 **`primary-distribution-id`**

Quando la distribuzione continua è abilitata, questo ID identifica quale distribuzione è la principale nella distribuzione corrente.

45 **`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).

> **Campi CMCD nei log in tempo reale**
>
> Per ulteriori informazioni su questi campi, consultate il documento CTA Specification Web Application Video Ecosystem - Common Media Client Data CTA-5004.

46 **`cmcd-encoded-bitrate`**

Il bitrate codificato dell'oggetto audio o video richiesto.

47 **`cmcd-buffer-length`**

La lunghezza del buffer dell'oggetto multimediale richiesto.

48 **`cmcd-buffer-starvation`**

Se il buffer si è esaurito a un certo punto tra la richiesta precedente e la richiesta dell'oggetto. Ciò può far sì che il player si trovi in una statistica di rebuffering, che può bloccare la riproduzione di video o audio.

49 **`cmcd-content-id`**

Una stringa univoca che identifica il contenuto corrente.

50. **`cmcd-object-duration`**

    La durata di riproduzione dell'oggetto richiesto (in millisecondi).

51. **`cmcd-deadline`**

    Scadenza dal momento della richiesta entro cui deve essere disponibile il primo campione di questo oggetto, in modo da evitare uno stato di esecuzione insufficiente del buffer o altri problemi di riproduzione.

52. **`cmcd-measured-throughput`**

    La velocità effettiva tra client e server, misurata dal client.

53. **`cmcd-next-object-request`**

    Il percorso relativo del successivo oggetto richiesto.

54. **`cmcd-next-range-request`**

    Se la richiesta successiva è una richiesta parziale di oggetto, questa stringa indica l'intervallo di byte da richiedere.

55. **`cmcd-object-type`**

    Il tipo di supporto dell'oggetto corrente richiesto.

56. **`cmcd-playback-rate`**

    1 se in tempo reale, 2 se a doppia velocità, 0 se non è in riproduzione.

57. **`cmcd-requested-maximum-throughput`**

    Il throughput massimo richiesto che il cliente ritiene sufficiente per la consegna degli asset.

58. **`cmcd-streaming-format`**

    Il formato di streaming che definisce la richiesta corrente.

59. **`cmcd-session-id`**

    Un GUID che identifica la sessione di riproduzione corrente.

60. **`cmcd-stream-type`**

    Token che identifica la disponibilità del segmento. `v`= tutti i segmenti sono disponibili. `l`= i segmenti diventano disponibili nel tempo.

61. **`cmcd-startup`**

La chiave viene inclusa senza un valore se l'oggetto è necessario urgentemente durante l'avvio, la ricerca o il ripristino dopo un evento di vuotamento del buffer.

62. **`cmcd-top-bitrate`**

    La resa in bitrate più elevata che il client può riprodurre.

63. **`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.

Endpoint (flusso di dati Kinesis)

L'endpoint contiene informazioni sul flusso di dati Kinesis in cui si desidera inviare registri in tempo reale. Fornisci il Amazon Resource Name (ARN) del flusso di dati.

Per ulteriori informazioni sulla creazione di un flusso di dati Kinesis, consulta i seguenti argomenti nella Guida per gli sviluppatori di Amazon Kinesis Data Streams.

- Gestione dei flussi utilizzando la console
- Esegui le operazioni di base di Kinesis Data Stream utilizzando AWS CLI
- Creazione di uno stream (utilizza il AWS SDK for 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 tua CloudFront distribuzione.

   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 log in tempo reale.

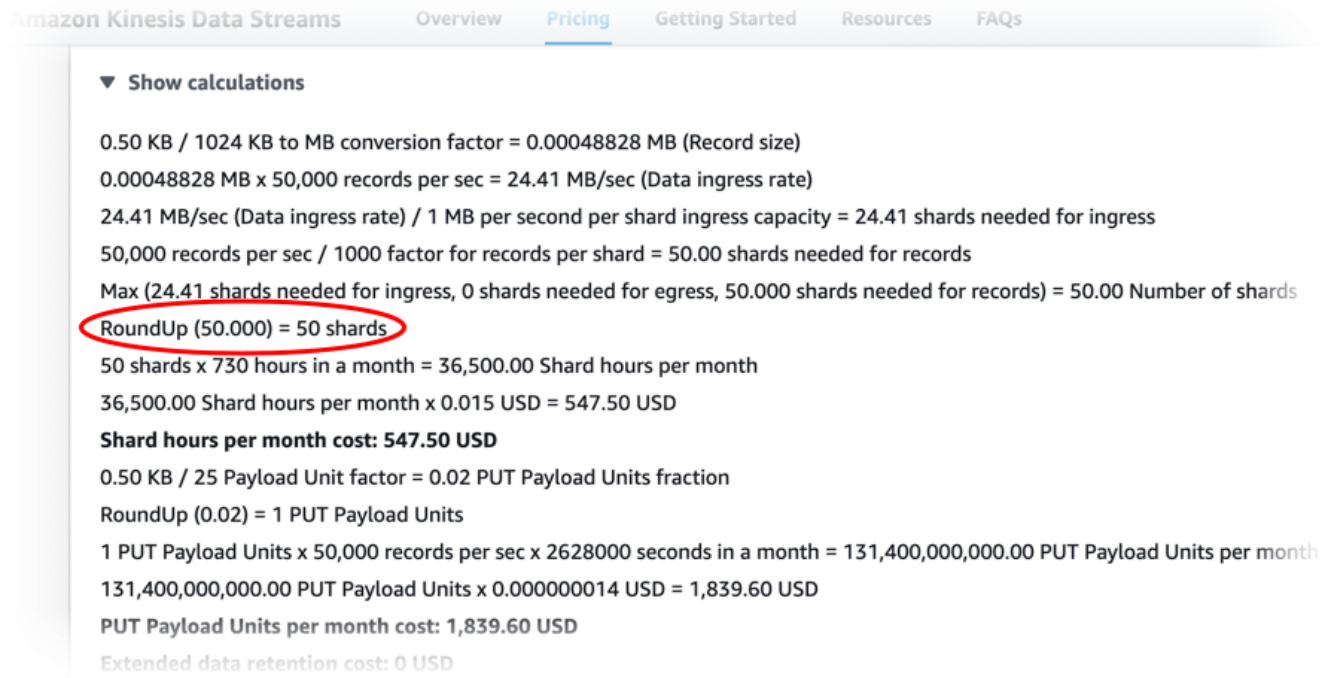
   In generale, un singolo record di log è di circa 500 byte. Un record di grandi dimensioni che include tutti i campi disponibili è generalmente di circa 1 KB.

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. Nel Calcolatore prezzi nella pagina dei prezzi Amazon Kinesis Data Streams, inserisci il numero di richieste (record) al secondo e la dimensione media del record di un singolo record di log. Quindi scegli Show calculations (Mostra calcoli).

   Il calcolatore prezzi mostra il numero di shard di cui hai bisogno. (Mostra anche il costo stimato.)

   Nell'esempio seguente viene illustrato che per una dimensione media di record di 0,5 KB e 50.000 richieste al secondo, sono necessari 50 shard.



Ruolo IAM

Il ruolo AWS Identity and Access Management (IAM) che consente CloudFront di fornire log in tempo reale al flusso di dati Kinesis.

Quando crei una configurazione di log 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 di log in tempo reale con AWS CloudFormation o l' CloudFrontAPI (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 attendibilità del ruolo IAM, sostituire *111122223333* con il numero Account AWS . L'`Condition`elemento di questa policy aiuta a prevenire il confuso problema del vicesceriffo perché CloudFront può assumere questo ruolo solo per conto di una distribuzione del proprio territorio. Account AWS

```
{
    "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 policy, sostituisci *arn:aws:kinesis:us-east-2:123456789012:stream/ con l'ARN del tuo flusso di dati Kinesis*. StreamName

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

```
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        }
    ]
}
```

Policy di autorizzazioni del ruolo IAM per un flusso di dati crittografato

Per utilizzare la seguente policy, sostituisci arn:aws:kinesis:us-east- 2:123456789012:stream/ con l'ARN del tuo flusso di dati Kinesis e arn:aws:kms:us-east- StreamName 2:123456789012:key/e58a3d0b-fe4f-4047-a495-ae03cc73d486 con l'ARN del tuo. AWS KMS key

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-
ae03cc73d486"
            ]
```

```
        }
    ]
}
```

Creazione e utilizzo di configurazioni di log in tempo reale

È possibile utilizzare una configurazione di registro in tempo reale per ottenere informazioni sulle richieste effettuate a una distribuzione in tempo reale (i registri vengono consegnati entro pochi secondi dalla ricezione delle richieste). Puoi creare una configurazione di log in tempo reale nella CloudFront console, con AWS Command Line Interface (AWS CLI) o con l' CloudFront API.

Per utilizzare una configurazione di registro in tempo reale, è necessario collegarla a uno o più comportamenti della cache in una CloudFront distribuzione.

Creare una configurazione di log in tempo reale (console)

Per creare una configurazione di log in tempo reale

1. Accedi AWS Management Console 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. In Nome, inserisci un nome per la configurazione.
5. Per Frequenza di campionamento, inserite la percentuale di richieste per le quali desiderate ricevere i record di registro.
6. Per Fields, scegliete i campi da ricevere nei log in tempo reale.
   - Per includere tutti i campi CMCD per i tuoi registri, scegli CMCD tutte le chiavi.
7. Per Endpoint, scegli uno o più flussi di dati Kinesis per ricevere i log in tempo reale.

> **Note**
>
> CloudFront i log in tempo reale vengono inviati al flusso di dati specificato in Kinesis Data Streams. Per leggere e analizzare i log 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 il ruolo IAM, scegli Crea nuovo ruolo di servizio o scegli 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 collegare alla configurazione del registro in tempo reale.
10. Scegli Crea configurazione.

In caso di successo, la console mostra i dettagli della configurazione del registro in tempo reale appena creata.

Per ulteriori informazioni, consulta Informazioni sulle configurazioni dei log in tempo reale.

Configurazione del log in tempo reale (AWS CLI)

Per creare una configurazione di log in tempo reale con AWS Command Line Interface (AWS CLI), utilizzate 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 di log 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. Modificare il file per specificare le impostazioni di configurazione del registro in tempo reale desiderate, quindi salvare il file. Tieni 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 Informazioni sulle configurazioni dei log in tempo reale.
3. Utilizzare il comando seguente per creare la configurazione del registro in tempo reale utilizzando i parametri di input dal file `rtl-config.yaml`.

```
aws cloudfront create-realtime-log-config --cli-input-yaml file://rtl-config.yaml
```

In caso di esito positivo, l'output del comando mostra i dettagli della configurazione del log in tempo reale appena creata.

Per collegare una configurazione di log in tempo reale a una distribuzione esistente (CLI con file di input)

1. Utilizzate il comando seguente per salvare la configurazione di CloudFront distribuzione per la distribuzione che desiderate 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 configurazione di registro in tempo reale.

   - Nel comportamento della cache, aggiungere un campo denominato `RealtimeLogConfigArn`. Per il valore del campo, utilizzare l'ARN della configurazione del log in tempo reale che si desidera collegare a questo 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 configurazione del registro in tempo reale. Sostituire *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.

Creare una configurazione di log in tempo reale (API)

Per creare una configurazione di log in tempo reale con l' CloudFront API, usa CreateRealtimeLogConfig. Per ulteriori informazioni sui parametri specificati in questa chiamata API, consulta Informazioni sulle configurazioni dei log in tempo reale la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Dopo aver creato una configurazione di registro in tempo reale, è possibile collegarla a un comportamento della cache, utilizzando una delle seguenti chiamate 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 chiamate API, fornire l'ARN della configurazione del registro in tempo reale nel campo `RealtimeLogConfigArn`, all'interno di un comportamento della cache. Per ulteriori informazioni sugli altri campi specificati in queste chiamate API, consulta Riferimento alle impostazioni di distribuzione la documentazione di riferimento sull'API per il tuo AWS SDK o altro client API.

Creazione di consumer Kinesis Data Streams

Per leggere e analizzare i log in tempo reale, si crea o si utilizza 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 in tempo reale vengono sempre consegnati nello stesso ordine, come indicato nella Campi sezione. Assicurati di creare il tuo consumatore per soddisfare questo ordine fisso.

Ad esempio, si consideri una configurazione di registro in tempo reale che include solo i tre campi seguenti: `time-to-first-byte`, `sc-status` e `c-country`. In questo scenario, l'ultimo campo, `c-country`, è sempre il numero di campo 3 in ogni record di registro. Tuttavia, se successivamente si aggiungono campi alla configurazione del registro in tempo reale, il posizionamento di ciascun campo in un record può cambiare.

Ad esempio, se si aggiungono i campi `sc-bytes` e `time-taken` alla configurazione del registro in tempo reale, questi campi vengono inseriti in ogni record di registro in base all'ordine mostrato nella sezione Campi. 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. Assicurarsi che l'applicazione consumer sia in grado di gestire i campi che cambiano posizione in un record di registro, nel caso in cui si aggiungono campi alla configurazione del registro in tempo reale.

Risoluzione dei problemi di log in tempo

Dopo aver creato una configurazione di log in tempo reale, è possibile che non vengano recapitati record (o non tutti i record) a Kinesis Data Streams. In questo caso, devi prima verificare che la tua CloudFront distribuzione riceva le richieste degli spettatori. In tal caso, è possibile controllare le seguenti impostazioni per continuare la risoluzione dei problemi.

Autorizzazioni del ruolo IAM

Per fornire record di log in tempo reale al flusso di dati Kinesis, CloudFront utilizza il ruolo IAM nella configurazione dei log 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 record di log in tempo reale nel 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 Accedi 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 .

Registri di Lambda@Edge

Lambda @Edge invia automaticamente i log delle funzioni ai CloudWatch registri, creando flussi di log nel luogo in Regioni AWS cui vengono eseguite le funzioni. Il nome del gruppo di log è formattato come`/aws/lambda/us-east-1.`*`function-name`*: dove *`function-name`* è il nome che hai dato alla funzione quando l'hai creata ed `us-east-1` è il codice regionale del Regione AWS luogo in cui è stata creata la funzione. Il nome del gruppo di log contiene sempre`us-east-1`, anche per i gruppi di log di altre regioni in cui viene eseguita la funzione.

> **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 forma corretta Regione AWS 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 AWS. 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 quanto segue:

- Per ulteriori informazioni sulla visualizzazione dei grafici nella sezione Monitoraggio della CloudFront console, consulta. the section called “Monitoraggio delle CloudFront metriche con Amazon CloudWatch”
- Per informazioni sulle autorizzazioni necessarie per inviare dati ai CloudWatch registri, vedere. the section called “Configura le autorizzazioni e i 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 settentrionale`us-east-1`), indipendentemente dalla posizione periferica in cui è stata eseguita la funzione. Il nome del gruppo di log è nel formato `/aws/cloudfront/function/`*`FunctionName`* dove *`FunctionName`* è il nome assegnato alla funzione al momento della creazione. Il nome del flusso di log è nel formato `YYYY/M/D/`*`UUID`*.

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
```

> **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 dell'account. CloudWatch Un ruolo collegato al servizio è un ruolo IAM collegato direttamente a un servizio. AWS I ruoli collegati ai servizi sono predefiniti dal servizio e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS CloudFront Functions utilizza un ruolo collegato al servizio chiamato. 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 CloudFront log in tempo reale. Le informazioni sull'errore vengono registrate nei campi `x-edge-result-type`, `x-edge-response-result-type` e `x-edge-detailed-result-type`.

Registrazione delle chiamate CloudFront API Amazon tramite AWS CloudTrail

CloudFront è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API CloudFront come eventi. Le chiamate acquisite includono chiamate dalla CloudFront console e chiamate di codice alle operazioni CloudFront API. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata effettuata CloudFront, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori 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 IAM Identity Center.
- 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 Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un percorso a

regione singola o multiregione utilizzando. AWS CLI La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio account Regioni AWS . Se crei un percorso a regione singola, puoi visualizzare solo gli eventi registrati nel percorso. Regione AWS Per ulteriori informazioni sui percorsi, consulta Creazione di un percorso per te Account AWS e Creazione di un percorso per un'organizzazione nella Guida per l'AWS CloudTrail utente.

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi 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 CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei 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 ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

> **Note**
>
> CloudFront è un servizio globale. CloudTrail registra gli eventi CloudFront nella regione degli Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni, consulta Global Service events nella Guida per l'AWS CloudTrail utente.
> Se si utilizzano credenziali di sicurezza temporanee utilizzando AWS Security Token Service, le chiamate agli endpoint regionali, ad esempio`us-west-2`, vengono registrate nella regione CloudTrail appropriata.
> Per ulteriori informazioni sugli CloudFront endpoint, consulta CloudFront endpoint e quote in. Riferimenti generali di AWS

CloudFront eventi relativi ai dati in CloudTrail

Gli eventi relativi ai dati forniscono informazioni sulle operazioni eseguite sulle risorse su o all'interno di una risorsa (ad esempio, lettura o scrittura su una CloudFront distribuzione). 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 relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Puoi registrare gli eventi relativi ai dati per i tipi di CloudFront risorse utilizzando la CloudTrail console o AWS CLI le operazioni CloudTrail dell'API. Per ulteriori informazioni su come registrare gli eventi relativi ai dati, vedere Registrazione degli eventi relativi ai dati con AWS Management Console e Registrazione degli eventi relativi ai dati con the AWS Command Line Interface nella Guida per l'AWS CloudTrail utente.

La tabella seguente elenca i tipi di CloudFront risorse per i quali è possibile registrare gli eventi relativi ai dati. La colonna Data event type (console) mostra il valore da scegliere dall'elenco Data event type (console) sulla CloudTrail console. La colonna del valore resources.type mostra il `resources.type` valore da specificare durante la configurazione dei selettori di eventi avanzati utilizzando le API o. AWS CLI CloudTrail La CloudTrail colonna Data API loggate mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore resources.type	API di dati registrate su CloudTrail
CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`	• DeleteKeys • DescribeKeyValueStore • GetKey • ListKeys • PutKeys • UpdateKeys

Puoi configurare selettori di eventi avanzati per filtrare in base a `eventName`, `readOnly`, e `resources.ARN` i campi per registrare solo gli eventi che ritieni importanti. Per ulteriori informazioni su questi campi, consulta AdvancedFieldSelectorl'AWS CloudTrail API Reference.

CloudFront eventi di gestione in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'azienda 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 CloudFront del piano di controllo come eventi di gestione. Per un elenco delle operazioni del piano di CloudFront controllo di Amazon a cui si CloudFront accede CloudTrail, consulta Amazon CloudFront API Reference.

CloudFront esempi di eventi

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Indice

Esempio: UpdateDistribution

L'esempio seguente mostra un CloudTrail evento che dimostra l'UpdateDistributionoperazione.

Per le chiamate all' CloudFront API, `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"
}
```

Esempio: UpdateKeys

L'esempio seguente mostra un CloudTrail evento che dimostra l'UpdateKeysoperazione.

Per le chiamate all' CloudFront KeyValueStore API, `eventSource` is `edgekeyvaluestore.amazonaws.com` anzichécloudfront.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 dei CloudTrail record, consulta i contenuti dei CloudTrail record nella Guida AWS CloudTrail per l'utente.

Monitoraggio delle modifiche alla configurazione con AWS Config

AWS Config Utilizzalo per registrare le modifiche alla configurazione delle impostazioni CloudFront di distribuzione. Puoi acquisire le modifiche agli stati di 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 in streaming. CloudFront

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.

Per tenere traccia delle modifiche alla configurazione CloudFront della tua distribuzione, devi accedere alla CloudFront console negli Stati Uniti orientali (Virginia settentrionale) Regione AWS.

> **Note**
>
> Potrebbe verificarsi un ritardo nella registrazione delle risorse con AWS Config. AWS Config registra le risorse solo dopo averle scoperte.

Console

Da configurare AWS Config con CloudFront (console)

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
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 l' StartConfigurationRecorderazione e altre informazioni 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.

È possibile visualizzare le cronologie di configurazione nei seguenti modi.

Console

Per ogni risorsa registrata, è possibile visualizzare una pagina temporale 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'azione ListDiscoveredResources.

Per ottenere i dettagli di configurazione di una distribuzione per un intervallo di tempo specifico, usa l'azione GetResourceConfigHistory. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Config.

Sicurezza in Amazon CloudFront

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS. Per maggiori informazioni sui programmi di conformità applicabili ad Amazon CloudFront, consulta AWSServices in Scope by Compliance Program.
- Sicurezza nel cloud: la responsabilità è determinata dal servizio AWS che viene utilizzato. 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 configurare per CloudFront 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 esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog AWS Shared Responsibility Model and GDPR nel Blog sulla sicurezza AWS.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la registrazione di log sulle attività di API e utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in 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 necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

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

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 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 (POP) dell'edge location e tra altre posizioni di archiviazione utilizzate da. CloudFront

Crittografia a riposo

Il codice e la configurazione CloudFront delle funzioni in Functions vengono sempre archiviati in un formato crittografato nei POP delle edge location 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:

Usa URL o cookie firmati

Puoi limitare l'accesso ai contenuti destinati a utenti selezionati, ad esempio utenti che hanno pagato una tariffa, pubblicando questi contenuti privati tramite CloudFront URL firmati o cookie firmati. Per ulteriori informazioni, consulta Offri contenuti privati con URL firmati e cookie firmati.

Limitare l'accesso ai contenuti nei bucket Amazon S3

Se limiti l'accesso ai tuoi contenuti utilizzando, ad esempio, URL CloudFront firmati o cookie 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 “Limita l'accesso a un'origine Amazon Simple Storage Service”.

Limitare l'accesso al contenuto gestito da un Application Load Balancer

Quando utilizzi CloudFront un Application Load Balancer in Elastic Load Balancing come origine, puoi CloudFront configurare per impedire 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 Limita l'accesso agli Application Load Balancer.

Usa ACL Web AWS WAF

Puoi utilizzare AWS WAF, un servizio firewall per applicazioni Web, per creare una lista di controllo accessi Web (ACL) per restringere 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 Usa AWS WAF protezioni.

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 Limita la distribuzione geografica dei tuoi contenuti.

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

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come CloudFront funziona Amazon con IAM
- Esempi di policy basate sull'identità per Amazon CloudFront
- AWSpolitiche gestite per Amazon CloudFront
- Risoluzione dei problemi relativi all' CloudFront identità e all'accesso ad Amazon

Destinatari

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

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

Amministratore del servizio: se sei responsabile delle CloudFront risorse della tua azienda, probabilmente hai pieno accesso a CloudFront. È tuo compito determinare a quali CloudFront funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con CloudFront, consultaCome CloudFront funziona Amazon con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy a cui gestire l'accesso CloudFront. Per visualizzare esempi di policy CloudFront basate sull'identità che puoi utilizzare in IAM, 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 essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

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

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

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

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

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

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

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

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

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

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'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 ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

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

Gestione dell'accesso con policy

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

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

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

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

Policy basate su identità

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

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

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Liste di controllo degli accessi (ACL)

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

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

Altri tipi di policy

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

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

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire 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 su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	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 su identità	Sì

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

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

Esempi di 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. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste

ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per CloudFront

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni 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 a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Per visualizzare un elenco di 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 di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale 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'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di CloudFront risorse e dei relativi ARN, 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. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni

condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

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

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

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. 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

ACL in CloudFront

Supporta le ACL	No

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

ABAC con CloudFront

Supporta ABAC (tag nelle policy)	Parziale

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

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

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

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

Per ulteriori informazioni su ABAC, consulta Che cos'è 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

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

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

Sessioni di accesso diretto per CloudFront

Supports forward access sessions (FAS)	No

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

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 la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. 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 ai servizi, ma non modificarle.

Lambda @Edge utilizza ruoli collegati ai servizi per eseguire azioni al posto tuo. Per ulteriori informazioni sulla creazione o la gestione di ruoli collegati CloudFront ai servizi, 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 sono autorizzati a creare o modificare risorse. CloudFront Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Per dettagli sulle azioni e sui tipi di risorse definiti da CloudFront, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon CloudFront nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di CloudFront
- Consentire agli utenti di visualizzare le loro autorizzazioni

- Autorizzazioni per l'accesso programmatico CloudFront
- Autorizzazioni necessarie per utilizzare la console CloudFront
- AWS politiche gestite (predefinite) per CloudFront
- Esempi di policy gestite dal cliente

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 crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.

- 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, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console di CloudFront

Per accedere alla CloudFront console Amazon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle CloudFront risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

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

Per garantire che utenti e ruoli possano ancora utilizzare la CloudFront console, allega anche la policy CloudFront *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. 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.

```
{
   "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:

```
{
   "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 CloudFront console.

`cloudwatch:GetMetricStatistics`

Consente di CloudFront eseguire il rendering CloudWatch delle metriche nella CloudFront console.

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`elasticloadbalancing:DescribeLoadBalancers`

Durante la creazione e l'aggiornamento delle distribuzioni, consente di visualizzare un elenco di load balancer di Elastic Load Balancing nell'elenco delle origini disponibili.

Questa autorizzazione non è richiesta se non utilizzi la CloudFront console.

`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 ai bucket S3, consente a un utente di aggiornare la policy del bucket per concedere l'accesso all'identità di accesso di origine. CloudFront Per ulteriori informazioni, consulta the section called “Usa un'identità di accesso all'origine (legacy, non consigliata)”.

Questa autorizzazione non è richiesta se non utilizzi la console. CloudFront

`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 si utilizza la console. CloudFront

`waf:GetWebACL` e **`waf:ListWebACLs`**

Consente di visualizzare un elenco di ACL AWS WAF Web nella CloudFront console.

Queste autorizzazioni non sono necessarie se non si utilizza la CloudFront console.

AWS politiche gestite (predefinite) per CloudFront

AWS affronta molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da. AWS Queste policy AWS gestite concedono le autorizzazioni necessarie per i casi d'uso comuni in modo da evitare di dover esaminare quali autorizzazioni sono necessarie. Per ulteriori informazioni, consulta Policy gestite da AWS nella Guida per l'utente di IAM. Infatti CloudFront, IAM fornisce due policy gestite:

- CloudFrontFullAccess— Garantisce l'accesso completo alle CloudFront risorse.

> **Important**
>
> Se si desidera CloudFront creare e salvare i registri di accesso, è necessario concedere autorizzazioni aggiuntive. Per ulteriori informazioni, consulta Autorizzazioni richieste per configurare la registrazione standard e per accedere ai file di log.

- CloudFrontReadOnlyAccess— Garantisce l'accesso in sola lettura alle risorse. CloudFront

Esempi di policy gestite dal cliente

Puoi creare policy IAM personalizzate per consentire le autorizzazioni per le azioni API. CloudFront 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, gli AWS SDK 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, vedi. Autorizzazioni 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: consenti 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

```
{
   "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

```
{
   "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:

```
{
   "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: consenti la creazione di una distribuzione

La seguente politica di autorizzazione concede all'utente l'autorizzazione a creare ed elencare le distribuzioni nella CloudFront console. Per l'`CreateDistribution`azione, specificate il carattere jolly (*) per la distribuzione ARN () `Resource` invece di un carattere jolly per la distribuzione ARN (). `arn:aws:cloudfront::123456789012:distribution/*` Per ulteriori informazioni sull'*`Resource`*elemento, consulta IAM JSON Policy elements: Resource in the IAM User Guide.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "cloudfront:CreateDistribution",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "cloudfront:ListDistributions",
            "Resource": "*"
```

```
        }
    ]
}
```

AWSpolitiche gestite per Amazon CloudFront

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere le policy in autonomia. 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, utilizza le nostre policy gestite da AWS. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

I servizi AWS mantengono e aggiornano le policy gestite da AWS. Non è possibile modificare le autorizzazioni nelle policy gestite da AWS. 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 gestita da AWS, pertanto gli aggiornamenti delle policy non interrompono le autorizzazioni esistenti.

Inoltre, AWS supporta policy gestite per le funzioni di processi che coprono più servizi. Ad esempio, la policy ReadOnlyAccess gestita da AWS fornisce l'accesso in sola lettura sia ai servizi AWS che a tutte le risorse. Quando un servizio avvia 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, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Policy gestita da AWS: CloudFrontReadOnlyAccess

È possibile allegare la policy CloudFrontReadOnlyAccessalle 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 dell'autorizzazione

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 dirigenti di ottenere informazioni sull'archivio di valori chiave.
- `cloudfront-keyvaluestore:Get*`- Consente ai responsabili di ottenere informazioni e configurazioni dettagliate per il Key Value Store.
- `cloudfront-keyvaluestore:List*`- Consente ai presidi di ottenere elenchi degli archivi di valori chiave.
- `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 alle entità di ottenere un elenco di liste di ACL Web in AWS WAF.
- `waf:GetWebACL`: consente alle entità di ottenere informazioni dettagliate su ACL Web in AWS WAF.
- `wafv2:ListWebACLs`: consente alle entità di ottenere un elenco di liste di ACL Web in AWS WAF.
- `wafv2:GetWebACL`: consente alle entità di ottenere informazioni dettagliate su ACL Web in AWS WAF.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cfReadOnly",
      "Effect": "Allow",
      "Action": [
        "acm:ListCertificates",
```

```
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSPolicy gestita: CloudFrontFullAccess

È possibile allegare la policy CloudFrontFullAccessalle identità IAM. Questa politica consente autorizzazioni amministrative alle risorse. CloudFront Consente inoltre autorizzazioni di sola lettura per altre risorse di AWS servizio correlate CloudFront e visibili nella console. CloudFront

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `s3:ListAllMyBuckets`: consente alle entità di ottenere un elenco di tutti i bucket Amazon S3.
- `acm:ListCertificates`: consente alle entità di ottenere un elenco di certificati 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 chiave.
- `iam:ListServerCertificates`: consente alle entità di ottenere un elenco dei certificati del server archiviati in IAM.
- `waf:ListWebACLs`: consente alle entità di ottenere un elenco di liste di ACL Web in AWS WAF.
- `waf:GetWebACL`: consente alle entità di ottenere informazioni dettagliate su ACL Web in AWS WAF.

- `wafv2:ListWebACLs`: consente alle entità di ottenere un elenco di liste di ACL Web in AWS WAF.
- `wafv2:GetWebACL`: consente alle entità di ottenere informazioni dettagliate su ACL Web in AWS WAF.
- `kinesis:ListStreams`: consente alle entità di ottenere un elenco di flussi Amazon Kinesis.
- `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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cfflistbuckets",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "cffullaccess",
      "Action": [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "cffdescribestream",
      "Action": [
        "kinesis:DescribeStream"
```

```
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid": "cfflistroles",
      "Action": [
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:*"
    }
  ]
}
```

AWSPolicy gestita: AWSCloudFrontLogger

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 di ruolo collegate al servizio per logger CloudFront”.

AWSPolicy gestita: AWSLambdaReplicator

Non puoi allegare la AWSLambdaReplicatorpolicy 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 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”.

CloudFront aggiornamenti alle politiche gestite AWS

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 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 chiave e di agire su di essi.	19 dicembre 2023
CloudFrontReadOnlyAccess: aggiornamento a 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.	8 settembre 2021
CloudFront ha iniziato a tenere traccia delle modifiche	CloudFront ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	8 settembre 2021

Risoluzione dei 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 e IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna 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 alcuna 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 messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a CloudFront.

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

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

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

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

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se CloudFront supporta queste funzionalità, consultaCome 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Registrazione e monitoraggio in Amazon CloudFront

Il monitoraggio è importante per garantire la disponibilità e le prestazioni di CloudFront e delle soluzioni AWS. Dovresti raccogliere i dati di monitoraggio da tutte le parti della tua AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWSfornisce diversi strumenti per monitorare le CloudFront risorse e le attività e rispondere a potenziali incidenti:

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, osservi una singola metrica per un periodo di tempo specificato. Se il parametro supera una determinata soglia, viene inviata una notifica a un argomento Amazon SNS o alla policy 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 CloudFront metriche con Amazon CloudWatch.

Log di AWS CloudTrail

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 delle chiamate CloudFront API Amazon tramite AWS CloudTrail.

CloudFront registri standard e registri 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, consulta CloudFront e registrazione delle funzioni edge.

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

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 Visualizza CloudFront i report 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 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 PoP integrati) come servizio idoneo alla normativa HIPAA. CloudFront Se disponi di un Business Associate Addendum (BAA) eseguito con AWS, puoi utilizzare CloudFront (esclusa la distribuzione di contenuti tramite POP CloudFront incorporati) 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— 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 per valutare CloudFront le risorse, consulta CloudFront i controlli di Amazon nella Guida per l'AWS Security Hub 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 Configurazione e utilizzo di registri standard (registri di accesso).
- Acquisisci le richieste inviate all' CloudFront API. Per ulteriori informazioni, consulta Registrazione delle chiamate CloudFront API Amazon tramite 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 PoP CloudFront integrati) 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'intestazione `Cache-Control:no-cache="`*`nome campo`*`"` nelle risposte che contengono informazioni su carte di credito, ad esempio le ultime quattro cifre di un 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 PoP CloudFront integrati) 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 raggiungere i controlli e gli obiettivi chiave di conformità. AWS 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 velocità effettiva elevata. 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 sulle regioni AWS e sulle zone di disponibilità, consulta Infrastruttura globale di AWS.

CloudFront failover di origine

Oltre al supporto dell'infrastruttura AWS globale, Amazon CloudFront offre una funzionalità di failover di origine per supportare le tue 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 punti di presenza (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 designare un'origine principale CloudFront più una seconda origine. CloudFront passa automaticamente alla seconda origine quando l'origine principale restituisce risposte di errore specifiche del codice di stato HTTP. Per ulteriori informazioni, consulta Ottimizza l'alta disponibilità con il failover di CloudFront origine.

Sicurezza dell'infrastruttura in Amazon CloudFront

In quanto servizio gestito, Amazon CloudFront è protetto dalla sicurezza di rete AWS globale. 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.

Utilizzi chiamate API AWS pubblicate per accedere 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.

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

CloudFront Functions utilizza una barriera di isolamento altamente sicura tra AWS gli account, garantendo che gli ambienti dei clienti siano protetti da 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 qualsiasi punto di presenza (POP) di CloudFront edge location, 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

Risolvi i problemi più comuni che potresti riscontrare durante la configurazione di Amazon CloudFront per la distribuzione dei tuoi contenuti o quando usi Lambda @Edge e trova le possibili soluzioni.

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

Hai specificato un oggetto mancante dall'origine Amazon S3

Verifica che l'oggetto richiesto nel tuo bucket esista. I nomi degli oggetti distinguono tra maiuscole e minuscole L'immissione di un nome di 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 tuo browser web, se inserisci `https://d111111abcdef8.cloudfront.net/INDEX.HTML` invece di`https://d111111abcdef8.cloudfront.net/index.html`, potresti visualizzare un messaggio simile perché il `index.html` file 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>
```

La tua origine Amazon S3 non dispone delle autorizzazioni IAM

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 specifichi le autorizzazioni corrette, ai tuoi spettatori può apparire il seguente messaggio di accesso negato.

```
<Code>AccessDenied</Code>
<Message>User: arn:aws:sts::856369053181:assumed-role/OriginAccessControlRole/
EdgeCredentialsProxy+EdgeHostAuthenticationClient is not authorized to perform:
 kms:Decrypt on the resource associated with this ciphertext because the resource does
 not exist in this Region, no resource-based policies allow access, or a resource-based
 policy explicitly denies access</Message>
<RequestId>22Q367AHT7Y1ABCD/RequestId>
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
```

```
</Error>
```

> **Note**
>
> In questo messaggio di errore, l'ID account 856369053181 è un account gestito. AWS

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.

Per 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 tuo bucket Amazon S3 per la crittografia predefinita. Per ulteriori informazioni, consulta Specificare la 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 sui bucket di Amazon S3 che utilizza il controllo dell'accesso all'origine, consulta. Concedi all'origine il permesso di controllo dell'accesso per accedere al bucket S3
4. Modifica la politica delle chiavi KMS per concedere CloudFront l'autorizzazione a eseguire le azioni `aEncrypt`, `Decrypt` e. `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 politica chiave KMS, consulta laSSE-KMS.

Se utilizzi Origin Access Identity (OAI) anziché OAC, le autorizzazioni per il bucket Amazon S3 sono leggermente diverse perché concedi l'autorizzazione a un'identità anziché a. Servizio AWS Per

ulteriori informazioni, consulta Concedi l'autorizzazione all'identità di accesso all'origine per leggere i file nel bucket Amazon S3.

Se ancora non riesci a visualizzare i file nella tua distribuzione, consulta. Non posso visualizzare i file nella distribuzione

Stai utilizzando credenziali non valide o non disponi di autorizzazioni sufficienti

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 risorsa. CloudFront Per ulteriori informazioni sui messaggi di errore di accesso negato, consulta Risoluzione dei messaggi di errore di accesso negato nella Guida per l'utente IAM.

Per informazioni su come funziona IAM CloudFront, consultaIdentity 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 certificato SSL/TLS 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.

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. Configurazione

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. Il modo più semplice da usare CloudFront con Amazon S3 consiste nel rendere tutti gli oggetti leggibili pubblicamente in Amazon S3. A questo proposito, devi attivare esplicitamente privilegi di lettura pubblica per ogni oggetto che carichi in Amazon S3.

Se i tuoi contenuti non sono leggibili pubblicamente, devi creare un controllo di accesso all' CloudFront origine (OAC) in modo che possa accedervi. CloudFront Per ulteriori informazioni sul controllo dell'accesso all' CloudFront origine, consulta. the section called “Limita l'accesso a un'origine Amazon Simple Storage Service”

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 sui CNAME, consulta Utilizza URL personalizzati aggiungendo nomi di dominio alternativi (CName).

Stai facendo riferimento all'URL corretto per la tua distribuzione? CloudFront

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 SSL/TLS personalizzato. Prima di poter eliminare un certificato SSL/TLS, è necessario ruotare il certificato (sostituire il certificato SSL/TLS personalizzato corrente con un altro certificato SSL/TLS personalizzato) o tornare dall'utilizzo di un certificato SSL/TLS personalizzato all'utilizzo del certificato predefinito. CloudFront Per risolvere questo problema, completa le fasi in una delle procedure seguenti:

- Ruota i certificati SSL/TLS
- Passa da un certificato SSL/TLS personalizzato al certificato predefinito CloudFront

Risoluzione di risposte di errore dall'origine

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. Negli argomenti seguenti vengono descritte le cause comuni per alcuni di questi codici di stato HTTP e alcune possibili soluzioni.

Argomenti

- Codice di stato HTTP 400 (richiesta errata)
- 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)

La tua CloudFront distribuzione 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 '<AWS Region>' è sbagliata; si prevede '< Region>'AWS

Per 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 AWS Management Console 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 la distribuzione, lo stato di distribuzione viene visualizzato nella colonna Ultima modifica. Qualche tempo dopo il completamento della distribuzione, dovresti smettere di ricevere le risposte di `AuthorizationHeaderMalformed` errore.

Codice di stato HTTP 502 (Gateway non valido)

Un codice di stato HTTP 502 (Bad Gateway) indica che 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

- Errore di negoziazione SSL/TLS tra e un server di origine personalizzato CloudFront
- L'origine non risponde con crittografie/protocolli supportati
- 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
- Errore DNS () NonS3OriginDnsError

Errore di negoziazione SSL/TLS tra e un server di origine personalizzato CloudFront

Se utilizzi un'origine personalizzata e sei configurato CloudFront per richiedere HTTPS tra CloudFront e la tua origine, il problema potrebbe essere dovuto alla mancata corrispondenza tra i nomi di dominio. Il certificato SSL/TLS installato nell'origine include un nome di dominio nel campo Common Name (Nome comune) e possibilmente altri nomi nel campo Subject Alternative Names (Nomi alternativi oggetto). (CloudFront supporta caratteri jolly nei nomi di dominio dei certificati.) Uno dei nomi di dominio nel certificato deve corrispondere a uno o entrambi i seguenti valori:

- Il valore che hai specificato per Origin Domain per l'origine applicabile nella tua distribuzione.
- Il valore dell'`Host`intestazione se hai configurato CloudFront per inoltrare l'`Host`intestazione all'origine. Per ulteriori informazioni sull'inoltro dell'intestazione `Host` alla tua origine, consulta Contenuto della cache in base alle intestazioni delle richieste.

Se i nomi di dominio non corrispondono, l'handshake SSL/TLS ha esito negativo e CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) e imposta l'intestazione su. `X-Cache Error from cloudfront`

Per determinare se i nomi di dominio nel certificato corrispondono al dominio di origine nella distribuzione o nell'`Host`intestazione, puoi utilizzare un correttore SSL online o OpenSSL. Se i nomi di dominio non corrispondono, hai due opzioni:

- Il valore specificato per Origin Domain Name (Nome dominio origine) per l'origine applicabile nella tua distribuzione.
- Il valore dell'`Host`intestazione se hai configurato l'inoltro dell'intestazione CloudFront all'origine. `Host` Per ulteriori informazioni sull'inoltro dell'intestazione `Host` alla tua origine, consulta Contenuto della cache in base alle intestazioni delle richieste.

Se i nomi di dominio non corrispondono, l'handshake SSL/TLS ha esito negativo e CloudFront restituisce un codice di stato HTTP 502 (Bad Gateway) e imposta l'intestazione su. `X-Cache Error from cloudfront`

Per determinare se i nomi di dominio nel certificato corrispondono a Origin Domain Name (Nome 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:

- Ottenere un nuovo certificato SSL/TLS che include i nomi di dominio applicabili.

Se utilizzi AWS Certificate Manager (ACM), consulta Richiesta di un certificato pubblico nella Guida per l'utente per richiedere un nuovo certificato.AWS Certificate Manager

- 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, specifichi il nome del tuo dominio e lo strumento restituisce varie informazioni sul tuo certificato SSL/TLS. 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 SSL/TLS al tuo server di origine. 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 (*`sostituisci`* il dominio di origine con il nome di dominio del tuo 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'opzione `-servername` al comando OpenSSL, come nell'esempio seguente (sostituisci *`CNAME`* con il CNAME configurato nella 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 CloudFront e l'origine” 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 CloudFront e l'origine”.

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 certificato SSL/TLS sul server di origine personalizzato, consultare the section called “Richiedi 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 che CloudFront si connettono 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 di AWS nella Riferimenti generali di Amazon Web Services. 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 ed esegui il debug delle funzioni Lambda @Edge.

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.

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 nella posizione periferica

- 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 richieste PUT/COPY/POST/DELETE o 5.500 richieste GET/HEAD al secondo per prefisso Amazon S3 partizionato. Quando Amazon S3 restituisce una risposta 503 Slow Down, in genere indica una frequenza di richieste eccessiva rispetto a uno specifico prefisso Amazon S3.

    Poiché le tariffe di richiesta si applicano a ogni 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 per gestire le richieste per ciascuno dei prefissi separatamente. Di conseguenza, la frequenza di richiesta 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 Elastic Load Balancing come server di origine:
  - Assicurati che le tue istanze di backend possano rispondere ai controlli di integrità.
  - Assicurati che il tuo sistema di bilanciamento del carico e le istanze di backend siano in grado di gestire il carico.

  Per ulteriori informazioni, consultare:
  - Come posso risolvere gli errori 503 restituiti durante l'utilizzo di 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 assicurarti che l'origine disponga di risorse sufficienti, come memoria, CPU e dimensioni del disco.

  - Se utilizzi Amazon EC2 come back-end, assicurati che il tipo di istanza disponga delle risorse appropriate per soddisfare le richieste in entrata. Per maggiori informazioni, consulta Tipi di istanza nella Guida per l'utente di Amazon EC2.
- Se utilizzi API Gateway:
  - Questo errore è correlato all'integrazione del backend quando l'API API Gateway non è in grado di ricevere una risposta. Il server di backend potrebbe essere:
    - Sovraccarico oltre la capacità e incapace di elaborare le nuove richieste dei client.
    - In manutenzione temporanea.
  - Per risolvere questo errore, esamina i log delle applicazioni API Gateway per determinare se c'è un problema con la capacità di backend, l'integrazione o altro.

CloudFront ha causato l'errore a causa di vincoli di risorse nella posizione periferica

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 sulla CloudFront distribuzione. 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 accade nel tuo ambiente di produzione, contatta AWS Support.

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 ed esegui il debug delle funzioni Lambda @Edge

Per ulteriori informazioni sul test CloudFront delle funzioni, consultaFunzioni di test.

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 ed esegui il debug” Puoi anche vedere le quote dei servizi Lambda nella Developer Guide.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 firewall IPTable su un server Linux, puoi cercare strumenti e informazioni per lavorare meglio con IPTables.
- 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 Posizioni e intervalli di indirizzi IP dei server periferici 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 gli errori HTTP 504 consiste semplicemente nell'impostare un valore di CloudFront timeout più elevato 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, modifica il valore di timeout per la distribuzione. CloudFront

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 "Connect time: %{time_connect} Time to first byte: %{time_starttransfer} Total
 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'istanza Amazon EC2 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'istanza Amazon EC2 come server back-end, assicurati che il tipo di istanza disponga delle risorse appropriate per soddisfare le richieste in entrata. Per maggiori informazioni, consulta Tipi di istanza nella Guida per l'utente di Amazon EC2.

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 server di origine, scopri in che modo è possibile ridurre la latenza rivedendo i suggerimenti nel seguente articolo del Knowledge Center: Come posso risolvere i problemi di alta latenza sul mio ELB Classic Load Balancer?

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 (solo origini personalizzate)”.

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 client riceverà quindi un set diverso di indirizzi IP dal DNS.
- Per ogni client che effettua richieste, distribuisci le richieste dei client sul set di indirizzi IP restituiti dal 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 della cache con trigger di richiesta o risposta del visualizzatore Lambda @Edge.
> - Il test di carico non è consentito sulle origini con Origin Shield abilitato.

Quote

CloudFront è soggetto alle seguenti quote.

Argomenti

Quote generali

Entità	Quota predefinita
Velocità di trasferimento dati per distribuzione	150 Gbps Richiedi una quota più elevata.
Richieste al secondo per distribuzione	250.000 Richiedi una quota più elevata.

Entità	Quota predefinita
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 di origine, incluse le intestazioni e le stringhe di query, ma escluso il contenuto del corpo	20.480 byte
Lunghezza massima di un URL	8,192 byte

Quote generali sulle distribuzioni

Entità	Quota predefinita
Nomi di dominio alternativi (CNAME) per distribuzione Per ulteriori informazioni, consulta Utilizza URL personalizzati aggiungendo nomi di dominio alternativi (CName).	100 Richiedi una quota più elevata.
Comportamenti cache per distribuzione	25 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
Distribuzioni per Account AWS Per ulteriori informazioni, consulta Creazione di una distribuzione.	200

Entità	Quota predefinita
	Richiedi una quota più elevata.
Distribuzioni per origine e controllo degli accessi	100 Richiedi una quota più elevata.
Compressione dei file: gamma di dimensioni dei file che CloudFront vengono compressi Per ulteriori informazioni, consulta Servire file compressi.	Da 1.000 a 10.000.000 byte
Timeout Keep-alive per origine Per ulteriori informazioni, consulta Timeout keep-alive origine (solo origini personalizzate).	1-60 secondi Richiedi una quota più elevata.
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
Identità di accesso all'origine per Account AWS	100 Richiedi una quota più elevata.
Origini per distribuzione	25 Richiedi una quota più elevata.

Entità	Quota predefinita
Gruppi di origine per la distribuzione	10 Richiedi una quota più elevata.
Timeout di risposta per origine Per ulteriori informazioni, consulta Timeout di risposta (solo origini personalizzate).	1-60 secondi Richiedi una quota più elevata.
Distribuzioni stagionali per Account AWS Per ulteriori informazioni, consulta the section called “Utilizza la distribuzione continua per testare le modifiche in sicurezza”.	20 Richiedi una quota più elevata.

Quote generali sulle policy

Entità	Quota predefinita
Politiche di cache per Account AWS	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

Entità	Quota predefinita
	Richiedi una quota più elevata.
Lunghezza totale combinata di tutti i nomi di stringhe di query, intestazioni e cookie in una policy della cache	1.024
Politiche di richiesta Origin per Account AWS	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 relative alle intestazioni di risposta per Account AWS	20 Richiedi una quota più elevata.

Entità	Quota predefinita
Distribuzioni associate alla stessa policy delle intestazioni di risposta	100 Richiedi una quota più elevata.
Intestazioni personalizzate per policy delle intestazioni di risposta	10 Richiedi una quota più elevata.
Politiche di implementazione continua per Account AWS	20 Richiedi una quota più elevata.

Quote sulle funzioni CloudFront

Entità	Quota predefinita
Funzioni per Account AWS	100
Dimensione massima della funzione	10 KB Richiedi una quota più elevata.
Memoria massima funzione	2 MB
Distribuzioni associate alla stessa funzione	100

Oltre a queste quote, esistono altre restrizioni quando si utilizzano CloudFront le funzioni. Per ulteriori informazioni, consulta Restrizioni sulle funzioni CloudFront .

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 chiavi 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

Le quote in questa sezione si applicano a Lambda@Edge. Queste quote si aggiungono alle AWS Lambda quote predefinite, anch'esse valide. Per le quote Lambda, consulta Quote nella Guida per gli sviluppatori di AWS Lambda .

> **Note**
>
> Lambda dimensiona dinamicamente la capacità in risposta a un aumento del traffico, sempre nel rispetto delle quote dell' Account AWS. Per ulteriori informazioni, consulta Dimensionamento della funzione nella Guida per gli sviluppatori di AWS Lambda .

Quote generali

Entità	Quota predefinita
Le distribuzioni per Account AWS cui possono avere funzioni Lambda @Edge	500 Richiedere una quota più elevata.
Funzioni Lambda@Edge per distribuzione	100 Richiedere una quota più elevata.
Richieste al secondo	10.000 (in ciascuna) Regione AWS Richiedere una quota più elevata.
Esecuzioni simultanee Per ulteriori informazioni, consulta Dimensionamento della funzione nella Guida per gli sviluppatori di AWS Lambda .	1.000 (in ciascuno Regione AWS) Richiedere una quota più elevata.
Distribuzioni associate alla stessa funzione	500

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 quali bucket Amazon S3, tabelle DynamoDB o	5 secondi	30 secondi

Entità	Eventi di richiesta e risposta del visualizzatore	Eventi di richiesta e risposta origine
istanze Amazon EC2 nelle regioni Regioni AWS.		
Dimensione di una risposta generata da una funzione Lambda, inclusi intestazioni e corpo	40 KB	1 MB
Dimensione compressa massima di una funzione Lambda e delle eventuali librerie incluse	1 MB	50 MB

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 Account AWS si applicano 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 dei certificati SSL/TLS con CloudFront (HTTPS solo tra i visualizzatori e solo tra i visualizzatori) CloudFront .

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 Aumenta le quote per i 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 Invalida i file per rimuovere il contenuto.	3.000
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.

Entità	Quota predefinita
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 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

Entità	Quota predefinita
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
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 politica di cache o una politica di richiesta di origine anziché le impostazioni precedenti.

Entità	Quota predefinita
Cookie per il comportamento della cache	10
Per ulteriori informazioni, consulta Contenuto della cache basato sui cookie.	Richiedi una quota più elevata.
Numero totale di byte nei nomi dei cookie (non si applica se si configura CloudFront l'inoltro 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 politica di cache o una politica di richiesta di origine anziché le impostazioni precedenti.

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 Per ulteriori informazioni, consulta Contenuto della cache in base ai parametri della stringa di query.	10 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 “Contenuto della cache in base alle intestazioni delle richieste”.	10 Richiedi una quota più elevata.
Intestazioni personalizzate: numero massimo di intestazioni personalizzate che puoi configurare CloudFront per aggiungere alle richieste di origine Per ulteriori informazioni, consulta the section called “Aggiungi intestazioni personalizzate alle richieste di origine”.	10 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.

Entità	Quota predefinita
Intestazioni personalizzate: lunghezza massima di un nome di intestazione	256 caratteri
Intestazioni personalizzate: lunghezza massima di un valore di intestazione	1,783 caratteri
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.

Esempi di codice per l' CloudFront utilizzo degli AWS SDK

I seguenti esempi di codice mostrano come utilizzare un kit CloudFront di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Azioni per l' CloudFront utilizzo AWS degli SDK
  - Utilizzo CreateDistribution con un AWS SDK o una CLI
  - Utilizzo CreateFunction con un AWS SDK o una CLI
  - Utilizzo CreateInvalidation con un AWS SDK o una CLI
  - Utilizzo CreateKeyGroup con un AWS SDK o una CLI
  - Utilizzo CreatePublicKey con un AWS SDK o una CLI
  - Utilizzo DeleteDistribution con un AWS SDK o una CLI
  - Utilizzo GetCloudFrontOriginAccessIdentity con un AWS SDK o una CLI
  - Utilizzo GetCloudFrontOriginAccessIdentityConfig con un AWS SDK o una CLI
  - Utilizzo GetDistribution con un AWS SDK o una CLI
  - Utilizzo GetDistributionConfig con un AWS SDK o una CLI
  - Utilizzo ListCloudFrontOriginAccessIdentities con un AWS SDK o una CLI
  - Utilizzo ListDistributions con un AWS SDK o una CLI
  - Utilizzo UpdateDistribution con un AWS SDK o una CLI
- Scenari per l' CloudFront utilizzo AWS degli SDK
  - Elimina le risorse di CloudFront firma utilizzando AWS SDK
  - Crea URL e cookie firmati utilizzando un SDK AWS

Azioni per l' CloudFront utilizzo AWS degli SDK

I seguenti esempi di codice mostrano come eseguire CloudFront azioni individuali con gli AWS SDK. Questi estratti richiamano l' CloudFront API e sono estratti di codice di programmi più grandi che devono essere eseguiti nel contesto. Ogni esempio include un collegamento a GitHub, dove è possibile trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta Amazon CloudFront API Reference.

Esempi

- Utilizzo CreateDistribution con un AWS SDK o una CLI
- Utilizzo CreateFunction con un AWS SDK o una CLI
- Utilizzo CreateInvalidation con un AWS SDK o una CLI
- Utilizzo CreateKeyGroup con un AWS SDK o una CLI
- Utilizzo CreatePublicKey con un AWS SDK o una CLI
- Utilizzo DeleteDistribution con un AWS SDK o una CLI
- Utilizzo GetCloudFrontOriginAccessIdentity con un AWS SDK o una CLI
- Utilizzo GetCloudFrontOriginAccessIdentityConfig con un AWS SDK o una CLI
- Utilizzo GetDistribution con un AWS SDK o una CLI
- Utilizzo GetDistributionConfig con un AWS SDK o una CLI
- Utilizzo ListCloudFrontOriginAccessIdentities con un AWS SDK o 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

I seguenti esempi di codice mostrano come utilizzare`CreateDistribution`.

CLI

AWS CLI

Per creare una distribuzione CloudFront

L'esempio seguente crea una distribuzione per un bucket S3 denominato `awsexamplebucket` e lo specifica anche `index.html` come oggetto root predefinito, utilizzando argomenti della riga di comando:

```
aws cloudfront create-distribution \
    --origin-domain-name awsexamplebucket.s3.amazonaws.com \
    --default-root-object index.html
```

Invece di utilizzare argomenti della riga di comando, è possibile fornire la configurazione della distribuzione in un file JSON, come illustrato nell'esempio seguente:

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

Il file `dist-config.json` è un documento JSON nella cartella corrente che contiene quanto segue:

```
{
    "CallerReference": "cli-example",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                "DomainName": "awsexamplebucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
```

```
    "DefaultCacheBehavior": {
        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-example",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
```

```
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": true,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Sia che si forniscano le informazioni sulla distribuzione con un argomento della riga di comando o un file JSON, l'output è lo stesso:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EMLARXS9EXAMPLE",
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-11-22T00:55:15.705Z",
        "InProgressInvalidationBatches": 0,
```

```
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "awsexamplebucket.s3.amazonaws.com-cli-example",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
```

```
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
```

```
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- 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

Esempio 1: crea una CloudFront distribuzione di base, configurata con registrazione e memorizzazione nella cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "ps-cmdlet-sample.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
```

```
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
      -Logging_Bucket ps-cmdlet-sample-logging.s3.amazonaws.com `
      -Logging_Prefix "help/" `
      -DistributionConfig_CallerReference Client1 `
      -DistributionConfig_DefaultRootObject index.html `
      -DefaultCacheBehavior_TargetOriginId $origin.Id `
      -ForwardedValues_QueryString $true `
      -Cookies_Forward all `
      -WhitelistedNames_Quantity 0 `
      -TrustedSigners_Enabled $false `
      -TrustedSigners_Quantity 0 `
      -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
      -DefaultCacheBehavior_MinTTL 1000 `
      -DistributionConfig_PriceClass "PriceClass_All" `
      -CacheBehaviors_Quantity 0 `
      -Aliases_Quantity 0
```

- Per i dettagli sull'API, vedere CreateDistributionin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateFunction`** con un AWS SDK o una CLI

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 con un SDK CloudFront AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateInvalidation`** con un AWS SDK o una CLI

I seguenti esempi di codice 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 propri `CallerReference` parametri 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 Command Reference. CreateInvalidationAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio crea una nuova invalidazione su una distribuzione con un 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 memorizza tre percorsi di immagini e file multimediali che l'utente non desidera vengano inseriti nella cache della distribuzione. 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 in Cmdlet Reference. CreateInvalidationAWS Tools for PowerShell

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateKeyGroup`** con un AWS SDK o una CLI

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 gli URL o i cookie 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 sezione CreateKeyGroup AWS SDK for Java 2.xAPI Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo con un SDK CloudFront 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

I seguenti esempi di codice 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 denominato`pub-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. Si noti 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 AWS CLI Command CreatePublicKeyReference.

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 con un SDK CloudFront 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

I seguenti esempi di codice mostrano come utilizzare`DeleteDistribution`.

CLI

AWS CLI

Per eliminare una distribuzione CloudFront

L'esempio seguente elimina la CloudFront distribuzione con l'ID. `EDFDVBD6EXAMPLE` Prima di poter eliminare una distribuzione, è necessario disattivarla. Per disabilitare una distribuzione, usa il comando update-distribution. Per ulteriori informazioni, consulta gli esempi di update-distribution.

Quando una distribuzione è disabilitata, puoi eliminarla. Per eliminare una distribuzione, è necessario utilizzare l'`--if-match`opzione per fornire la distribuzione`ETag`. Per ottenere la`ETag`, usa il comando get-distribution oget-distribution-config .

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

In caso di successo, questo comando non produce alcun risultato.

- Per i dettagli sull'API, consulta DeleteDistribution 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 aggiorna una distribuzione in modalità disattivata, utilizza un cameriere 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 DeleteDistributionAPI Reference.AWS SDK for Java 2.x

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo con un SDK CloudFront AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetCloudFrontOriginAccessIdentity`** con un AWS SDK o una CLI

I seguenti esempi di codice 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. [GetCloudFrontOriginAccessIdentity](AWS CLI)

PowerShell

Strumenti per 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 [GetCloudFrontOriginAccessIdentity](in AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetCloudFrontOriginAccessIdentityConfig`** con un AWS SDK o una CLI

I seguenti esempi di codice 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'ID`E74FTE3AEXAMPLE`, 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

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 Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetDistribution`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetDistribution`.

CLI

AWS CLI

Per ottenere una distribuzione CloudFront

L'esempio seguente ottiene la CloudFront distribuzione con l'`IDEDFDVBD6EXAMPLE`, incluso il relativo`ETag`. L'ID di 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": "awsexamplebucket.s3.amazonaws.com-cli-example",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
```

```
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
```

```
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Per i dettagli sull'API, consulta Command Reference. GetDistributionAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: recupera le informazioni per una distribuzione specifica.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront 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

I seguenti esempi di codice mostrano come utilizzare`GetDistributionConfig`.

CLI

AWS CLI

Per ottenere una configurazione di CloudFront distribuzione

L'esempio seguente ottiene i metadati sulla CloudFront distribuzione con l'ID`EDFDVBD6EXAMPLE`, incluso il relativo`ETag`. L'ID di 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": "awsexamplebucket.s3.amazonaws.com-cli-example",
                    "DomainName": "awsexamplebucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
```

```
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
```

```
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

- Per i dettagli sull'API, consulta Command Reference. GetDistributionConfigAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: recupera la configurazione per una distribuzione specifica.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Per i dettagli sull'API, vedere GetDistributionConfigin AWS Tools for PowerShell Cmdlet Reference.

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 con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListCloudFrontOriginAccessIdentities`** con un AWS SDK o una CLI

I seguenti esempi di codice 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 all' CloudFront origine (OAI) presenti nel tuo account: AWS

```
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 AWS CLI Command ListCloudFrontOriginAccessIdentitiesReference.

PowerShell

Strumenti per 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 Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo con un SDK CloudFront 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

I seguenti esempi di codice 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": "EMLARXS9EXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
EMLARXS9EXAMPLE",
                "Status": "InProgress",
                "LastModifiedTime": "2019-11-22T00:55:15.705Z",
                "InProgressInvalidationBatches": 0,
                "DomainName": "d111111abcdef8.cloudfront.net",
                "ActiveTrustedSigners": {
```

```
                    "Enabled": false,
                    "Quantity": 0
                },
                "DistributionConfig": {
                    "CallerReference": "cli-example",
                    "Aliases": {
                        "Quantity": 0
                    },
                    "DefaultRootObject": "index.html",
                    "Origins": {
                        "Quantity": 1,
                        "Items": [
                            {
                                "Id": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                                "DomainName":
 "awsexamplebucket.s3.amazonaws.com",
                                "OriginPath": "",
                                "CustomHeaders": {
                                    "Quantity": 0
                                },
                                "S3OriginConfig": {
                                    "OriginAccessIdentity": ""
                                }
                            }
                        ]
                    },
                    "OriginGroups": {
                        "Quantity": 0
                    },
                    "DefaultCacheBehavior": {
                        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-cli-
example",
                        "ForwardedValues": {
                            "QueryString": false,
                            "Cookies": {
                                "Forward": "none"
                            },
                            "Headers": {
                                "Quantity": 0
                            },
                            "QueryStringCacheKeys": {
                                "Quantity": 0
                            }
```

```
                    },
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "MinTTL": 0,
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "DefaultTTL": 86400,
                    "MaxTTL": 31536000,
                    "Compress": false,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": ""
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "Logging": {
                    "Enabled": false,
                    "IncludeCookies": false,
                    "Bucket": "",
                    "Prefix": ""
                },
                "PriceClass": "PriceClass_All",
```

```
                    "Enabled": true,
                    "ViewerCertificate": {
                        "CloudFrontDefaultCertificate": true,
                        "MinimumProtocolVersion": "TLSv1",
                        "CertificateSource": "cloudfront"
                    },
                    "Restrictions": {
                        "GeoRestriction": {
                            "RestrictionType": "none",
                            "Quantity": 0
                        }
                    },
                    "WebACLId": "",
                    "HttpVersion": "http2",
                    "IsIPV6Enabled": true
                }
            },
            {
                "Id": "EDFDVBD6EXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
EDFDVBD6EXAMPLE",
                "Status": "InProgress",
                "LastModifiedTime": "2019-12-04T23:35:41.433Z",
                "InProgressInvalidationBatches": 0,
                "DomainName": "d930174dauwrn8.cloudfront.net",
                "ActiveTrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "DistributionConfig": {
                    "CallerReference": "cli-example",
                    "Aliases": {
                        "Quantity": 0
                    },
                    "DefaultRootObject": "index.html",
                    "Origins": {
                        "Quantity": 1,
                        "Items": [
                            {
                                "Id": "awsexamplebucket1.s3.amazonaws.com-cli-
example",
                                "DomainName":
 "awsexamplebucket1.s3.amazonaws.com",
                                "OriginPath": "",
```

```
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            }
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "awsexamplebucket1.s3.amazonaws.com-
cli-example",
                    "ForwardedValues": {
                        "QueryString": false,
                        "Cookies": {
                            "Forward": "none"
                        },
                        "Headers": {
                            "Quantity": 0
                        },
                        "QueryStringCacheKeys": {
                            "Quantity": 0
                        }
                    },
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "MinTTL": 0,
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
```

```
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "DefaultTTL": 86400,
                    "MaxTTL": 31536000,
                    "Compress": false,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": ""
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "Logging": {
                    "Enabled": false,
                    "IncludeCookies": false,
                    "Bucket": "",
                    "Prefix": ""
                },
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": true,
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "http2",
                "IsIPV6Enabled": true
            }
        },
        {
```

```
                "Id": "E1X5IZQEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E1X5IZQEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2019-11-06T21:31:48.864Z",
                "DomainName": "d2e04y12345678.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Id": "awsexamplebucket2",
                            "DomainName": "awsexamplebucket2.s3.us-
west-2.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            }
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "awsexamplebucket2",
                    "ForwardedValues": {
                        "QueryString": false,
                        "Cookies": {
                            "Forward": "none"
                        },
                        "Headers": {
                            "Quantity": 0
                        },
                        "QueryStringCacheKeys": {
                            "Quantity": 0
                        }
                    },
                    "TrustedSigners": {
```

```
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "MinTTL": 0,
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "DefaultTTL": 86400,
                    "MaxTTL": 31536000,
                    "Compress": false,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": ""
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": true,
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
```

```
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "HTTP1_1",
                "IsIPV6Enabled": true
            }
        ]
    }
}
```

- Per i dettagli sull'API, consulta ListDistributions AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce le distribuzioni.

```
Get-CFDistributionList
```

- Per i dettagli sull'API, vedere ListDistributionsin AWS Tools for PowerShell Cmdlet Reference.

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 con un SDK CloudFront 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

I seguenti esempi di codice mostrano come utilizzare`UpdateDistribution`.

CLI

AWS CLI

Per aggiornare l'oggetto radice predefinito di una CloudFront distribuzione

L'esempio seguente aggiorna l'oggetto root predefinito `index.html` per la CloudFront distribuzione con l'IDEDFDVBD6EXAMPLE:

```
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
        }
    }
}
```

Per 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'`--if-match`opzione per fornire quella della distribuzione. `ETag` Per ottenere la`ETag`, usa il comando get-distribution oget-distribution-config .

Dopo aver utilizzato l'esempio seguente per disabilitare una distribuzione, è possibile utilizzare il comando delete-distribution per eliminarla.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Il file `dist-config-disable.json` è un documento JSON nella cartella corrente che contiene quanto segue. Nota che il `Enabled` campo è impostato su: `false`

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
                "DomainName": "awsexamplebucket.s3.amazonaws.com",
```

```
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
```

```
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": false,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

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":
 "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "awsexamplebucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId":
 "awsexamplebucket.s3.amazonaws.com-1574382155-273939",
```

```
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
```

```
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": false,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Per i dettagli sull'API, consulta UpdateDistribution 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.

```
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 con un SDK CloudFront AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari per l' CloudFront utilizzo AWS degli SDK

I seguenti esempi di codice mostrano come implementare scenari comuni CloudFront con gli AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno. CloudFront Ogni scenario include un collegamento a GitHub, dove è possibile trovare istruzioni su come configurare ed eseguire il codice.

Esempi

- Elimina le risorse di CloudFront firma utilizzando AWS SDK
- Crea URL e cookie firmati utilizzando un SDK AWS

Elimina le risorse di CloudFront firma utilizzando AWS SDK

Il seguente esempio di codice 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 delle 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 con un SDK CloudFront AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Crea URL e cookie firmati utilizzando un SDK AWS

Il seguente esempio di codice mostra come creare URL e cookie firmati 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 URL 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 URL o cookie con una politica personalizzata. I `activeDate` e `ipRange` sono metodi opzionali.

```
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;

public class CreateCustomPolicyRequest {

    public static CustomSignerRequest createRequestForCustomPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expireDate = Instant.now().plus(7, ChronoUnit.DAYS);
        // URL will be accessible tomorrow using the signed URL.
        Instant activeDate = Instant.now().plus(1, ChronoUnit.DAYS);
        Path path = Paths.get(privateKeyFullPath);

        return CustomSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expireDate)
```

```
                .activeDate(activeDate) // Optional.
                // .ipRange("192.168.0.1/24") // Optional.
                .build();
    }
}
```

L'esempio seguente dimostra l'uso della CloudFrontUtilitiesclasse per produrre cookie e URL firmati. 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 con un SDK CloudFront 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 CloudFront documentazione. Per ricevere le notifiche sugli aggiornamenti, è possibile effettuare la sottoscrizione al feed RSS.

Modifica	Descrizione	Data
Sono state aggiunte nuove politiche di cache gestita	Sono state aggiunte nuove politiche di cache gestita `UseOriginCacheControlHeaders` `eUseOriginCacheControlHeaders-QueryStrings` .	24 maggio 2024
Aggiunto il supporto per il controllo dell'accesso all'origine	Ora puoi creare un controllo di accesso all'origine (OAC) per AWS Elemental MediaPackage V2 e l'URL AWS Lambda della funzione.	11 aprile 2024
Campi di registro in tempo reale per CMCD	Aggiunti 18 campi CMCD (Common Media Client Data) per la registrazione in tempo reale.	9 aprile 2024
Iniziare con una distribuzione di base CloudFront	Tutorial aggiornato per una distribuzione di base che utilizza un'origine Amazon S3 con controllo dell'accesso all'origine (OAC).	18 marzo 2024
Esempi di codice per l' CloudFront utilizzo AWS degli SDK	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	16 febbraio 2024

	che mostrano come richiamar e le singole funzioni di servizio ed esempi che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.	
AWS aggiornamento della politica gestita	Le policy IAM `CloudFron tReadOnlyAccess` 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'inte rno di CloudFront Functions, abilitando una logica personali zzabile avanzata nelle edge location. 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
Abilitare le ACL per 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 visualizz atore 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 l'utente	Lingua aggiornata e collegame nto aggiunto ai CloudFront controlli Amazon riorganizzati nella Guida per l'AWS Security Hub 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 intestazi oni HTTP o i cookie, ad eccezione di quelli specifica ti, 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'intesta zione 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 configurazione CDN eseguendo test con un sottoinsieme del traffico di produzione.	18 novembre 2022
Rilascio dell'intestazione `CloudFront-Viewer-JA3-Fingerprint`	È ora possibile utilizzare l'impronta JA3 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 AWS 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 -Viewer-TLS CloudFront	È possibile visualizzare nuove informazioni sull'handshake SSL/TLS 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	Ora puoi utilizzare l'`CloudFront-Viewer-TLS` intestazione per ottenere informazioni sulla versione di TLS (o SSL) e sul codice utilizzato per la connessio ne 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 gli URL delle funzioni Lambda	Se crei un'applicazione web serverless utilizzando le funzioni Lambda con gli URL delle funzioni, 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 prestazio ni 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 caratteristica	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 `CloudFront-Viewer-Address` di richiesta	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.	8 settembre 2021
Nuova caratteristica	CloudFront ora supporta i certificati ECDSA per le connessioni HTTPS rivolte agli spettatori. Per ulteriori informazioni, consulta Protocolli e cifrari supportati tra i visualizzatori CloudFront e Requisiti per l'utilizzo dei certificati SSL/TLS con. CloudFront	14 luglio 2021
Nuova caratteristica	CloudFront ora supporta più modi per spostare un nome di dominio alternativo da una distribuzione all'altra, senza contattare. AWS Support Per ulteriori informazioni, consulta Spostare un nome di dominio alternativo in una distribuzione diversa.	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 caratteristica	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 le domande frequenti sul Savings Bundle.	5 febbraio 2021

Nuovo tutorial	L'Amazon CloudFront Developer Guide ora include un tutorial per usare Amazon per limitare l'accesso CloudFront a un Application Load Balancer in Elastic Load Balancing. Per ulteriori informazioni, consulta Limitazione dell'accesso agli Application Load Balancers.	18 dicembre 2020
Nuova opzione per la gestione delle chiavi pubbliche	CloudFront ora supporta la gestione delle chiavi pubbliche per gli URL firmati e i cookie firmati tramite la CloudFront console e l'API, senza richiedere l'accesso all'utente Account AWS root. Per ulteriori informazioni, consulta Specificare i firmatari che possono creare URL firmati e cookie firmati.	22 ottobre 2020
Nuova funzionalità: Origin Shield	CloudFront ora supporta CloudFront Origin Shield, 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. 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 Servire file compressi e Supporto per la 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 in tempo reale	CloudFront ora supporta log configurabili in tempo reale. Con i registri in tempo reale, è possibile ottenere informazioni sulle richieste effettuate a una distribuzione in tempo reale. È possibile utilizzare i registri in tempo reale per monitorar e, analizzare e agire in base alle prestazioni di distribuz ione dei contenuti. Per ulteriori informazioni, consulta Registri 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 caratteristica	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. CloudFront Per ulteriori informazioni, consulta Controllare la chiave della cache e Controllare le richieste di 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 ancora, tutti implementati con. AWS 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 standard dei file di log.	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. 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 caratteristica	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 caratteristica	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 caratteristica	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 Protocolli e cifrari SSL/TLS supportati per la comunicazione tra e l'origine e Informazioni sui cifrari RSA ed ECDSA. CloudFront	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 i 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.